[H.A.S.C. No. 110–148]

NATIONAL INDUSTRIAL SECURITY PROGRAM: ADDRESSING THE IMPLICATIONS OF GLOBALIZATION AND FOREIGN OWNERSHIP FOR THE DEFENSE INDUSTRIAL BASE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES
ONE HUNDRED TENTH CONGRESS
SECOND SESSION

HEARING HELD
APRIL 16, 2008

U.S. GOVERNMENT PRINTING OFFICE
45-132 WASHINGTON : 2009

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

HOUSE COMMITTEE ON ARMED SERVICES

ONE HUNDRED TENTH CONGRESS

IKE SKELTON, Missouri, *Chairman*

JOHN SPRATT, South Carolina
SOLOMON P. ORTIZ, Texas
GENE TAYLOR, Mississippi
NEIL ABERCROMBIE, Hawaii
SILVESTRE REYES, Texas
VIC SNYDER, Arkansas
ADAM SMITH, Washington
LORETTA SANCHEZ, California
MIKE McINTYRE, North Carolina
ELLEN O. TAUSCHER, California
ROBERT A. BRADY, Pennsylvania
ROBERT ANDREWS, New Jersey
SUSAN A. DAVIS, California
RICK LARSEN, Washington
JIM COOPER, Tennessee
JIM MARSHALL, Georgia
MADELEINE Z. BORDALLO, Guam
MARK E. UDALL, Colorado
DAN BOREN, Oklahoma
BRAD ELLSWORTH, Indiana
NANCY BOYDA, Kansas
PATRICK J. MURPHY, Pennsylvania
HANK JOHNSON, Georgia
CAROL SHEA-PORTER, New Hampshire
JOE COURTNEY, Connecticut
DAVID LOEBSACK, Iowa
KIRSTEN E. GILLIBRAND, New York
JOE SESTAK, Pennsylvania
GABRIELLE GIFFORDS, Arizona
NIKI TSONGAS, Massachusetts
ELIJAH E. CUMMINGS, Maryland
KENDRICK B. MEEK, Florida
KATHY CASTOR, Florida

DUNCAN HUNTER, California
JIM SAXTON, New Jersey
JOHN M. McHUGH, New York
TERRY EVERETT, Alabama
ROSCOE G. BARTLETT, Maryland
HOWARD P. "BUCK" McKEON, California
MAC THORNBERRY, Texas
WALTER B. JONES, North Carolina
ROBIN HAYES, North Carolina
W. TODD AKIN, Missouri
J. RANDY FORBES, Virginia
JEFF MILLER, Florida
JOE WILSON, South Carolina
FRANK A. LoBIONDO, New Jersey
TOM COLE, Oklahoma
ROB BISHOP, Utah
MICHAEL TURNER, Ohio
JOHN KLINE, Minnesota
PHIL GINGREY, Georgia
MIKE ROGERS, Alabama
TRENT FRANKS, Arizona
BILL SHUSTER, Pennsylvania
THELMA DRAKE, Virginia
CATHY McMORRIS RODGERS, Washington
K. MICHAEL CONAWAY, Texas
GEOFF DAVIS, Kentucky
DOUG LAMBORN, Colorado
ROB WITTMAN, Virginia

ERIN C. CONATON, *Staff Director*
ANDREW HUNTER, *Professional Staff Member*
STEPHANIE SANOK, *Professional Staff Member*
CATERINA DUTTO, *Staff Assistant*

CONTENTS

CHRONOLOGICAL LIST OF HEARINGS

2008

WEDNESDAY, APRIL 16, 2008

NATIONAL INDUSTRIAL SECURITY PROGRAM: ADDRESSING THE IMPLICATIONS OF GLOBALIZATION AND FOREIGN OWNERSHIP FOR THE DEFENSE INDUSTRIAL BASE

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

WITNESSES

APPENDIX

NATIONAL INDUSTRIAL SECURITY PROGRAM: ADDRESSING THE IMPLICATIONS OF GLOBALIZATION AND FOREIGN OWNERSHIP FOR THE DEFENSE INDUSTRIAL BASE

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
Washington, DC, Wednesday, April 16, 2008.

The committee met, pursuant to call, at 10:05 a.m., in room 2118, Rayburn House Office Building, Hon. Ike Skelton (chairman of the committee) presiding.

OPENING STATEMENT OF HON. IKE SKELTON, A REPRESENTATIVE FROM MISSOURI, CHAIRMAN, COMMITTEE ON ARMED SERVICES

The CHAIRMAN. Ladies and gentlemen, we welcome you to today's hearing on the "National Industrial Security Program: Addressing the Implications of Globalization and Foreign Ownership for the Defense Industrial Base."

I am pleased that we are able to focus on this all-important topic. And, too often, the pace of events and the demands of the war consume us so much that we have a hard time stepping back and looking at the defense industrial base and how, over the years, it is changing.

Today's hearing does just that, by exploring how the Department of Defense (DOD) works to protect the classified information in the hands of the private-sector companies who develop and build and maintain defense systems. These companies are home to the vast majority of our classified information. The National Industrial Security Program is the primary means for ensuring that this information is truly protected.

It has long been this Nation's official policy to be open to the rest of the world. We open our markets to goods from all countries. We are open to foreign investment. And closer to home for this committee, we have sought to be interoperable with the North Atlantic Treaty Organization (NATO) allies, sharing standards, technology, information on both our tactics as well as our procedures.

We provide exceptions to various domestic source restrictions for companies located in NATO allies. The story for our defense industry is no different. We have allowed foreign investment in our defense industry and developed mechanisms like government security committees on corporate boards to ensure the national security is protected.

All of these policy choices are predicated on two fundamental assumptions: that, in working more closely together, we are all made

stronger and that reasonable measures can be taken to protect that which must be protected while remaining open to most things.

Today we examine in greater depth what reasonable measures need to be taken to protect American national security. Industry is changing as the economy globalizes. How rapidly are issues of foreign ownership, control, influence impacting the defense industry? Will new investment vehicles like hedge funds and sovereign wealth funds require us to change how we determine what constitutes foreign ownership? How can the National Industrial Security Program keep up with the scope and pace of these changes? Is the Defense Security Service staffed, is it trained, is it equipped well enough to implement the policy?

Here today to help us answer these questions is a very distinguished group: Troy Sullivan, Deputy Under Secretary for Defense for Counterintelligence and Security; Kathleen Watson, Director of the Defense Security Service; Dr. Bill Schneider, Chairman of the Defense Science Board; Ann Calvaresi Barr, Director of Acquisition and Sourcing Management at the U.S. Government Accountability Office (GAO); and also at the table is Mr. Greg Torres of the Department of Defense, who is here to answer questions.

We welcome you. And before we ask you for your testimony, let me turn to my friend, my colleague from California, Duncan Hunter.

STATEMENT OF HON. DUNCAN HUNTER, A REPRESENTATIVE FROM CALIFORNIA, RANKING MEMBER, COMMITTEE ON ARMED SERVICES

Mr. HUNTER. Mr. Chairman, thank you for holding this very important hearing.

And I think this is an issue that has received little congressional attention but addresses a subject that goes to the heart of an issue that this committee cares very deeply about. In the era of globalization, where international firms regularly compete for U.S. Government contracts, the subject of how the Department of Defense manages the risks associated with foreign ownership, control or influence is of paramount importance, particularly in classified contracts.

This challenge confronts the Department on two fronts. First, consolidation within the defense industry and a weakened U.S. dollar has resulted in an increase of foreign interests acquiring U.S. companies that generate and support what I call militarily critical technology. Second, U.S. defense contractors increasingly rely upon foreign-owned subcontractors to support their contracts and almost always utilize hardware and software that is produced or manufactured overseas.

My overarching concern and issue that I would like this hearing to address today is how we ensure that these trends and developments do not lead to the deterioration of our qualitative edge over potential adversaries.

This is not an irrational fear or veiled protectionism. This is a real national security concern. We are in a period where industrial espionage is on the rise and where cyber attacks on U.S. Government networks are the rule, not the exception. Dr. Schneider's testimony aptly captures this issue when he argues that the success

the defense industry has enjoyed in exploiting modern technology must be, and I quote, "tempered with recognition of the risks and vulnerabilities created by using these cutting-edge systems."

As we manage these risks and vulnerabilities, our initial focus should prioritize the most sensitive national security information and programs: classified contracts. Currently there are over 8,000 companies cleared to conduct classified work for the Department of Defense. They are all governed by the National Industrial Security Program, or NISP, a program which essentially imposes a set of requirements upon a contractor in exchange for a facility security clearance that allows a contractor's facility to access and hold classified information.

The most important feature of the NISP is that contractors are obligated to comply. Unlike the Committee on Foreign Investment in the United States, or CFIUS, the NISP framework is mandatory in nature. All Department contractors holding a facility security clearance are obtained to ensure that classified information is handled in accordance with the NISP.

This raises two primary concerns. The first is a policy question: How do we know that the policies of the NISP adequately manage the risks and vulnerabilities generated by the ever-evolving defense industrial base? My sense is that between the concerns raised in Defense Science Board reports and industrial espionage developments raised by the Department, we face challenges that our current policy is not tailored to address.

A second area of concern is whether the policy presently in place is being implemented properly. In other words, does the pool of 8,000 contractors cleared to conduct classified work for the Department vigilantly follow the requirements in the National Industrial Security Program? Both the GAO report and my own impression are that the culture of compliance varies widely among the population of cleared contractor companies.

I emphasize compliance because the NISP rests on a paradigm that depends upon the self-reporting of cleared contractor companies and their commitment to adopting business and management practices that do not result in the compromise of classified information or adversely affect the performance of classified contracts. In the current climate of industrial espionage and cyber attacks that I have described, we need to ensure that best practices are applied across the board, and vigilant compliance is the only acceptable standard.

One practice that incentivizes contractors to vigilantly comply with the NISP is making a corporation's board of directors serve as fiduciaries for the corporation's fulfillment of NISP obligations. This practice ensures that the most senior corporate officers are attentive to the company's adherence to the NISP. In other words, making the corporation's directors apply the same rigor to NISP compliance as they do with complying with the tax code is a proven way to affect corporate behavior. If these schemes work to ensure that corporations do not run afoul of the U.S. Tax Code, they should probably be adopted in an arena of at least equal importance: national security.

Cleared contractor corporations clearly create this culture of compliance on their own. These companies need the support and guid-

ance of the Department. It is not reasonable to have a policy of, "If you see something, say something," if our government is not educating these companies on what exactly they should be looking for. My understanding is that the Defense Security Service, the DSS, has struggled in recent years in this regard, and I am curious to hear from DSS on the steps that they are taking to ensure that industry has a partner in government that aids and supports industry as they carry out their NISP obligations.

And, finally, Mr. Chairman, I would like to take this committee back to a hearing we held in this room March 2, 2006. On that day over two years ago, we examined the national security implication of the Dubai Ports World deal to take over port terminal operations in six U.S. cities and the ensuing CFIUS review. At the heart of that high-profile crisis were issues that we are talking about today. How does the U.S. Government manage the national security risks related to foreign ownership, control and influence, or FOCI?

In my view, that case was an easier problem to solve than the one before us today, because with Dubai Ports we knew that a foreign entity was making an acquisition. That is not always the case. The tougher problems are the types of cases the NISP is tasked to manage where the FOCI is more subtle and less conspicuous. This is truly a complicated and difficult task and, in my view, requires no less attention by the Congress than what was given to Dubai Ports in the subsequent CFIUS legislation.

So I want to thank you, Mr. Chairman, for holding this hearing. I want to thank our witnesses.

And last, Mr. Chairman, Business Week this week has on its front cover, "E-spionage," a Business Week investigation entitled, "The U.S. military created the Internet. Now the Web may be turning against its maker." "As America fights to protect itself, we uncover startling new instances of cyber spies targeting the government, and traced a path of a pernicious attack aimed at a defense consultant."

The fact that this is in the news, and, Mr. Chairman, we have seen a number of other cases, industrial espionage is now the order of the day and is receiving national attention. And if we are going to maintain this qualitative edge over potential adversaries for the next 5 to 10 to 20 years, we have to ensure that we are not accommodating their industrial bases with a less-than-adequate security arrangement for our own private contractors in this country.

And with the wave of fresh money coming in and acquiring American defense interests and American defense contractors, it has become clear to me that there is only one entity which is truly responsible for making sure that our industrial base is secure, and that is us. And I hope that this hearing lays a base for this committee taking action that will ensure that we have, indeed, a secure technological system in the defense industrial base.

So thanks a lot, Mr. Chairman, for holding this hearing.

I thank our witnesses, and I look forward to your testimony.

The CHAIRMAN. Thank you, Mr. Hunter.

I first call on Troy Sullivan, the Deputy Under Secretary of Defense for Counterintelligence and Security.

Mr. Sullivan, welcome.

STATEMENT OF TROY SULLIVAN, ACTING DEPUTY UNDER SECRETARY OF DEFENSE FOR COUNTERINTELLIGENCE AND SECURITY

Mr. SULLIVAN. Thank you, sir.

Good morning, Mr. Chairman, Ranking Member Hunter, members of the committee. I am Troy Sullivan, Acting Deputy Under Secretary of Defense for Counterintelligence and Security. I am pleased to be here today to talk to you about the Department of Defense's role in the Industrial Security Program.

First I would like to introduce two key players on the Department of Defense team who are here today: Ms. Kathleen Watson, the Director of the Defense Security Service; Mr. Greg Torres, down at the end of the table, who is our Director of Security for the Department of Defense.

Ms. Watson's organization administers the National Industrial Security Program on behalf of the Department and 23 other federal agencies within the executive branch.

Mr. Torres, among other things, is responsible for working with Ms. Watson and others to develop security policy. His office writes and staffs the National Industrial Security Program Operating Manual.

They work closely with the Director of the Information Security Oversight Office and its staff, who are responsible for implementing and monitoring the National Industrial Security Program.

The National Industrial Security Program was created to protect classified information in industry. The Department of Defense has a unique partnership with industry to produce the systems that provide our country with military advantages over current and future adversaries. We have a crucial interest in protecting classified information from compromise, and we take our role as the executive agent for the National Industrial Security Program very seriously.

Globalization and foreign ownership have created a number of serious challenges to the protection of classified information as we process an increasing number of foreign ownership, control or influence actions in defense industry. Our policies must take into consideration this ever-changing dynamic.

In addition to the challenges posed by globalization, the Defense Security Service workforce must be well-trained in these complex areas and be sufficiently sized to address situations in a timely manner. We are not yet where we want to be, but since the arrival of the new leadership in 2006 at the Defense Security Service and in the Security Directorate, we are moving forward smartly.

For example, years of very intense work culminated in the publication of a new National Industrial Security Program Operating Manual in 2006. Based on experience to date with the new manual, we have identified several areas that, if clarified or strengthened, would improve the effectiveness of the Defense Security Service. These issues are being addressed by the Department with the goal of ensuring the Defense Security Service can accomplish its mission.

The other key document, the Industrial Security Regulation, is 22 years old. Portions are out of date and in conflict with the newer National Industrial Security Program Operating Manual. To ad-

dress these concerns, we drafted a revised version of the regulation that complements the newer manual. This draft will enter the coordination process later this month.

The National Industrial Security Program is a cornerstone in the Department's efforts to protect classified research and technology from compromise, but it is not the only arrow in our quiver. Our first line of defense is a personnel security clearance program and the granting of security clearances to industry workers who require access to classified information.

The Department is proud to be working with the Office of Management and Budget, Office of the Director of National Intelligence, and the Office of Personnel Management to develop a new and more effective and timely personnel security and investigative system. The transformation team working this project has a status report due to the President at the end of this month.

While the National Industrial Security Program focuses on classified information, we must not forget the threats to and impact of the loss of unclassified information. The Department has an effort under way to help the defense industrial base better secure defense information on their unclassified networks.

We also work with other federal criminal investigative and counterintelligence agencies on a wide range of defense and proactive programs to identify, neutralize and exploit the threats to our most critical technologies. We work closely with the Federal Bureau of Investigation (FBI) in its program to protect technology and industry, identified by DOD to the FBI as critical.

Defense security and counterintelligence organizations, coupled with the Defense Security Service, provide a formidable capability to assist in protecting our most important research and technologies. But when the FBI joins us in a focused protection program, our capabilities are significantly enhanced.

We must not overlook our partnership with industry. Its very dedicated and talented cadre of security officers is on the front lines of this battle.

Finally, defense counterintelligence and security partner with the scientific, acquisition and defense industry communities to protect from compromise the critical information and technologies from the time the scientist has a "eureka" moment through the decommissioning or demilitarization of a system.

I am sure you are aware of the 2005 GAO report that was critical of the Department's program that addresses security concerns with companies under foreign ownership, control or influence. Although the Department nonconcurred with almost all of the GAO recommendations, the current Defense Security Service Director recognized areas within that program that needed improvement, and she has incorporated the recommendations into her agency's transformation plan. She is also keeping the GAO informed of her progress.

The dramatic changes in the Defense Security Service during the last two years, under the very aggressive and tireless leadership of Ms. Watson, have turned a broken organization into a more robust, fully funded and aggressive agency that is better suited to protect our Nation's secrets.

My boss, the Under Secretary of Defense for Intelligence, Jim Clapper, asked me to relay his personal support for this important program.

In conclusion, the Department works closely with industry in many ways to protect critical technology and infrastructure. The cornerstone of our efforts to protect our classified information and programs is the National Industrial Security Program. We take our community responsibility as the National Industrial Security Program executive agent very seriously.

We understand that globalization and the active efforts of our friends and adversaries to acquire restricted technologies have not abated. With the ongoing revitalization and transformation of the Defense Security Service, we will be even better postured to accomplish this mission.

Mr. Chairman, this concludes my prepared remarks, and I would be happy to respond to any questions.

[The joint prepared statement of Mr. Sullivan and Ms. Watson can be found in the Appendix on page 43.]

The CHAIRMAN. Thank you very much, Mr. Sullivan.

Kathleen Watson, who is the Director of the Defense Security Service.

Ms. Watson.

STATEMENT OF KATHLEEN WATSON, DIRECTOR, DEFENSE SECURITY SERVICE

Ms. WATSON. Good morning, Mr. Chairman, Ranking Member Hunter and members of the committee. I am pleased to appear before you today. I am Kathy Watson, Director of the Defense Security Service.

As Mr. Sullivan indicated in his remarks, the Security Directorate of the Deputy Under Secretary of Defense for Counterintelligence and Security provides security policy for the Department of Defense, to include industrial security policy. The Defense Security Service implements those policies on behalf of the Department of Defense and 23 other federal agencies through the National Industrial Security Program. Through the National Industrial Security Program, the Defense Security Service provides security oversight of cleared companies to ensure they are properly protecting the classified information in their possession.

When I arrived at the Defense Security Service two years ago, I found an agency that was underfunded and understaffed. I think everyone, including the members of this committee, know of our funding shortfalls in the personnel security area. What is perhaps less well-known but equally critical to national security is the National Industrial Security Program and the oversight role we play in regard to industry.

I spent my first year at the Defense Security Service doing a top-to-bottom review. The result is a transformation plan that affects the entire agency. The plan was approved by the Department and includes an additional 145 full-time government positions for the agency. The majority of these positions are in the Industrial Security Program. I am also pleased to report that the Defense Security Service is fully funded in fiscal year 2008 and in the President's budget for fiscal year 2009.

In addition to an increase in resources, the Defense Security Service initiated a number of internal changes in the Industrial Security Program. Most significantly, we developed a risk-based approach to our facility inspections. Of the more than 12,000 facilities we oversee, we identified approximately 1,400 cleared facilities that we considered to be of special interest.

In developing the special interest list, we considered risk factors, such as: poor security ratings in the past; security incidents resulting in loss or compromise of security information; facility size and complexity; performance on classified programs targeted by foreign entities; companies under foreign ownership, control or influence; and other risk factors, such as frequent turnover of facility senior managers and financial difficulties. We continue to define our risk criteria.

This new approach allows our industrial security representatives to better prioritize our reviews, improve quality, and to conduct a more thorough inspection. The result is better security. As I said, all of our 300-plus companies under foreign ownership, control or influence now receive special attention. Our goal is to ensure that necessary countermeasures are in place by the closing date of the transaction.

The Defense Security Service took to heart the recommendations of the 2005 GAO report and has incorporated them into its transformation plan. For instance, we are improving and increasing training for our personnel working foreign ownership, control or influence issues, and we are devoting 11 of our new full-time government positions to this area. Three of these positions will be at our headquarters, and eight new positions will be in the field. Both of these initiatives address the GAO's recommendation that the Defense Security Service formulate a human capital management strategy for our foreign ownership, control or influence personnel.

The Defense Security Service is now contracting for an independent study of the effectiveness of the overall foreign ownership, control or influence process, to include a review of our internal business processes. This study will also evaluate whether we are gathering the proper information to effectively analyze and oversee these companies and we have fully integrated counterintelligence into the foreign ownership, control or influence analysis and oversight.

Finally, the Defense Security Service has reviewed and plans to adopt the Department of Energy's automated foreign ownership, control or influence management application called e-FOCI. We completed a six-month test phase in March of 2008 and plan to phase in additional users between now and fulfilling of the complete application in September of 2009.

After some modification, the application will give us visibility of all such transactions in real-time, from inception to final mitigation. e-FOCI will also improve our capability to conduct analysis and improve our ability to identify trends. I believe these initiatives will help us meet the final two GAO recommendations for better data collection and a more systematic analysis.

There is still much work to be done at the Defense Security Service. We still rely on antiquated information systems internally and face a serious hiring lag for new positions. But now that we have

the appropriate resources, we can fully implement our transformation plan and strategically position the agency for the future.

Mr. Chairman, this concludes my statement. I am available to answer any questions you may have. Thank you.

[The joint prepared statement of Ms. Watson and Mr. Sullivan can be found in the Appendix on page 43.]

The CHAIRMAN. I thank the gentlelady.

A longtime friend of this committee, Dr. William Schneider, Chairman of the Defense Science Board, welcome again. Good to see you.

STATEMENT OF DR. WILLIAM SCHNEIDER, JR., CHAIRMAN, DEFENSE SCIENCE BOARD

Dr. SCHNEIDER. Thank you, Mr. Chairman. It is a great privilege to be here. I look forward to this opportunity to present my testimony.

I have provided the committee with a detailed statement, and, with your permission, I would like to just give a brief oral summary of that statement.

The CHAIRMAN. Without objection, each of the prepared statements will be put in the record. Thank you.

Dr. SCHNEIDER. Thank you, Mr. Chairman.

The impact of globalization on the Department of Defense and its mission has been an important aspect of Defense Science Board studies for more than a decade. The globalization of technology is no longer a choice for governments planning to modernize their military forces; it is a characteristic of the environment in which military capabilities will be developed and produced for the foreseeable future.

Among the most pervasive factors responsible for the vast increase in international trade and investment since the end of the Cold War has been the deregulation of trade in advanced technology. The globalization of access to advanced technology has meant that users as well as producers of modern technology are able to share access to a common global technology base and markets. This nearly universal access to advanced technology has accelerated its propagation and has revolutionized the process of innovation in most technology-driven industrial and service industries, including the defense sector.

Although legal and regulatory factors in the defense sector have slowed the impact of globalization on its research and development (R&D) and acquisition processes compared to the private sector, the DOD too has succumbed to its technical, commercial and industrial logic. By exploiting the technologies created or enhanced by the process of globalization, the military capabilities fielded by the Department of Defense have been swiftly transformed from its industrial-age character that dominated its capabilities at the end of the Cold War. The process of transforming of U.S. military capabilities to highly adaptive information-age capabilities appropriate to the 21st-century threat environment is now at an advanced stage.

The globalization process has provided important cost, schedule and performance benefits to the DOD and its industrial base. The underlying technologies which create the most decisive modern

military capabilities are derived from developments in the civil technology sector. The highly competitive civil technology sector is thoroughly globalized. The pace of its development of technology is very rapid compared to the technologies developed solely within the defense sector and are usually associated with both declining costs and increasing capabilities.

The DOD has been very successful in applying the benefits of globalization to many of its critical mission areas. For example, substantial improvements in counter-improvised explosive devices (IED) technologies and mine-resistant armor-protected vehicles used in Iraq and Afghanistan are products of foreign developments brought to the United States through the CFIUS process and managed as foreign owned, controlled or influenced entities by the Defense Security Service.

The success the defense industry has enjoyed in its exploitation of the globalization of modern technology must, as the ranking member noted, be tempered with the recognition of the risks and vulnerabilities created by this evolution in the manner in which military capabilities are created.

Protecting America's military edge depends in part on the effectiveness of the National Industrial Security Program. The fact that an increasing fraction of the underlying technologies that are drawn upon by the defense industrial sector to create advanced military capabilities developed in the civil sector—and, in many cases, are developed abroad—changes the environment in which the Industrial Security Program must operate.

This is so because the core military capabilities we create resides not in the technology itself, but in the manner in which these civil technologies are converted into military capabilities. The details of how these technologies are engineered into military systems, especially the software and algorithms used to render the hardware effective in its military applications, and the manner in which individual systems interact in a system of systems is at the heart of what the industrial base needs to protect from potential adversaries.

In the 1990's, the DOD recognized that it was becoming increasingly dependent on the globalization of the technology base. To increase DOD's access to advanced technology, the DOD made some shrewd decisions in the 1990's that have been re-enforced by subsequent decisions in recent years. The executive branch took two parallel paths toward improving access to advanced technology in the international market.

First, the U.S. Government sought to reform the process by which the DOD could procure defense products from producers abroad. The executive branch sought to liberalize the defense trade process both during the Clinton and the current Bush Administrations. The key elements of the proposed process-liberalization initiatives—the Clinton Administration's Defense Trade Security Initiative in 2000 and the Bush Administration's NSPD–19 defense trade process reform initiative in 2002—were both rejected by the Congress, although some of the reforms were subsequently incorporated in U.S. Government practice administratively.

The other dimension of the reform process has been much more successful. In the early 1990's, the DOD liberalized the process per-

taining to the regulation of foreign investment in the defense sector. The policy change encouraged foreign investment in the defense sector, but did so by the DOD's embracing of mitigation measures known as special security agreements, and some variants of those, which mitigates the risk that the presence of a foreign investor might pose to the security of U.S. classified and export-controlled technology in the possession of a cleared U.S. company. The mitigation process focused heavily on industrial security, as established in the National Industrial Security Program Operating Manual.

The mitigation process I have described is one with which I have considerable personal experience. For more than 15 years, I have served as an outside director on the U.S. subsidiary of foreign-domiciled firms in the U.S. defense sector. My personal experience with this process is entirely satisfactory from the perspective of meeting the aims of the program. The security compliance with both classified and export-controlled information is of a very high order, reflecting the preoccupation with security of the U.S. managers of the subsidiaries. At the same time, the firms are adding value to the U.S. defense program by bringing investment and advanced technology to the defense market that expands and strengthens the industrial base resident in the United States.

The threat posed to the security of information for both foreign firms present in the U.S. market as well as U.S. firms, including classified and export-controlled information, is evolving. As I have noted, much of the underlying technology that drives the creation of advanced military capabilities is unclassified, and this information resides on computer networks. These networks are now the focus of attacks by potential adversary states and nonstate entities.

The President's Cyber Security Initiative addresses a very important gap in the ability of the industrial base to protect its proprietary, unclassified information. The industrial base, domestic- or foreign-owned, lacks the knowledge that only the U.S. Government possesses about how to protect their computer networks that are part of a larger, national information infrastructure from foreign computer network exploitation and attack.

The area of cyber security appears to be the domain in which the technology security of the defense industrial base is most at risk for both domestic- and foreign-owned firms operating in the U.S.

Mr. Chairman, I would be pleased to respond to any question you or members of the committee may have. Thank you very much.

[The prepared statement of Dr. Schneider can be found in the Appendix on page 51.]

The CHAIRMAN. Dr. Schneider, thank you for being with us.

Ann Calvaresi Barr, welcome.

STATEMENT OF ANN CALVARESI BARR, DIRECTOR, ACQUISITION AND SOURCING MANAGEMENT, GOVERNMENT ACCOUNTABILITY OFFICE

Ms. CALVARESI BARR. Thank you.

Mr. Chairman, members of the committee, thank you for inviting me here today to discuss GAO's work on the National Industrial Security Program and Defense Security Service's (DSS) oversight of it.

As you know, our body of work on government mechanisms designed to protect critical technologies while advancing U.S. interests has revealed alarming gaps in our safety net for keeping certain defense-related knowledge out of the wrong hands. Systemic vulnerabilities, not only in industrial security but also with export controls, foreign military sales and foreign acquisitions, were so significant that GAO designated the effective protection of technologies critical to U.S. national security interests as a government-wide high-risk area in 2007.

Today I will describe how improvements to DSS's Industrial Security Program could strengthen our protection of critical technologies. Let me start by briefly summarizing three key weaknesses we reported on in 2004 and 2005.

First, DSS cannot determine how well facilities are protecting classified information because it lacked overall data on the quality of compliance, the types of violations and their frequency. Regarding contractors under foreign ownership, control or influence, DSS did not know the extent to which these contractors reported foreign involvement in a timely manner or had access to classified information before protective measures were put in place.

Second, DSS did not properly identify possible compromises to classified information, as required in their operating manual. For roughly 75 percent of the 93 violations we reviewed, DSS either made no determination regarding compromise or made determinations that were ambiguous and not covered in the manual. As a result, affected agencies were not notified of violations and, therefore, could not take any action to mitigate damage that may have occurred. In cases where clear determinations were made, DSS often did not notify affected agencies in a timely manner. In one case, notification was delayed five months.

Third, DSS field staff lack the guidance, training and tools necessary to effectively carry out their oversight responsibilities. Of particular concern is their lack of understanding about corporate structures, legal ownership and complex financial relationships. And this occurs when foreign entities are involved. This is knowledge that is basic to determining and mitigating risk and then effectively overseeing contractors' actions.

Addressing these and other weaknesses we found would help mitigate the risk of classified information being compromised. For example, identifying patterns of violations based on factors such as the type of work conducted at the facilities, the facility's government customer and the facility's corporate affiliations would enable DSS to identify problems and target needed actions. Similarly, timely notification of potential compromises to classified information would allow affected agencies to take stock of the damage and promptly take needed action to further minimize loss.

We made a number of operational recommendations aimed at better ensuring that classified information entrusted to contractors would not be compromised, many of which DOD did not initially concur with. We are pleased, very pleased, to hear, as Ms. Watson pointed out, that DSS is now working to strengthen its Industrial Security Program. Notably, and also as Ms. Watson pointed out, DSS implemented a strategy to better position its industrial security representatives, a strategy consistent with our recommenda-

tions to provide targeted training for identified skill gaps and explore options for improving headquarters' support of field operations.

While we are certainly encouraged by DSS's initiative, other actions, as Ms. Watson also alluded to, are needed to fully address our recommendations.

Mr. Chairman, I would like to thank you again for giving us the opportunity to be here today. As our designation of "high-risk" indicates, the protection of critical technologies warrants a strategic re-examination of existing programs to identify needed changes and ensure the advancement of U.S. interests. I believe this hearing contributes to that strategic re-examination.

This concludes my statement. I would be happy to answer any questions that you or other members of the committee have. Thank you.

[The prepared statement of Ms. Calvaresi Barr can be found in the Appendix on page 60.]

The CHAIRMAN. Thank you very much.

I understand, Mr. Torres, you are here to answer questions. Am I correct?

Mr. TORRES. Yes, sir, that is correct.

The CHAIRMAN. Thank you.

I will just begin with two very quick questions to Ms. Watson, if I may.

You stated that the Defense Security Service was underfunded and understaffed when you first arrived. That was two years ago. Is that correct?

Ms. WATSON. Yes, sir.

The CHAIRMAN. Do you have enough staff today and are you fully funded today to do your job?

Ms. WATSON. I am fully funded to do my job. We had an increase in our budget in the last year of $80 million, which is substantial.

We are not properly resourced yet in terms of personnel because of the hiring process in the Department. I have the government positions available. We are hiring at DSS across the board. Almost half of the new hires are going to the Industrial Security Program, both in headquarters and in the field.

The CHAIRMAN. How short are you, as we speak, in staff?

Ms. WATSON. Well over 100.

The CHAIRMAN. What is your total number of staff members?

Ms. WATSON. Total DSS is about 750, give or take a few positions.

The CHAIRMAN. Good. Thank you very much.

Mr. Hunter.

Mr. HUNTER. Thank you, Mr. Chairman. And, again, thanks for holding this hearing.

Let me go to a—I have here one of the certificates that are filled out with respect to the degree of foreign ownership. And I noted that the requirement to update the certificates has been changed, the reporting requirements have been changed to be updated only when there are, quote, "material changes" to the information previously reported.

Are any of you folks up to speed on this certificate and the fact that it is now—that the update for the certificate of foreign owner-

ship is now basically discretionary and it is only triggered when you, the company, feel that there is a, quote, "a material change" in the ownership, which would seem to be very vague?

Are you up to speed on that at all?

Mr. TORRES. Sir, I will take that question.

The requirement was changed in the 2006 National Industrial Security Program Operating Manual (NISPOM) from a mandatory filing every five years, and that is no longer required. However, there is a requirement that any time a material change occurs, reporting is required. And a material change is defined as any change to the answers to the questions on the form.

In addition to that, we——

Mr. HUNTER. Now, say it again. A material change is identified as what?

Mr. TORRES. Any change to any of the answers on the form. So if you changed an answer to the question from a "no" to a "yes," that now somebody has more than a five percent interest, you need to report that.

We have received information that this information, what a material change is, may not be sufficiently understood, and we are working with the Defense Security Service on a process to make sure that that is clearly understood.

But in addition to that requirement to report voluntarily, Defense Security Service, in their program of oversight, does ensure that those questions are asked and that is part of their inspection cycle. And Ms. Watson may have additional information on that.

Ms. WATSON. Mr. Torres is correct; we do routinely inspect these companies, usually at least once every 12 months.

In addition to the formal inspections, we have a robust advice and guidance program at DSS, which takes much of the time of the industrial security representatives in the field. We have a robust relationship with our industry partners, with the facility security officers. So any time they have a question or are looking for guidance, they contact us as a matter of routine.

So there is much more to the DSS oversight than a once-a-year inspection.

Mr. HUNTER. Okay. Well, the reason I ask that question is, I mean, the term "material" is in the eyes of the beholder. And it seems to me, on something this important and in an area that requires clarity and requires accountability, that is generally tossing the ball to the contractor and letting them make a determination, which may or may not be a timely response to something that is very important.

Now, with respect to the ownership of a company, you have all these new devices now that manifest property ownership—hedge funds, for example. How do you tell if a hedge fund has now become part owner of this organization if you don't know who the investors in the hedge fund are?

Ms. WATSON. Well, you have pointed out how difficult our job is at DSS. I want to make a couple of comments about your question.

In terms of the definition of "material change," we agree with you that it needs to be clarified in order for us to perform our oversight function. We are issuing, in conjunction with the Security Directorate, an industrial security letter. That is a tool that we have

to update policy as a matter of routine. And that will be going out in the near term.

DSS, after implementing the new NISPOM for the last two years, has recommended that additional guidance be provided, because there is confusion in industry on that point.

Mr. HUNTER. Well, why don't we just go back to the time-certain reporting requirement that you had, where it wasn't discretionary as to whether or not these companies report in?

Ms. WATSON. Well, it seems to me that that is one way to attack the problem, but with the fast-paced business world that we are living in, I don't know that an update every five years is going to give us the information we need.

Mr. HUNTER. Well, then make it shorter, but make it—you could have both cases. That is, if you have a material change—and make sure that they know up front precisely what that means—that if there is any change in ownership, that it be reported. But then also have a time certain when they simply have to submit a new report.

But of the 8,000 contractors that you folks are monitoring, how many DSS industrial security personnel do you have monitoring those 8,000 contractors?

Ms. WATSON. We have approximately—in the agency, about half of the workforce is dedicated to the Industrial Security Program. We have about 350 full-time equivalents (FTEs) in that program.

Mr. HUNTER. So you have about 175 people?

Ms. WATSON. No, no, 350 on the industrial security——

Mr. HUNTER. But you said about half of them—okay, about 350 people monitoring the contracts?

Ms. WATSON. Yes.

Mr. HUNTER. Okay. And that is for about 8,000 contractors?

Ms. WATSON. And 12,000 facilities, yes.

Mr. HUNTER. Okay.

Now, Ms. Calvaresi Barr—did I get that right?

Ms. CALVARESI BARR. You did get that right. Thank you.

Mr. HUNTER. Okay. You said that the GAO's analysis here, you found that you had folks in DSS that didn't understand the complexity of these ownership vehicles. I think that is something that we are seeing across the financial world right now, is that things are packaged, repackaged, ownerships are less than transparent, you have these funds—I have talked to defense contractors, in an anecdotal sense, who have said, "My gosh, we have this new entity come in, and we say, 'Who are the owners coming to buy very sophisticated, very sensitive stuff?', 'It is a fund.' Well, who owns the fund?"

So my question is—and this goes back to whether there is a material change in ownership. If you have a hedge fund getting into basically an investment pool, getting into ownership of a sensitive defense contractor, how do we ascertain who the real owners are, who the owners in interest are of this particular entity?

Ms. CALVARESI BARR. Representative Hunter, you raise a very good issue and one which not only the U.S. is concerned about but many other countries as well. Hedge funds, sovereign wealth funds—this is an issue of great complexity, and it is very often difficult to know where the money is coming from and who the rightful players are.

I believe that this speaks to the work that we conducted at DSS on a couple of fronts. One was that many of the industrial security representatives that are out there trying to determine the extent to which there is foreign involvement, ownership and influence have difficulty navigating their way through these complex financial relationships, corporate structures.

And it was for that very reason that we made a series of recommendations that indicated that there needed to be more training or guidance in terms of how to review contractors that are under foreign ownership. It is a difficult job. The industrial security representatives, many of them, spoke with us about the difficulties that they had, that they lacked the basic tools and the knowledge to really do their job well. And I think the examples that you bring up with hedge funds and sovereign wealth funds point to those difficulties.

The other point that I would like to make was earlier about when a material change has occurred. Our work did point to the fact that very long periods had transpired before DSS was aware of any material changes. And that was one concern that we had regarding the timely notification when changes did occur.

So those were some of our findings, and we made some recommendations to address both of those points.

Mr. HUNTER. Okay. And you made a statement about the shortcomings you saw in the security system. Then you stated that DSS has moved to address those shortcomings; you are pleased in some areas to see the progress.

So I think the general question from the committee would be evaluating—that you saw a problem, that DSS is moving at least in the direction of solving the problem. How would you grade the—where would you put the present state of affairs, with respect to security? On a 1 to 10, where were they when you made your analysis?

Ms. CALVARESI BARR. We——

Mr. HUNTER. And I know it is broad, but we are trying to get a bird's-eye view here.

Ms. CALVARESI BARR. It is very broad. I can comment back on when we looked at it. I want to be fair here. We looked in 2004, and we looked in 2005. So we are not current, given the changes that have occurred.

But on a scale of 1 to 10, I think the fact that we made 8 recommendations in one report, 8 recommendations in another, we felt that the program was woefully inadequate to identify when there were risks in place and the fact that they had measures to protect unwarranted access to classified information. I would certainly put it below average.

Mr. HUNTER. Okay. Now that they have undertaken some steps that you have talked about, have you evaluated where they are now, having taken those steps?

Ms. CALVARESI BARR. We have not had an opportunity to go back and evaluate. As part of GAO's process, every year when we make recommendations, we go back and follow up to document the extent to which those recommendations have been implemented. We made a total of 16 recommendations in those 2 reports. We have currently closed two of those recommendations, but we are working

closely with Ms. Watson to gather documentation to determine what impact they have had.

And, again, these are steps in the right direction. The initiatives are good. But, as we all know, guidelines and initiatives are one thing. It comes when you really look at the implementation, what differences are really occurring once the new guidelines and implementation takes place. And we have not done that yet.

Mr. HUNTER. So you haven't. So that is a work in progress, so you can't tell where you would place them right now.

Ms. CALVARESI BARR. I could not.

Mr. HUNTER. Would you agree that this is a critical area to national security and one in which Congress should be involved in oversight?

Ms. CALVARESI BARR. Absolutely a critical area.

And as I mentioned in the beginning, I wanted to put the Industrial Security Program in the context of the larger safety net of those programs that are there to protect what is critical to the U.S. Those include things like, as you mentioned, CFIUS, foreign military sales, anti-tamper, the export control process. Industrial security is just one component of that.

But I think, as we talk about the rapidly growing trends in globalization and the foreign influence that we have, it is absolutely essential that each individual program within that safety net work effectively. And they all rely on each other working effectively.

I would say, right now, the larger safety net of programs that we have in place to protect what is critical, that safety net looks like Swiss cheese. It needs to be addressed; it needs to be fixed.

Mr. HUNTER. Okay. Thank you.

Mr. Chairman, I would just say to my colleagues, I think this is going to be one of the critical issues of the coming years, because there is a lot of cash money out there in the world now; there are a lot of cash-hungry American companies, including companies in the defense complex. And the potential for targeting sensitive security areas by these sovereign wealth funds and by nefarious participants in these hedge funds, that opportunity is very large right now and will be large for the coming years.

And there is one entity that is responsible for making sure that we keep this security; that is us. And my urging to the committee is that we exercise strong oversight in this area, much more than we have done in the past.

And I am reminded about the Huawei corporation, this Chinese corporation which was trying to buy 3Com in partnership with Bain Capital. 3Com does cybersecurity contracting for the Department of Defense. And the fact that Huawei is a Chinese corporation closely connected with the Chinese military—also happens to be the people that helped Saddam Hussein set up his air defense systems against Americans—and the fact that they came close, from the report that I got—we urged CFIUS not to support this, not to give the okay or the green light to this particular transaction—but they came close to making that acquisition with the compliance and participation of a so-called responsible American investment fund, I think is illustrative of this challenge we are going to have over the next 5 to 10 years.

We have people with lots of cash, and we have American companies desperate for cash, and that creates a very difficult situation. So I hope that the committee weighs in in this area.

And I will have some other questions at the end. Thank you for letting me take so much time, Mr. Chairman.

Mr. ORTIZ [presiding]. Thank you. Let me say thank you so much for the work that you do. This is not an easy job that you have. It is a very sensitive area. Sometimes it is hard to understand.

Like my good friend, Mr. Hunter, was stating, there are people all over the world, a lot of joint ventures going on, people going to different countries to join in the joint ventures; and sometimes in these joint ventures they might develop something that, unknown, later becomes a very sensitive equipment.

So how do we get these people to apply or work with your office and to tell you that they have developed this sensitive equipment? How do you police that? Sometimes it might be ignorance of some people. And some people might be hungry for money, and they just want to develop that incentive. So at what point do you get some of these companies or joint ventures to come and report to you? Or do you go to them?

Any one of you that can try to answer that.

Ms. WATSON. The role of DSS, sir, is right now confined to the classified arena. So DSS would only be involved if there was a classified contract.

Mr. ORTIZ. Okay. I know that your problem has been complicated. As I was looking at the statement by Ms. Calvaresi Barr, where you state here that DSS industrial security representatives face several challenges in carrying out the foreign ownership control responsibilities, largely due to complexities in cases because of the limited tools that you have, the research, insufficient foreign ownership control, training, staff turnover, and inconsistencies in implementing guidance on these foreign licenses.

Now let's talk a little bit about staffing. Are you adequately staffed now?

Ms. WATSON. Not at this moment. I have available positions, and I am hiring. I believe we will be adequately staffed once we fill up all of our positions.

Mr. ORTIZ. How many staff members will you normally have when you are staffed adequately?

Ms. WATSON. We are authorized around 750 people now. That is an increase of about 150 from a year ago.

Mr. ORTIZ. Now when you talk about tools that you might not have, what are the tools that you will try to either obtain so that they can make your job easier for you or maybe we are not giving you enough money to buy those tools?

Ms. WATSON. In the past, we did not have enough money to buy the tools. We have right now an electronic database that we use. It does not provide us with the information we need to properly manage our workload or to perform analysis, so data retrieval is still a problem for us. We have analyzed that system. We are in the process of defining requirements to upgrade it so it will get us the information we need.

In addition to that, we are adopting the electronic tool that the Department of Energy uses to manage their FOCI cases. I believe

the Central Intelligence Agency (CIA) will be using the same system. So all the keys agencies that are involved in this process will be on the same electronic system, which will allow us to do, again, better data retrieval and provide us with the analytic tools that we are now lacking.

In terms of training for our people, I do want to make a comment about that. We recognize how complex the FOCI world is. GAO is right to point out that our folks in the field were not properly trained. Training was one of the first things to go at DSS over five years ago.

Because of the complex workload that we have, what we have done now is singled out a cadre of 12 people that are currently employed in DSS in the field, and we are in the process right now of giving them specialized training so that they understand business structures better and are better armed to perform the work. So that we will be funneling FOCI cases to those folks in the field. The more complex cases will still come to headquarters, where we have a very small core. Right now, we have five people, two of whom are leaving. We are in the process of beefing up the staff, but it is a challenge right now.

When I came to this agency two years ago, it was broken across the board, and it took a year to figure out where the problems were and design a transformation plan. We just got our resources six months ago. This is an agency in transition. It will be an agency in transition for as long as I am there. We have a lot of work to do; and, in my view, we have just started.

Mr. ORTIZ. If you don't mind, we want to help you; and I think this is a very, very important subject we are talking about today. It is a very important issue. We talk about the world getting smaller because of new technology, coming closer and closer to each other. We want to help you.

If you don't mind, if you can give a list to the chairman, we want to help you with the technology you need, the tools that you need, so that we can help you.

Ms. WATSON. Okay.

Mr. ORTIZ. We want to work with you.

Let me compliment you on the great job that you do. It is not easy. I know it is very complicated. I don't want to take too much time because we have got a lot of members who would like to ask a lot of questions.

Now to my good friend, Mr. Saxton.

Mr. SAXTON. Mr. Chairman, thank you.

Let me just follow up on a couple of the chairman's points.

First of all, Ms. Watson, let me add my thanks to you for what you are doing. I think all the members of the committee appreciate the job that you are doing, because this is such an important set of issues, and it is important and emerging, I guess.

Ms. WATSON. Yes.

Mr. SAXTON. The subject of globalization of the economy certainly has ramifications on this topic. In fact, it is driving what it is that we are concerned about here. International investment, international cross business tendencies, and the openness that the chairman talked about when he was opening this hearing all are issues that are helping to drive our concern and your concern as

well. When I say "your concern," I am talking about all of you who are here trying to help us understand this set of issues.

Let me just ask this. In terms of our acquisition program, the total universe of issues that we need to be concerned about are not just those that are worked by the Defense Security Service. We also have to have concerns about—while you are concerned about classified programs, we also have to be concerned about nonclassified programs, don't we?

Ms. WATSON. Yes, sir.

Mr. SAXTON. So is there anybody watching the nonclassified programs?

Mr. TORRES. I will take a little bit of that question, if I could.

Another responsibility within our office is to write policy for research technology protection. Particularly, that program is designed to help research and technology personnel in identifying what their critical information is, specifically, CUR, controlled unclassified information, so we can make sure the right protections are put in place for that classified information. That particular document for research technology protection is drafted and currently in coordination in the Department.

But, to answer your larger question, I am not aware of anyone who has an affirmative role or mission over industry to actually look at those particular programs similar to the way Defense Security Service does for classified programs.

Mr. Sullivan may have some additional information.

Mr. SULLIVAN. There is one initiative going on being led by Mr. John Grimes, Assistant Secretary of Defense for Network Integration; and that is to take a look at unclassified computers in the defense industry. As we all know, the unclassified computers have been subjected to an awful lot of attacks by foreign governments, foreign countries, or at least coming from those directions.

There is an extremely important program going on right now to work with industry to do a couple of things, and I can't discuss most of them in this forum. But I think it would be handy for either us to point your staff toward Mr. Grimes and his staff or us to give you a little background.

Mr. SAXTON. Outside of Mr. Grimes, there is no—yes, sir.

Dr. SCHNEIDER. Mr. Saxton, if I could add a point on this. An important fraction of the unclassified information is export-controlled. Those technologies are managed under the International Traffic and Arms Regulations, which in turn is the responsibility of the Department of State. The mitigation plans required for foreign-owned, controlled or influenced companies, for example, in their special security agreements, include provisions relating to the protection of export control but unclassified information.

The Department of State has conducted some inspections, I know, of foreign-owned, controlled, and influenced companies. I suspect that if the committee wanted further information on the management of the unclassified defense technology that is export controlled, it could be obtained from the Department of State.

In parallel, the Department of Commerce has the Export Administration Regulations, which it is responsible for enforcing.

Mr. SAXTON. Ms. Calvaresi Barr, I know you want to say something, but let me just try to put a frame around what I think I am hearing.

There are a variety of organizations, computers, Department of State, maybe some others, who have some fragmented responsibility of looking at Defense procurement as it relates to unclassified programs. But there is nothing like the Defense Security Service in the Department of Defense looking particularly at unclassified programs.

Ms. Calvaresi Barr.

Ms. CALVARESI BARR. I think it is correct that there are a myriad of programs and policies that are in place, some of which deal with unsensitive, unclassified information, equipment, know-how components. Export controls plays, as Dr. Schneider said, a very, very large part in that.

What I wanted to mention is that GAO has conducted a body of work on the export control system and has found significant weaknesses and vulnerabilities in those systems as well. And I think I would take it back to where I started, that you have this larger safety net of programs with overlapping roles and responsibilities, and it is absolutely critical that each of those programs work hand in hand with one another and coordinate closely in our work, not only within the individual systems but looking at how well they were working in terms of sharing information and cooperation was not very good.

Mr. SAXTON. Thank you.

My time has expired, Mr. Chairman. I thank you for having this hearing.

I wanted to ask if you could describe—and perhaps some other members can pick up, because my time is over—but I wanted to ask you if you can describe exactly what an FOCI case is. I wanted to delve into this so-called self-reporting issue a little bit more. Because, obviously, we need help, Ms. Watson, and you need help in providing your role as a monitor on these so-called self-reporting—my word—self-reporting cases. Perhaps some other members will pick up on those issues.

Thank you.

Mr. ORTIZ. Thank you.

Mr. Snyder.

Dr. SNYDER. Dr. Schneider, I am over here. You can call me doctor, because I am a medical doctor.

Earlier, Mr. Hunter was having a question with the other panelists about the hedge funds and the flow of money. Do you have any comments on that issue of investors?

Dr. SCHNEIDER. Yes. There is, especially in the case of advanced technology industries, a great deal of interest on the part of passive investors, including hedge fund and investment in this sector. The responsibility, of course, for managing these investors largely falls to the Securities and Exchange Commission because of their responsibilities in that segment of the financial services sector. Publicly held companies, the ownership is changing hour by hour. It is an unusually complicated arrangement.

This is why the Defense Security Service, in the implementation that I am familiar with, with foreign-owned, controlled, and influ-

enced companies, that when an investor buys it there is a great deal of specific disclosure required to understand who is the ultimate owner of the company. But, in addition, there are other provisions in the mitigation measures to separate the foreign investor from the control technology. The details of that are contained in the agreement between the parent company and the Department of Defense that separates them from those matters.

So the effectiveness of protecting the information from unauthorized disclosure, whatever the ownership situation is, is critical. That is those mitigation measures must be in place and must be effectively administered in order to maintain this barrier between the foreign investor and the information that is managed by American citizens who would be working in the subsidiary in the U.S.

Dr. SNYDER. Regardless of who is buying in and out of the hedge fund or in or out of the investor pool of money.

Dr. SCHNEIDER. Correct.

Dr. SNYDER. Ms. Watson, I had a couple of questions I wanted to ask you.

In the GAO statement, on page two, it talks about your files on contract or facilities security program and their security violations. It says, "Further, the manner in which this information was maintained, geographically dispersed, paper-based files, did not lend itself to this type of analysis." Do you all have paper-based files?

Ms. WATSON. We did.

Dr. SNYDER. Why?

Ms. WATSON. The agency has been underresourced for approximately 20 years. We now have a database, the industrial securities facility database we use. It is not a system that I would call the system of the future. It is what we have now. It now houses the information that is collected in the field so that we have a more robust oversight and cross-fertilization within the agency.

Again, that is a system we have just looked at, and we are making recommendations for upgrades and in the process of defining the requirements for the upgrade so that we have a better system.

Dr. SNYDER. Do you even know how many geographically based dispersed files are out there? I would think you would be talking thousands.

Ms. WATSON. In terms of files, exactly, no. We have 71 field locations throughout the United States, and one of the responsibilities of the industrial security representatives who are doing this work is to input the data they collect from the companies into the database.

Dr. SNYDER. Would all those geographically dispersed files be at one of those 71 sites?

Ms. WATSON. They all have access to the entire database.

Dr. SNYDER. But the files would not still be at the companies. They would have been filed at one of your sites. Is that correct?

Ms. WATSON. Our files are not at the companies. They are at our sites and at our database, yes, sir.

Dr. SNYDER. You made reference to lack of resources in the past and your improvement in resources and you are still working up your staff as far as the security clearances. What is your current backlog in terms of how far behind are you in numbers and of time in terms of the security clearances?

Ms. WATSON. Are you talking personnel security clearances or facility clearances?

Dr. SNYDER. For the facilities.

Ms. WATSON. Facility, it generally takes us—I don't know the current backlog, but it takes approximately up to 180 days to get a facility clearance. The reasons for that are, one, we need to make sure that the company has a facility security officer. They have to have a facility security program.

Dr. SNYDER. But you don't know right now how many companies are waiting?

Ms. WATSON. No.

Dr. SNYDER. How much delay there is?

Ms. WATSON. No.

Dr. SNYDER. Thank you.

Mr. ORTIZ. Now we have our own scientist, Mr. Bartlett.

Mr. BARTLETT. Thank you very much.

With the globalization of technology and industry, we are increasingly challenged to maintain the premier military in the world. Essential to that, of course, is our ability to be able to tap into the enormous resources represented by our small business community.

A bit more than half of all the employees in our country work for small businesses. Way more than half of all of the new innovations come from small business. I note that in the little summary given to us by staff it says that private industry or college or university must have a bona fide contract requirement that necessitates a facility to hold or store classified information before they can get a classified contract. But to get a classified contract, you have got to have a facility that is cleared. Not only that, you have to have employees that are cleared to do classified work.

Now we have kind of solved the employee problem by having a mentor program where the employees of small business are temporarily moved to a large business which has a classified contract so that they then have a justification for asking for a security clearance for the individual.

How do we work around this catch-22, that in order to get a security clearance for your facility you have got to have a contract that requires that, but, to get the contract, you have to have the clearance? How are we working around that?

Ms. WATSON. I would like to take that question for the record.

Mr. BARTLETT. You would like to take that question for the record.

[The information referred to can be found in the Appendix on page 77.]

Mr. BARTLETT. On almost a daily basis I have representatives from small business coming through my office with exciting new technologies, and they are out there waving their hands. And here I am. I have got this great new technology, and nobody is noticing.

You can't ask for what you don't know exists. When they have the additional hurdle of—many of these things are going to end up classified, because they really are cutting-edge technologies. They have the additional hurdle of not being able to get a classified contract because they don't have a facility which has clearance.

So we have got to work around that somehow. How are we doing that?

Ms. WATSON. One way to work around it is if there is a government activity that is interested in contributing with that company on a classified basis, they can sponsor the company for a facility clearance.

Mr. BARTLETT. Do what?

Ms. WATSON. Sponsor the company for a facility clearance.

Mr. BARTLETT. Before they have the classified contract.

Ms. WATSON. Yes, sir.

Mr. BARTLETT. Somehow, Mr. Chairman, there has to be a shortcut to this. Because these small businesses have limited capital. They really can't hold on for a year or so while these things happen.

And from my personal experience, I know that there is a great deal of technology out there in the small business world that we are having great difficulty accessing because of the bureaucratic hurdles. They are intimidated by all of the red tape in getting a contract. Then when they have the additional burden that they can't get the classified contract until they have a cleared facility, that they can't get the cleared facility until they have a classified contract——

This requires a working relationship that is not easy to create. Where you have to have the government agency saying, gee, I would like this small business to work for me. Therefore, won't you give them a security clearance?

I don't know the proper procedure for developing a work around this. I know we have to have classified facilities, cleared facilities. I know that. But, right now, we are having great difficulty getting access to a lot of really important technology in the small business world because of this difficulty.

What are the recommendations and how do we get there?

Ms. CALVARESI BARR. Representative Bartlett, I would like to make a comment based upon your question.

We also raised sort of on our high-risk list the need for the Department of Defense to recognize what are the key technologies and what is critical to the U.S. in order to maintain military superiority. We have done some work looking at how well informed we are about knowing what is militarily critical, where do those technologies reside. Oftentimes, as you say, some of the more innovative technologies and research and development resides at some of the smaller companies that are more innovative.

What we call for is that the Department of Defense sort of take stock of what is needed, what is critical, where does it reside, and then look at all of the programs and policies that we have in place that bring these needed technologies to the forefront and look to see what are the barriers, what are the challenges. This needs to be a constant relook and re-examination. Because, as we know, businesses continue to grow. There is rapid advancements in technology. So it calls for that kind of continual oversight on behalf of industrial policy to recognize where we need to go and how well equipped those entities are to overcome some of the obstacles and barriers that you spoke about.

Mr. BARTLETT. Mr. Chairman, we have common cause with our Small Business Committee in desiring more access to the skills and resources of the small business community, and I would suggest it might be productive to collaborate with them in seeing how we can work around this, obviously, catch-22 kind of a problem that we have.

Thank you very much. I yield back.

Mr. ORTIZ. Thank you.

Mrs. Boyda.

Mrs. BOYDA. Thank you so much, Mr. Chairman, for calling this hearing.

Thank you all for your service.

I represent Kansas, so there is a little issue about a contract going to Airbus as opposed to Boeing. Knowing it is certainly a complicated issue, but clearly I get asked on a regular basis not about so much why are we outsourcing our jobs, it is why are we outsourcing our national security.

What role do you all play or do you play any role when it comes to those contracts? Are you consulted on that? Do you weigh in on how well these people have done in the past or what their expectation is? What role do you play in the contracting process?

Ms. WATSON. I would say we play a minor role, but it is important. Any company that currently has a classified contract that is under the oversight of DSS gets a facility security rating every year after we do an inspection. We notify the government contracting activities of those ratings. So they are aware of how well we assess the company is postured to protect classified in their hands.

Mrs. BOYDA. Would you happen to know on the Airbus contract, what we have finally called the Boeing contract in Kansas, do you know if they already had a security clearance?

Ms. WATSON. I don't know.

Mrs. BOYDA. Could I just ask for the record just some background? Is it publicly available on what that was, what the standing was? Was it part of your contracting?

Ms. WATSON. Just for the record, DSS does not get involved in the contributing process itself.

Mrs. BOYDA. Okay. My follow-up question would be to you or to any of you on the panel. Because the issue of outsourcing our national security, clearly. This was about jobs. But it is not just about jobs. It is about outsourcing our national security. What would you have me tell the good people of Kansas when they ask me what are we doing to safeguard that national security?

From what I have heard today, we have had our fair share of challenges in this area, and we are doing better. As you have said, we are going to be in transition for quite a while. What am I supposed to tell them about the security of our secrets and our classified information?

Ms. WATSON. I think we have the proper framework in place to provide the security that we need. Any company that has access to classified information needs a facility security clearance. In order to get that, their key management personnel need a personnel security clearance. Usually, that is the head of the company. The facility security officer needs a security clearance, and so does anyone

in that company that has access to classified information. So that is the general framework.

There is another comment I want to make about FOCI companies, to put this in perspective. FOCI companies come to us in two ways. One is a new company that is already under FOCI is seeking access to classified and needs a facility security clearance. So during the course of processing that company for the clearance, we understand what the foreign ownership control or influence is in it.

There was a question earlier about hedge funds. We do not approve companies for access to classified unless we understand completely the ownership chain. So there is some transparency there.

The second class of cases are companies that already have facilities security clearances that are then—there is a foreign interest that acquires part of the business or there is a control element that comes into play. That is when there would be a material change that they need to report to us.

There have been lags in reporting. But, again, the facilities security officers, if they are doing their jobs—and we train them on how to do their jobs—report to us information like that on a routine basis.

Mrs. BOYDA. I am going to run out of time, but thank you.

If you would again, for the record, give me some background about what the status of Airbus was, if they were already in the category and they already have some of the clearances, you have already done some of your inspections on that. I appreciate that.

[The information referred to can be found in the Appendix on page 77.]

Mrs. BOYDA. Again, it is very concerning to hear that we have left this very important process pretty unfunded and without what they need to get the job done. So it is a little concerning. Actually, it is very, very concerning. I appreciate the work that you are doing to clear it up.

Thank you. I yield back.

Mr. ORTIZ. Mr. Thornberry.

Mr. THORNBERRY. Thank you, Mr. Chairman.

Thank you all for being here.

I start out with a statement in Dr. Schneider's testimony that says, "Globalization of technology is no longer a choice. It is a characteristic of the environment." I am afraid that some people haven't quite realized that there is no going back. The question is, how are we going to deal with this environment that we are in? And that means we have got to sort out the good from the bad and avoid knee-jerk reactions, which I think we have seen in some past cases.

In my mind, I kind of differentiate two sets of issues, one, what we are looking for, what are the standards; and the second one is the enforcement of those standards.

Dr. Schneider, you were asked by Dr. Snyder a little bit earlier about the hedge funds and those kind of ownership standards. But I notice in your testimony you talk about the key thing we want to protect is the software algorithms that make the hardware effective and work. I think about how much software is off the shelf, comes from potentially other countries, software providers that may not be a part of the systems we are talking about here at all; and the concern I have is that we are not asking the right ques-

tions, that maybe we are not looking in all the places that we ought to look.

It even reminds me of the debate we are having now about financial institution regulation, which has not kept up with the changes in global markets. Isn't that true for technology as well?

Dr. SCHNEIDER. Yes, I think that is a generally accurate statement.

The defense establishment, for example, depends on computers. Computers use microprocessors. The software for those is largely produced in a globalized environment. Indeed, the nature of the industry is such that very little of this element of the business is actually created in the defense sector.

What the defense sector does is take that information and in a classified environment create these algorithms so that a microprocessor that you might buy from a north shore supplier is then put into a system in such a way that it performs a military task.

What is vital to us is to be able to protect the knowledge about those algorithms. The fact that it uses a commercial microprocessor illustrates the fact that the underlying technology is not, per se, the sensitive part of it. It is though algorithms that really create the military capabilities that we need to protect.

So I think what the Department of Defense has been trying to do is to get some of both worlds, have a very successful industrial security program that protects these algorithms in the example I gave, while being able to take advantage of the technical advances that exists in the globalized market.

The Defense Science Board did two recent studies dealing with the problem you mentioned. One is, how do we produce mission-critical software in a secure environment? The other one was basically the same question with respect to microprocessors and hardware that is used in information systems. It is a very challenging problem to be able to deal with it and one that I think may interest this committee.

Mr. THORNBERRY. Definitely.

Ms. Watson, who sets the standards that you go enforce? It is not clear to me if, say, we want to have a different standard or look at different questions, who decides that?

Ms. WATSON. Right now, I would tell you that it is a policy matter and that DSS provides input into the policy.

Mr. THORNBERRY. Who is the decider?

Ms. WATSON. The Security Directorate.

Mr. THORNBERRY. That is?

Ms. WATSON. Mr. Torres at the end of the table.

Mr. THORNBERRY. So it is up to Mr. Torres to say, yes, we are going to look for that because that matters or, no, we are not going to look for that.

Mr. TORRES. If I may interject here, the Security Directorate is responsible for publishing and staffing the policy with regard to two particular documents. One is the NISPOM. But the NISPOM, which is the overarching document that dictates what we are going to do from a security perspective, also has other signatories to it, including Energy, Nuclear Regulatory Commission (NRC) and CIA. So we cannot unilaterally decide what the standards will be on the NISPOM.

On the Industrial Security Regulation, which is the old document that we are now getting ready to restaff, although we do coordinate that with all the interested parties, we have more say in that particular document and we work closely with Defense Security Service because their input—they are the ones on the front lines telling us what is working and what is not, and we depend heavily on them to tell us what needs to be changed, as well as working with the National Industrial Security Program Advisor Committee (NISPAC), which is also an oversight group for industry.

Ms. WATSON. May I comment on that as well?

Mr. ORTIZ. Go right ahead.

Ms. WATSON. One of the things I mentioned in my oral statement is we are contracting out of DSS for the FOCI process. We are going to have people look at the forms that are filled out to make sure we are asking the right questions. So we will feed that into the policy.

But there is a gray area between the overarching policy and then how we implement it. We do have liberty at DSS in terms of how we are going to implement that policy. If we think there are things we need to look at in a company, we will look at them.

Mr. ORTIZ. Thank you, ma'am.

Mr. Sestak.

Mr. SESTAK. Thanks, Mr. Chairman.

First of all, Ms. Watson and the others, for the civilian employees over there in DOD, we often commend the military when they come up before us for their great service. And having served 31 years in the military and worked alongside a lot of civilians over there, given the resources, you are equally great. It really is a total force over there.

My question is—and this may have been asked because I have been in and out, and I am sorry about that. There is a primary in Pennsylvania debate tonight, and I'm——

Under the NISPOM, the FOCI chapter section of it—and if this has been asked, I apologize—there is an annual review, and an annual certification that is done. Who reads those? Who do they go to? How high up the chain of command? And do they or should they come to Congress?

That last one was for excitement.

Ms. WATSON. We do review the companies annually. We provide a security rating to the company.

Mr. SESTAK. Who reads them above you?

Ms. WATSON. Well, any government contracting activity——

Mr. SESTAK. I mean within the Department of Defense, within the government. Does the Secretary of Defense get a brief on how well we are doing this?

Ms. WATSON. No.

Mr. SESTAK. Sometimes, at least, my thing is, expect what you inspect. Shouldn't we be passing these up further the chain?

Ms. WATSON. They are passed up the chain.

Mr. SESTAK. Who gets them? That is what I am trying to get to.

Ms. WATSON. I understand that. I am trying to answer this.

Say if a company had a classified contract with the Army, the Army is the government contracting activity. We would provide our report and our findings to the Army. So it is their classified infor-

mation at risk, not DSS's. So they understand what the security posture is of the company within their contract.

Mr. SESTAK. So it gets passed to somebody in the Army.

Ms. WATSON. Yes. If the company had 12 contracts with 12 different entities, they would all get that.

Mr. SESTAK. My next question is, if it doesn't all come together, are you unable to tell us what the trend analysis is? In other words, what are the violations that are occurring that we are able, with this nice centralized data, being able to say that is a recurring problem. Do we do that?

Ms. WATSON. We are struggling with trends analysis, particularly in the FOCI world. We do have a counterintelligence element in the industrial security program. It is an integrated part of that program. They publish a document annually generally called Technology Trends. We have a classified and unclassified version.

So the basis for that report is we educate the facility security officers and the folks in industry. We gave over 1,000 briefings to industry last year.

Mr. SESTAK. I only have a few moments, because they always take away an extra minute from a freshman. I have one more question. I am going to ask you to answer this. The question I would like also, if there is time, are you able to tell in this trend analysis where technology is going?

Ms. WATSON. Yes.

Mr. SESTAK. Good. Those reports go to whom?

Ms. WATSON. That document is available in an unclassified and classified version. We do send it out to industry so that they understand what the threats are that they are dealing with.

Mr. SESTAK. Does it go above you?

Ms. WATSON. It is disseminated throughout the Department, yes, sir.

Ms. CALVARESI BARR. Yes, I just wanted to comment that the questions that you asked are where we saw some key vulnerabilities. One is that the overall performance ratings at the facilities were not being fed up to DSS headquarters so that they could do the kind of trend analysis that you pointed to: numbers of security violations, by what corporate affiliation, for what kind of data, which government customers or agencies were affected.

We raised this pretty significantly in the reports that GAO did so that you could do the trend analysis, target where there were problems, and put corrective actions in place.

Mr. SESTAK. Could you see there would be value if this report was required to go up further the chain of command or come to Congress or anything?

Ms. CALVARESI BARR. Well, I think holding folks accountable for their role and their mission needs leadership, and you need leadership at the top. It needs to be a priority. So you need to have those that are concerned about it, looking at it, asking questions and putting the right things in place.

To the extent that that is happening, I think we have great leadership here now at DSS. Kathy has done just an amazing job since GAO has looked at really trying to get her arms around this and address it. But I think the support going up the chain could be further advanced.

Mr. SESTAK. Mr. Chairman, really, the question sometimes, if it does go up the chain of command, it can actually get her support.

Thank you very much.

Mr. ORTIZ. Thank you.

The gentleman from Texas, Mr. Conaway.

Mr. CONAWAY. Thank you, Mr. Chairman. I appreciate that.

We have had some discussions about ownership of companies. Have we had instances where the owner of a company breached the agreement, the classified agreement within the company, and took access to classified data that it shouldn't have? Has there been a problem with ownership in terms of violations?

Okay. I actually have a copy of the last Technology Trends. The biggest trend is they simply ask for the information.

Ms. WATSON. Yes, sir.

Mr. CONAWAY. How successful are they at asking and getting classified information by just asking?

Ms. WATSON. I think they are fairly successful, and it wouldn't just be classified information.

Mr. CONAWAY. I think this is just for classified information. The most successful intelligence-gathering facility—about classified information is people just ask the folks who have it, and they give it to them?

Ms. WATSON. The reason we know that is because the companies are reporting that back.

Mr. CONAWAY. Those are the attempts. How successful are those attempts at getting classified information? We know that, say, 50 percent of the attempts were just simply asking for it. The company said that looks like a probe of some sort, and they stopped it. Can we tell if they are successful one percent of the time at getting classified information?

Ms. WATSON. I can't give you a percentage. What I can tell you is when the companies report that information back to us, we don't just hold it at DSS. We disseminate it across the counterintelligence and law enforcement community. The number of suspicious contacts reports we are receiving in the last couple of years has exploded.

Mr. CONAWAY. This is 2004 data. When will we get the new one?

Ms. WATSON. We are aiming for this fall. We have changed the methodology we use to prepare and coordinate that document. It will be coordinated within DSS and throughout the community.

In terms of dissemination of the document, I do want to note that it goes to the National Counterintelligence Executive, and they incorporate much of our annual report in their annual report to Congress on espionage.

Mr. CONAWAY. But in terms of your dealing with the companies—and I will get the phraseology wrong. In terms of the cleared, or whatever you call it, you have got an individual who has a security clearance appropriate for the level of classified information that they have——

Ms. WATSON. Yes.

Mr. CONAWAY [continuing]. And that is our basic last line of defense, is that person watching how the program works within the company, making sure that new employees don't just come tricky-

trotting in and get access to it, to the information. That is the person that you work the most with?

Ms. WATSON. The facility security officer, yes, sir.

Mr. CONAWAY. Okay. How good are they?

Ms. WATSON. They are very good. They are trained. They are well compensated in industry. They have robust programs. We have a robust relationship with them.

Most of the bigger companies have annual conferences with all their facilities security officers. We are invited to participate in them. We have ample opportunity to do so.

Mr. CONAWAY. We had a suggested violation from a hedge fund, sub-owner in a hedge fund that we talked about this morning. Any instances where one of the facility security officers has said, you know, a hedge fund bought 10 percent of the company and some minion from the hedge fund came tricky-trotting in here one day and asked to see classified information?

You better say no.

Ms. WATSON. The general comment—I wouldn't know that it would be from a hedge fund, but certainly we have seen instances where the foreign ownership interest is represented with visitors and they do try to seek access. That is one of the guards that are in place in the company.

Mr. CONAWAY. Okay. But the security—facility security officer would know that that is a risk that he or she should be on guard for.

Ms. WATSON. Absolutely.

Mr. CONAWAY. Have we had instances where the new owners attempted to bully that officer into doing something he or she knows that is not right? Where that new owner has feared or tried to replace someone in a position that was not letting them get access?

Ms. WATSON. I cannot today speak to a specific instance that comes to mind. But in a situation like that the government security committee, the outside directors, if you will, are in a position to monitor that type of activity as well.

Mr. CONAWAY. Protect them from undue influence.

Ms. WATSON. Yes.

Mr. CONAWAY. Thank you, Mr. Chairman. I yield back. Looking forward to getting this new report.

The CHAIRMAN [presiding]. The gentlelady from California, Ms. Davis.

Mrs. DAVIS OF CALIFORNIA. Thank you, Mr. Chairman.

Thank you to all of you for being here.

I wonder if you can clarify for me the role of the National Security Council (NSC). Mr. Thornberry mentioned the number of agencies that are involved. I am trying to get a handle on whether that is policy alone and if in fact you believe that perhaps there should even be a greater role. Could you describe that for me? Is that Mr. Torres?

Mr. TORRES. The role in the National Security Council, as it is with most security policy, is that from an oversight perspective. So most of the policy is not written there unless there is some reason for that level to decide that things are not working the way they should and take affirmative action. So it is an oversight role, but most of the policy is developed at a lower level with the national

security program, with us as the lead, the executive agency with the Information Security Oversight Office (ISOO). Of course, that would be coordinated up through the National Security Council to make sure that they are in agreement with what the policy will be.

Mrs. DAVIS OF CALIFORNIA. There have been a number of comments made basically that the agency was broken across the board, and you said that they might be dealing at the lower level with policy, but it should be going up the board if anything is going poorly. Were they playing a role?

Mr. TORRES. I can't comment as to whether they were involved previously, but I can tell you that at this point there really is not a need for their involvement. Because, as we stated previously, Defense Security Service now, in our opinion, has leadership that is needed to get this right. The working relationship between Defense Security Service, the Security Directorate, counterintelligence security, the GAO, I think is going very, very well.

I don't think that there is any need to push anything further, because we really need to, as the folks with boots on the ground at Security Defense Service, need tell us what is really needed, and they are actually doing that.

Mrs. DAVIS OF CALIFORNIA. Can I ask you, Ms. Watson, would it be helpful to have them feel like a stronger partner in this at all? Or basically you don't need that kind of oversight or coordination?

Ms. WATSON. I think there is a partnership here, and there is a role for everyone to play. The NSC is involved at a very top level.

More importantly is the role of the ISOO in developing policy here. The ISOO, Information Security Oversight Office, from National Archives Records Administration plays a role here, as does a group called the NISPAC. It is another acronym. That is the industry group that participates as well in the oversight and policymaking element here.

That group, the NISPAC, has a meeting semiannually. It is sponsored by ISOO. It has participation from all 23 government agencies that participate in the National Industrial Security Program and from DSS as well.

Mrs. DAVIS OF CALIFORNIA. But the final accountability, and I think you covered this earlier, but the final accountability is where?

Ms. WATSON. The accountability in terms of policy?

Mrs. DAVIS OF CALIFORNIA. Overall, yes.

Mr. SULLIVAN. Ma'am, according to the executive order that established the National Industrial Security Program, the NSC has overall responsibility for policy. The Information Security Oversight Office implemented the program on behalf of the NSC and establishes the committee that Kathy mentioned, which is an entity established to address major policy issues, the coordination of the information that goes into the operating manual. So I think the answer to your question by the executive order is the NSC for policy matters.

Mrs. DAVIS OF CALIFORNIA. And to the GAO, in your report did you locate that as the center of accountability or responsibility?

Ms. CALVARESI BARR. We really just focused on DSS and national industrial security and what was happening on the ground to even first identify that a risk occurred and then the timing of putting

protective measures. So we didn't really do the review looking at is the right accountability change. We just wanted to know whether they were doing their job as their mission called for in the first place, and our recommendations were directed in line with that.

Mrs. DAVIS OF CALIFORNIA. Thank you. I know that you mentioned earlier the importance of the accountability piece. I just wanted to be sure I understood that.

Ms. CALVARESI BARR. It is important. It is important in any program, particularly programs that are protecting critical technologies.

Mrs. DAVIS OF CALIFORNIA. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you very much.

The gentleman from Missouri, Mr. Akin.

Mr. AKIN. Thank you, Mr. Chairman.

A couple of different questions. The first is, my understanding is that there were 16 points that you made recommendations on. Two have been fully implemented, which suggests that there are 14 still being worked on. What is the status of the 14 other points?

Ms. WATSON. I can't answer that one by one. I will tell you we are a work in progress. We have taken all of the recommendations of GAO to heart, and we are addressing all of them in our implementation plan. It will take time.

I have got a very small cadre of folks who do this work right now, and they need training. We are getting them the training. We are trying to get people in the door at the same time and make our oversight program much more robust.

Mr. AKIN. So are you actually plussing up the number of employees, so you are actively building an organization at this time?

Ms. WATSON. We are. When I arrived at DSS not only were we understaffed but we had 80 vacancies and there was a hiring freeze in place due to lack of resources. The hiring freeze has been lifted, so we are trying to recover from the 80 vacancies we already had, as well as hire an additional 145 new employees. It takes time. They all need clearances.

Mr. AKIN. When each of us was first elected to Congress, we came down here and they told us you have got a week or two to hire an entire office. In the business world, somebody leaves and you replace them with somebody. But when you are going to try to create an organization overnight, I understand what you are saying.

Ms. WATSON. We don't do all of our hiring. We have to work through the Department. We are dependent on other offices in the Department for our hiring actions.

Mr. AKIN. So you can't hire the people you want to run your organization?

Ms. WATSON. There are challenges in the hiring process.

Mr. AKIN. Sounds like you have got the other arm tied behind your back, too.

I guess the question I have heard in terms of intelligence, that we have a gap where there is pure research, where the pure research then starts to get reported, that the Chinese can come and basically harvest anything they want, and there is some sort of a time period before there is a patent or something else that begins

to protect it. Is there some kind of gap from the time of pure research discovery in a lab somewhere along the line where people can just come in and basically help themselves to our information?

Mr. SULLIVAN. Sir, I am not a scientist, by any means, but I do know there is a document, National Security Defense Directive (NSDD) 189, that establishes the definition and parameters of basically research, essentially, in that it states basic research is generally not classified, at least within the Department, until you move down the spectrum of these different categories of research and get to something called fundamental research. Then you start getting into the classified area.

So in that arena of basic research there is all kinds of exchanges of information, publishing of research, interaction with people around the world to encourage scientists to, in fact, produce better products.

Mr. AKIN. My question is, do we have a gap somewhere in there where people can pick off a lot of our research, where we should be classifying things or protecting information?

Mr. SULLIVAN. I would have to defer to the people who own the technologies and are sponsoring the research. It would seem that there is an awful great potential for our adversaries to focus in the area of basic research to get information. But as to what we are losing or what there is to lose, that would be beyond our area of expertise.

Mr. AKIN. Who is in charge of that and who should know the answer to that question?

Mr. SULLIVAN. I would refer—at least at the Office of Secretary of Defense, it would be the Office of the Under Secretary of Defense for Acquisition Technology and Logistics, AT&L.

Mr. AKIN. They should know that. Doesn't sound like there is any one point person that is in charge of protecting our information security in terms of—is that true? That is kind of what I am sensing.

Ms. CALVARESI BARR. Let me just comment that we had mentioned a number of programs and policies that are designed to protect not only the systems, the components, the know-how, and the information. And I think on some of the basic research areas that you talked about, particularly with regards to export controls, the export control system is supposed to recognize, when we do have sensitive information, licenses are required for that. So that would be the role of State Department, looking over those things that are sensitive and have military application, and then Commerce Department, in terms of its licensing for dual use. We found major vulnerabilities in both of those programs.

Mr. AKIN. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you very much.

We are going to try to finish the hearing here shortly, because we have a series of four votes.

Mr. Taylor—and if there are other comments, I am sure we can get them in. Mr. Taylor.

Mr. TAYLOR. Thank you, Mr. Chairman.

I want to thank the panel for being here.

And I apologize for being late. There were some things going on at the White House this morning.

The Hughes-Loral deal strikes me as probably the poster child of "greed gone wild" in this town. I distinctly remember a member of the California delegation walking the floor, seeking people's signatures, saying it would be okay for the Loral Company to take some satellites over to China because there were huge profits to be made by sending satellites into space. And I remember not signing it, saying, "That just gives me heartburn. I can see all sorts of bad things coming from this, even with my lack of technical knowledge. I just don't think that is a good idea." Well, it was amazing that apparently your office signed off on the deal.

And I distinctly remember one employee sending a, what, 60-something-page fax out in the clear, explaining to the Chinese, in effect, kicker technology for launching multiple satellites. What has happened since then to keep that from happening again?

And do things like the European Aeronautic Defense and Space Company (EADS) successful bid on the tanker create more opportunities for mischief like that?

And I will just give you an example. Let's say, as an unintended consequence of refuelling an F–22, we discover that something on the tanker is jamming the fuel pumps on the F–22, some sort of a signal. So word gets back to the parent company, when you are fueling an F–22, you can't broadcast in this frequency because you shut off his fuel pumps, because so much of that is done by electronics now. How do we keep EADS or someone like EADS from not going to a potential enemy of the United States and saying, you know, "For X number of dollars, I will expose you to a vulnerability. Of course, then I am going to turn around to the United States Air Force and sell them a fix"?

To what extent do you get involved in things like that? Because the Hughes-Loral deal happened. It did. Regrettably, it happened. So what steps are being taken so that doesn't happen again and that the scenario that I just outlined doesn't happen as well?

Ms. CALVARESI BARR. I would just comment that it calls to the heart of these programs, such as industrial security and others, export controls and foreign military sales, all of that working as effectively as it can.

And I think, just with regard to the protections that need to be in place, you need to know what alliances you are building, you need to know what companies you are partnering with.

And I would even say, in the case of, as you said, the EADS deal, just because we would go with the U.S. company, it wouldn't necessarily preclude us from foreign ownership or influence, because, as we know, many of these large companies are going to have affiliations. So all the more reason for programs like Industrial Security and others to be effective.

Mr. TAYLOR. Walk me and the average American through why that does not somehow become the proprietary knowledge of an EADS or any other firm, that broadcasting in a certain frequency is going to shut down the fuel pumps.

I am just giving an analogy, because we have discovered a number of unintended consequences with our jammers in Iraq. And

that is what leads me to say this, and I don't need to go any further than that.

So let us just say a unintended consequence is to shut down the fuel pumps on an F–22 if you broadcast at a certain frequency; it suddenly becomes the information of EADS—or, heck, that is their company. They are an international aerospace firm in the business of selling information and technology.

So where do you step in and prevent that from happening?

Ms. CALVARESI BARR. There are programs in place in which we have agreements with other host governments that trickle down to—flow down to the contractors in the company that is supposed to say that we are supposed to protect certain of our classified information by the same standards as the U.S.

We haven't done any recent work looking at how well those programs are working, how current they are.

Mr. TAYLOR. If I may ask, why not? Because that strikes me as a very real vulnerability.

Ms. CALVARESI BARR. Well, GAO usually does work on the behalf of Congress, and we haven't had a request specifically aimed looking at some of those agreements for quite some time.

Mr. TAYLOR. Well, could I ask Dr. Schneider then?

And, again, let's use the very real analogy of the jammers in Iraq and the unintended consequences that they have. I don't need to go into further detail. But let's just say that jammer happened to have been made by a foreign firm. What is to keep them from turning around to the Iraqis or the Iranians or any number of potential foes and saying, "Oh, by the way, if you can broadcast a signal in this frequency, you can keep the Americans from talking to each other."

Dr. SCHNEIDER. In general, if there is classified information to that effect, that would only be in the hands of a U.S. citizen. If the U.S. citizen transferred it to someone who is not cleared and didn't have a need to know, that would be a violation of law, and they would be vulnerable to prosecution, whether or not there was a commercial relationship or not.

And I think the question that you had raised earlier about the effectiveness of circumstances where we do share classified information with allied countries is something that is undoubtedly worth knowing about and staying on top of it.

But my impression is that the rules on the protection of classified information bear on all of the holders who are U.S. citizens, and they have obligations which anyone who holds a security clearance knows, that they are not allowed to transfer classified information to anyone who does not have a security clearance and a need to know that information.

The CHAIRMAN. I think the gentleman has an excellent line of inquiry, but we have a vote.

Mr. SAXTON. May I just ask a couple of questions for the record?

The CHAIRMAN. Real quick.

Mr. SAXTON. We are flat out of time, as the Chairman said. I have two questions for Ms. Watson and Ms. Calvaresi Barr. Would you be able to respond in writing? Because we are going to have to go.

The first question is, recognizing that the information we have indicates that you have 647 FOCI cases, I am not clear on precisely what an FOCI case is, and if you could each clarify that for us.

And the second question is, because of the nature of the reporting requirements, which I have characterized as self-reporting—that may or may not be a good characterization—how much are we missing because of the current reporting process? And do we need to make modifications in the reporting process in order to help us get a better picture of what it is that we are after in the reporting process?

If you could get that back to us in short order, we would really appreciate it.

Thank you.

The CHAIRMAN. With that, we thank the gentleman.

And I certainly appreciate your being with us today. It has just been excellent.

And we are adjourned.

[Whereupon, at 12:06 p.m., the committee was adjourned.]

A P P E N D I X

APRIL 16, 2008

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

APRIL 16, 2008

STATEMENT OF

MR. TROY SULLIVAN,
ACTING DEPUTY UNDER SECRETARY FOR DEFENSE FOR
COUNTERINTELLIGENCE AND SECURITY

AND

MS. KATHY WATSON
DIRECTOR, DEFENSE SECURITY SERVICE

ON THE

NATIONAL INDUSTRIAL SECURITY PROGRAM

HOUSE COMMITTEE ON ARMED SERVICES

APRIL 16, 2008

Introduction:

Good morning Mr. Chairman and members of the Committee. I am Troy Sullivan, the Acting Deputy Under Secretary of Defense for Counterintelligence and Security, responsible for security policy across the Department of Defense. I am pleased to appear before you today to address how the Department is adapting the National Industrial Security Program (NISP) to the globalization of the defense industry.

I am joined by Ms. Kathleen Watson, Director of the Defense Security Service (DSS). We will briefly discuss implementation of the NISP and the role DSS plays.

Background:

The NISP was established by Executive Order 12829 to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. The Information Security Oversight Office, of the National Archives and Records Administration, is responsible for implementing and monitoring the NISP. The Department of Defense is the Executive Agent for inspecting and monitoring contractors, licensees, and grantees under the NISP and for determining their eligibility for access to classified information. DSS administers the NISP on behalf of the Department and 23 other Federal agencies within the Executive Branch.

Standardized policy is critical to the success of the program. 32 C.F.R. Part 2004, "National Industrial Security Program Directive No. 1" (Mar 2006) implements E.O. 12829, as amended, and is binding on all executive branch agencies. The Industrial Security Regulation (ISR), DoD 5220.22-R (Dec 1985), provides policy and guidance to government activities, to include DSS. The Department is also responsible for writing and coordinating the National Industrial Security Program Operating Manual (NISPOM),

DoD 5220.22-M, (Feb 2006), which conveys policy and guidance to industry in connection with performance on classified contracts under the NISP.

There are approximately 8,710 legal entities (e.g., corporations, Limited Liability Companies, partnerships, and sole proprietorships) with over 12,000 facilities that are cleared for access to classified information. To have access to U.S. classified information and participate in the NISP, a contractor facility must have a bona fide procurement requirement for access to classified information. Once this requirement has been established, a facility is eligible for a Facility Security Clearance. A Facility Security Clearance is an administrative determination, made by DSS, that a contractor facility is eligible to access classified information at the same or lower classification category as the clearance being granted. The Facility Security Clearance may be granted at the Top Secret, Secret or Confidential level.

As part of the facility clearance process, DSS clears key management personnel (e.g., President/Chief Executive Officer, Chairman of the Board, and facility security officer), and evaluates Foreign Ownership Control or Influence (FOCI), based on the contractor's Certificate Pertaining to Foreign Interests. In order to obtain the clearance, the contractor must execute a Department of Defense Security Agreement, which is a legally binding document that sets forth the responsibilities of both parties and obligates the contractor to abide by the security requirements of the NISPOM.

In addition, the Federal Acquisition Regulation (FAR) requires government contracting activities to insert a standard clause, when a contract requires contractor personnel to have access to classified information. This clause also requires the contractor to adhere to the NISPOM. The NISPOM provides security requirements, policy and guidance to contractors.

Once a facility is cleared, DSS has oversight authority to evaluate the security operations of the organization. During these visits, DSS Industrial Security

Representatives will interview employees, review the facility clearance documentation, examine classified contract requirements and security files, review the facility's security education program and provide guidance as needed, inspect classified storage/physical security, inspect classified holdings (to include inventory/disposition, reproduction procedures and destruction procedures), and inspect accredited information systems.

In fiscal year (FY) 2007 DSS conducted 8,812 inspections, which is a slight increase from FY 2006. We forecast conducting approximately the same number of inspections this year.

The Federal Government allows foreign investment consistent with the national security interest of the United States. However, a company that is determined to be under FOCI is not eligible for a facility clearance or to participate in the NISP, until the FOCI has been mitigated.

As defined by the NISPOM, a company is considered to be operating under FOCI whenever a foreign interest has the power, direct or indirect (whether or not exercised and whether or not exercisable), to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts (i.e., contracts requiring contractor personnel to have access to classified information).

DSS adjudicates FOCI factors of cleared contractors participating in the NISP. For new facilities, DSS accomplishes this during the facility clearance process. When a company with a facility security clearance enters into negotiations for the proposed merger, acquisition, or takeover by a foreign interest, the NISPOM requires the contractor to notify DSS of the commencement of such negotiations. The notification shall include the type of transaction under negotiation (stock purchase, asset purchase, etc.), the identity of the potential foreign investor, and a plan to mitigate/negate the FOCI.

Companies should also advise DSS if the parties to the proposed transaction will be filing with the Committee on Foreign Investment in the United States (CFIUS). CFIUS and FOCI are parallel, but separate processes.

The FOCI mitigation mechanisms defined in the NISPOM are Voting Trust Agreement, Proxy Agreement, Special Security Agreement, Security Control Agreement, and Board Resolution.

- A Board Resolution, the least intrusive and most common mitigation mechanism, is used when the foreign entity does not own voting stock sufficient to elect a representative to the company's governing board.
- A Security Control Agreement (SCA) is used when the cleared company is not effectively owned or controlled by a foreign entity and the foreign interest is entitled to representation on the company's governing board.
- A Special Security Agreement (SSA) is the second most common FOCI mitigation mechanism. An SSA is used when a company is effectively owned or controlled by a foreign entity. The SSA has access limitations and requires the establishment of a Government Security Committee, consisting of the company's cleared senior managers and U.S. citizens approved by the Federal Government (i.e., DSS). The Government Security Committee oversees security of classified and export controlled information. Access to proscribed information by a company cleared under a SSA may require that the Government Contracting Activity complete a National Interest Determination to show the release of proscribed information (TS, SCI, SAP, COMSEC or RD) to the company shall not harm the national security interest of the United States.
- Proxy Agreements (PA) and Voting Trust Agreements (VTA) are also used when a cleared company is owned or controlled by a foreign entity. The PA and VTA are substantially identical arrangements whereby the voting rights of the foreign owned stock are vested in cleared U.S. citizens approved by the

Federal Government (DSS). Neither arrangement imposes any restrictions on the company's eligibility to have access to classified information or to compete for classified contracts.

Of the 8,710 cleared legal entities under DSS Cognizance, 311 have FOCI mitigation agreements in place. DSS has seen a significant increase in the number of FOCI cases in the last 10 years.

DSS inspections or security reviews of FOCI companies are conducted much as any other review of a cleared facility. In addition to those areas of inspection noted earlier, DSS places special emphasis at FOCI companies on the firm's compliance with the FOCI agreement. One area of specific interest is the company's Technology Control Plan (TCP). These plans are approved by DSS, and prescribe security measures to reasonably foreclose the possibility of inadvertent access by non-U.S. citizen employees and visitors to information for which they are not authorized. DSS also assesses the firm's procedures for monitoring electronic communications between the cleared firm and foreign parent, interactions with representatives of the foreign parent and control of foreign visitors to ensure that classified or export controlled information (for which the foreign shareholder is not authorized) is not inadvertently released to the foreign parent or any of its affiliate companies.

In addition to the inspection, DSS also meets annually with the Government Security Committee (GSC) of firms cleared under the SCA, SSA and PA. During these meetings, DSS reviews the purpose and effectiveness of the FOCI mitigation agreement and establishes common understanding of the operating requirements and the firms' implementation of the agreement.

Policy Issues

Earlier I mentioned the importance of our two key policy documents, the ISR and the NISPOM. As one can imagine, producing a document that meets the needs of twenty-four organizations is a challenge. We have concerns about both issuances.

The ISR is 22 years old. Portions are out of date and in conflict with the newer NISPOM, and lack important and current guidance for classified information system security. We have a revised version that complements the NISPOM and will enter the coordination process later this month.

Two years ago, years of very intense work culminated in the publication of a new NISPOM. This was a great accomplishment as we collectively rewrote an 11 year old document. Based on two years of implementing the new NISPOM, the DSS director has identified several areas that she believes, if clarified or strengthened, would improve the effectiveness of her organization. These issues are being addressed in collaboration with the Office of the Under Secretary of Defense for Intelligence, Security Directorate, with the goal of ensuring DSS can accomplish its mission.

Three years ago, the Government Accountability Office (GAO) issued a critical report on the DSS execution of its FOCI mission and the Department's response to the GAO recommendations. Although the Department non-concurred with almost all of the recommendations, the current DSS director recognized areas within the FOCI program that needed improvement, and therefore made the FOCI process a high priority in the agency's Transformation Plan. The DSS leadership is keeping the GAO informed of their progress.

Finally, I would be remiss to overlook the tremendous improvements within DSS during the past year. Under the strong and aggressive leadership of Ms. Kathy Watson, DSS has spent the last year reviewing its entire agency – top to bottom. That effort resulted in a Transformation Plan that addresses critical problems across the agency,

including some of those I mentioned earlier in the Industrial Security Program. The Department approved all aspects of this Transformation Plan, and fully funded it and DSS in FY 2008 and in the FY 2009 President's Budget to ensure it can accomplish its critical mission in protecting the national security.

Conclusion:

The NISP is the cornerstone of our program within the Department of Defense to protect our leading edge research and technology from compromise. We take our community responsibility as the NISP Executive Agent very seriously. We understand that globalization and the active efforts of our friends and adversaries to acquire restricted technologies have not abated. The challenges for DSS have increased accordingly. The Honorable James Clapper, the Under Secretary of Defense for Intelligence, has committed to the transformation of DSS from the troubled agency of the recent past, to the more robust, fully-funded, and aggressive organization that it has become.

Mr. Chairman, this concludes my prepared remarks. We are ready to answer any questions you may have.

Testimony of
William Schneider, Jr.
Chairman, Defense Science Board
US Department of Defense

National Security Industrial Program: Implications of Globalization and Foreign Ownership and the Defense Industrial Base

April 16, 2008

Committee on the Armed Services
U.S. House of Representative
Washington, D.C.

Testimony of William Schneider, Jr., Chairman, Defense Science Board, US Department of Defense, Washington, D.C. before the Committee on the Armed Services, US House of Representatives, 16 April 08 on *THE NATIONAL INDUSTRIAL SECURITY PROGRAM: The Implications of Globalization and Foreign Ownership for the Defense Industrial Base.*[1]

MR. CHAIRMAN AND MEMBERS OF THE COMMITTEE:

I am William Schneider, Jr., Chairman of the Defense Science Board in the US Department of Defense, a Federal advisory committee. Thank you for offering me the privilege of testifying before this Committee on a subject of great importance to the Department of Defense.

Globalization and security

The impact of globalization on the Department of Defense and its mission has been an important aspect of DSB studies for more than a decade.[2] The globalization of technology is no longer a choice for governments planning to modernize their military forces; it is a characteristic of the environment in which military capabilities will be developed and produced for the foreseeable future.

Among the most pervasive factors responsible for the vast increase in international trade and investment since the end of the Cold War has been the deregulation of trade in advanced technology. The globalization of access to advanced technologies has meant that users as well as producers of modern technology are able to share access to a common global technology base and markets. This nearly universal access to advanced technology has accelerated its propagation, and has revolutionized the process of innovation in most technology-driven

[1] The views expressed here are solely those of the author and do not necessarily represent the view of the DSB, its members, or the US government.
[2] DSB reports can be found at http://www.acq.osd.mil/dsb/reports.htm.

industrial and service industries including the defense sector. Although legal and regulatory factors in the defense sector have slowed the impact of globalization on its R&D and acquisition processes compared to the private sector, the DoD too has succumbed to its technical, commercial, and industrial logic.

By exploiting the technologies created or enhanced by the process of globalization, the military capabilities fielded by the DoD have been swiftly transformed from its industrial age character that dominated its capabilities at the end of the Cold War. The process of transforming US military capabilities to highly adaptive information age capabilities appropriate to the 21st century threat environment it now employs is now at an advanced stage.

The globalization process has provided important cost, schedule, and performance benefits for the DoD and its defense industrial base. The underlying technologies which create the most decisive modern military capabilities are derived from developments in the civil technology sector. The highly competitive civil technology sector is thoroughly globalized. The pace of its development of technology is very rapid compared to technologies developed solely within the defense sector and are usually associated with both declining costs and increasing capabilities. The DoD has been very successful in applying the benefits of globalization to many of its critical mission areas. For example, the DoD has been able to place its C^4ISR (command-control-communications-computation-intelligence-surveillance-reconnaissance) network on a modernization path that permits US forces to adapt to rapid changes in the future military threat without necessarily needing to replace its platforms (e.g.

tactical aircraft, naval combatants, etc.) as would have been the case a generation ago as new threats emerged. Indeed, by connecting its C^4ISR system to networked platforms, the DoD has been able to perform its mission with far fewer personnel and platforms than would have been required a generation ago.

The unique skills of the defense industrial base provide the access to this global technology base. The defense industrial base adapts the technologies it draws from the global technology base to meet defense requirements using its specialized skills in system engineering and integration into superior military capabilities. It no longer needs to develop or "own" the underlying technologies to produce superior military capabilities, but it must protect the know-how that converted ubiquitous technologies into military capabilities.

The success the defense industry has enjoyed in its exploitation of the globalization of modern technology must be tempered with recognition of the risks and vulnerabilities created by this evolution in the manner in which military capabilities are created. Protecting America's military edge depends in part on the effectiveness of the national industrial security program.

The fact that an increasing fraction of the underlying technologies that are drawn upon by the defense industrial sector to create advanced military capabilities are developed in the civil sector, and in many cases are developed abroad changes the environment in which the industrial security program must operate. This is so because the core of the military capabilities we create resides not in the technology itself, but in the manner in which these "civil" technologies are converted

into military capabilities. The details of how the technologies are engineered into military systems, especially the software and algorithms used to render the "hardware" effective in its military applications, and the manner in which individual systems interact in a "system of systems" is at the heart of what the industrial base needs to protect from potential adversaries.

The effectiveness of the classification system is very important to protect these capabilities. In the past, an adversary could hope to exploit military equipment only if he got access to the equipment or manufacturing knowledge in some manner. Hence, protecting the physical security of the industrial base from adversary espionage was the most central dimension of industrial security. Today, many of the most decisive aspects of military technology can be compromised by merely putting the sensitive software and algorithmic information on a CD or DVD, hence the focus of industrial security now must incorporate both physical and information security to protect US military advantage. Doing so when much of the underlying technology is both unclassified as well as being developed and produced in the international market poses new challenges for the DoD's industrial security apparatus.

Foreign direct investment in the US defense sector

In the 1990's, the DoD recognized that it was becoming increasingly dependent on the globalization of the technology base. To increase the DoD's access to advanced technology, the DoD made some shrewd decisions in the 1990s that have been reinforced by subsequent decisions in recent years.

The Executive branch took two parallel paths improving its access to advanced technology on the international market. First, the US government sought to reform the process by which the DoD could procure defense products from producers abroad. The Executive branch sought to liberalize the defense trade processes during both the Clinton and the current Bush administrations. The key elements of the proposed process liberalization initiatives; the Clinton administrations *Defense Trade Security Initiative* in 2000, and the Bush administration's *NSPD-19* defense trade process reform initiative in 2002 were both rejected by the Congress, although some of the reforms were subsequently incorporated in US government practice administratively.

The other dimension of the reform process has been much more successful. In the early 1990s the DoD liberalized the process pertaining to the regulation of foreign investment in the defense sector. The policy change encouraged continued foreign investment in the defense sector, but did so by the DoDs embracing of a mitigation measure known as the Special Security agreement which mitigates the risks that the presence of a foreign investor might pose to the security of US classified and export controlled technology in the possession of a cleared US company. The mitigation process focused heavily on industrial security as established in the *National Industrial Security Program Operating Manual* (NISPOM). Under the NISPOM, to obtain or retain a US government facility security clearance at its US facilities, a foreign investor is required to implement changes in corporate governance, at the US-cleared companies to insulate the US companies against undue foreign influence, ensure that foreign ownership does not adversely affect the performance of classified

contracts, and protect classified and export controlled unclassified information. The procedures cover a range of options, depending on the level of foreign ownership control, or influence to include the Special Security Agreement.

Perhaps the most significant change wrought by the NISPOM is the effect on business practices for the US subsidiaries of foreign investors in the defense sector. Security of classified and export controlled information is a pre-occupation of the management of the US subsidiaries. There is a profound incentive for this to be so. The investor is critically dependent for its continued access to the US market on a very high level of compliance with US industrial security regulations for both classified information and US Department of State and Department of Commerce regulations regarding export controlled information.

The intense managerial focus on security compliance is facilitated by a unique DoD security innovation reflected in the NISPOM. As an element of the procedures foreign investors in the defense sector must put in place to mitigate the risk of foreign ownership, foreign majority controlled companies are normally required under a Special Security Agreement to appoint at least three non-executive outside directors to the Board of Directors of their US company who have not had any prior relationship with the cleared company, or the foreign owners and their affiliates. Those appointed must have current personnel security clearances at the level of the cleared company's DoD facility security clearances or be clearable under DoD personnel security clearance requirements and be approved by the Defense Security Service. They do serve as full members of the Board. At the same time, in addition

to the traditional fiduciary obligations of a Board member in a commercial firm, they also have obligations to the Defense Security Service for monitoring and assessing the security processes (including approval of visitors from the foreign owner (including its affiliates) to the US company). These outside directors, together with the US citizen officer-directors comprise a board-level Government Security Committee charged with ensuring proper implementation of the Special Security Agreement as well as ensuring that policies and procedures are in place to protect classified and export controlled information to the DoD and ITAR/EAR standards.

The mitigation process I have described is one with which I have considerable personal experience. For more than 15 years, I have served as an outside director on the US subsidiary of foreign domiciled firms operating in the US defense sector. My personal experience with the process is entirely satisfactory from the perspective of meeting the aims of the program. The security compliance – with both classified and export controlled information – is of a very high order reflecting the pre-occupation with security of the US managers of the subsidiaries. At the same time, the firms are adding value to the US defense program by bringing investment and advanced technology to the defense market that expands and strengthens the defense industrial base resident in the US.

The threats posed to the security of information for both foreign firms present in the US market as well as US firms – both classified and export controlled – is evolving. As I have noted, much of the underlying technology that drives the creation of advanced military capabilities is unclassified, and this information resides on computer

networks. These networks are now the focus of attacks by potential adversary states and non-state entities. The President's Cyber Security Initiative addresses a very important gap in the ability of the industrial base to protect its proprietary information. The industrial base – domestic or foreign owned – lacks the knowledge that only the US government possesses about how to protect their computer networks that are part of the larger national information infrastructure from foreign computer network exploitation and attack. The area of cyber security appears to be the domain in which the technology security of the defense industrial base is most at risk for both domestic and foreign owned firms operating in the US.

Mr. Chairman, I will be pleased to respond to any questions you or Members of the Committee may have.

United States Government Accountability Office

GAO

Testimony
Before the Committee on Armed Services, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, April 16, 2008

DEPARTMENT OF DEFENSE

Observations on the National Industrial Security Program

Statement of Ann Calvaresi Barr, Director
Acquisition and Sourcing Management

April 17, 2008

GAO
Accountability · Integrity · Reliability
Highlights

Highlights of GAO-08-636T, a testimony before the Ad Hoc Subcommittee on State, Local, and Private Sector Preparedness and Integration, Committee on Homeland Security and Governmental Affairs, U.S. Senate

HOMELAND SECURITY

Federal Efforts Are Helping to Address Some Challenges Faced by State and Local Fusion Centers

Why GAO Did This Study

Following the September 11 terrorist attacks, state and local governments formed fusion centers, collaborative efforts to detect, prevent, investigate, and respond to criminal or terrorist activity. Recognizing that the centers are a critical mechanism for sharing information, the federal government—including the Department of Homeland Security (DHS), Department of Justice (DOJ), and the Program Manager for the Information Sharing Environment (PM-ISE), which has primary responsibility for governmentwide information sharing—is taking steps to partner with fusion centers.

This testimony focuses on (1) the characteristics of fusion centers as of September 2007 and (2) federal efforts to help alleviate challenges centers identified. This testimony is based on GAO's October 2007 report on 58 fusion centers and related federal efforts to support them as well as updated information GAO obtained in March 2008 by reviewing plans describing selected federal efforts and attending the second annual national fusion center conference.

What GAO Recommends

While this testimony contains no new recommendations, GAO has recommended that the federal government define and articulate its long-term fusion center role and whether it expects to provide resources to help ensure their sustainability. PM-ISE agreed with the recommendation and is in the process of implementing it.

To view the full product, including the scope and methodology, click on GAO-08-636T. For more information, contact Eileen Larence at (202) 512-8777 or larencee@gao.gov.

What GAO Found

Almost all states and several local governments have established or are in the process of establishing fusion centers that vary in their characteristics. Centers were generally established to address gaps in information sharing, and the majority of the centers GAO contacted had adopted broad missions that could include both counterterrorism and law enforcement–related information. While law enforcement entities, such as state police, are the lead or managing agencies in the majority of the centers GAO contacted, the centers varied in their staff sizes and partnerships with other agencies. The majority of the operational fusion centers GAO contacted had federal personnel, including from DHS or the Federal Bureau of Investigation (FBI), assigned to them as of September 2007.

DHS and DOJ have several efforts under way that begin to address challenges fusion center officials identified.

- DHS and DOJ have provided many fusion centers access to their information systems, but fusion center officials cited challenges accessing and managing multiple information systems.
- Both DHS and the FBI have provided security clearances for state and local personnel and set timeliness goals for granting clearances. However, officials cited challenges obtaining and using clearances.
- DHS, DOJ, and the PM-ISE have also taken steps to develop guidance and provide technical assistance to fusion centers, for instance, by issuing guidelines for establishing and operating centers. However, officials at 21 centers cited challenges with the availability of training for mission-specific issues. DHS and DOJ have continued providing a technical assistance program for fusion centers and disseminated a baseline capabilities draft in March 2008 that outlines minimum operational standards for fusion centers. While this support and guidance is promising, it is too soon to determine the extent to which it will address challenges identified by officials contacted.
- Finally, officials in 43 of the 58 fusion centers contacted reported facing challenges related to obtaining personnel, and officials in 54 centers reported challenges with funding, some of which affected these centers' sustainability. To support fusion centers, both DHS and the FBI have assigned, and continue to assign, personnel to the centers. To help address funding issues, DHS has provided funding for fusion-center related activities.

The National Strategy for Information Sharing, issued in October 2007 by the President, states that the federal government will support the establishment of fusion centers and help sustain them through grant funding, technical assistance, and training. However, some fusion center officials raised concerns about how specifically the federal government was planning to assist state and local governments to sustain fusion centers as it works to incorporate fusion centers into the ISE and to implement the strategy.

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss our work on the National Industrial Security Program (NISP), which aims to ensure contractors adequately safeguard the government's classified information. The Defense Security Service (DSS) within the Department of Defense (DOD) administers NISP on behalf of DOD and other federal agencies. DSS grants clearances to contractor facilities so they can access and, in some cases, store classified information. In 2005, DSS monitored over 11,000 facilities' security programs to ensure that they met NISP requirements for protecting classified information. We have issued two reports that examined how DSS carried out its industrial security responsibilities. The first report assessed DSS oversight of contractor facilities and DSS actions after possible compromises of classified information. The second focused specifically on DSS oversight of contractors under foreign ownership, control, or influence (FOCI).[1]

Before I discuss our work on NISP, I would like to place the program in a larger context. NISP is just one element within a myriad of laws, regulations, policies, and processes intended to identify and protect technologies critical to maintaining U.S. technological superiority on the battlefield and to provide for the transfer of these technologies to foreign parties in a manner consistent with U.S. economic, foreign policy and national security interests. The government's other technology protection programs include export control regimes, national security reviews of foreign acquisitions of U.S. companies, the foreign military sales program, the national disclosure policy process, and DOD's anti-tamper policy. Over the past several years GAO has looked at each of these and identified weaknesses in their implementation. These weaknesses have been exacerbated by the increasingly globalized nature of the defense industrial base and the increased pace of technological innovation worldwide. As a result, in 2007, we designated the effective protection of technologies critical to U.S. national security interests as a governmentwide high-risk area, which warrants a strategic reexamination of existing programs to identify needed changes and better ensure the advancement of U.S. interests. I believe this hearing today contributes to that strategic reexamination.

[1]GAO, *Industrial Security: DOD Cannot Provide Adequate Assurances That Its Oversight Ensures the Protection of Classified Information*, GAO-04-332 (Washington, D.C.: Mar. 3, 2004), and *Industrial Security: DOD Cannot Ensure Its Oversight of Contractors under Foreign Influence Is Sufficient*, GAO-05-681 (Washington, D.C.: July 15, 2005).

This testimony is based on the cited reports, which were done in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Summary

Our work on DSS oversight of contractor facilities and DSS oversight of contractors under FOCI identified certain systemic weaknesses. In both areas DSS did not systematically collect and analyze information to assess the effectiveness of its operations. Such an assessment would have assisted DSS in better managing its processes and enabled it to identify problems and institute corrective actions. In terms of facility oversight, DSS maintained files on contractor facilities' security programs and their security violations, but it did not analyze this information to determine, for example, whether certain types of violations are increasing or decreasing and why. Further, the manner in which this information was maintained—geographically dispersed paper-based files—did not lend itself to this type of analysis. As a result, DSS was unable to identify patterns of security violations across all facilities based on factors such as the type of work conducted, the facilities' government customer, or the facilities' corporate affiliation. Identifying such patterns would enable DSS to target needed actions to reduce the risk of classified information being compromised. Similarly, DSS did not systematically collect or analyze information on foreign business transactions in a manner that helped it properly oversee contractors entrusted with U.S. classified information. Specifically, DSS did not know the universe of contractors operating under protective measures. With regard to contractors under FOCI, DSS did not collect and track in a timely manner the extent to which classified information was left in the hands of such contractors before measures were taken to reduce the risk of unauthorized foreign access. Specifically, we found instances in which contractors did not report foreign business transactions to DSS until several months after they had occurred.

DSS's process for notifying government agencies of possible compromises of their classified information has also been insufficient. When a contractor facility reports a violation and the possible compromise of classified information, DSS is required to determine whether compromise occurred and to notify the affected government agency so it can assess any damage and take actions to mitigate the effects of the suspected compromise or loss. However, for nearly 75 percent of the 93 violations

GAO reviewed, DSS either made no determination regarding compromise or made inappropriate determinations, such as "compromise cannot be precluded" or "compromise cannot be determined"—neither of which are covered by established criteria. In addition, in many cases in which DSS was required to notify the affected agencies of possible information compromises, the notification took more than 30 days; in one case, notification was delayed 5 months.

Finally, we found that DSS field staff lacked the guidance, tools, and training necessary to effectively carry out their responsibilities. DSS field staff faced a number of challenges that significantly limited their ability to sufficiently oversee contractors under FOCI. Field staff told us they lacked research tools and training to fully understand the significance of corporate structures, legal ownership, and complex financial relationships when foreign entities are involved. Staff turnover and inconsistencies over how guidance was to be implemented also detracted from field staff's ability to effectively carry out FOCI responsibilities.

Although in its initial response to our reports, DOD did not agree with many of our recommendations or the need for corrective actions, we understand that DSS has subsequently begun to address some of the issues we raised.

Background

NISP was established by executive order in 1993[2] to replace industrial security programs operated by various federal agencies. The goal of the national program is to ensure that contractors' security programs detect and deter espionage and counter the threat posed by adversaries seeking classified information. Contractor facilities must be cleared prior to accessing or storing classified information and must implement certain safeguards to maintain their clearance. The National Industrial Security Program Operating Manual (NISPOM) prescribes the requirements, restrictions, and safeguards that contractors are to follow to prevent the unauthorized disclosure—or compromise—of classified information.

DSS is responsible for providing oversight, advice, and assistance to U.S. contractor facilities that are cleared for access to classified information. Contractor facilities can range in size, be located anywhere in the United

[2]Executive Order no. 12829, signed January 6, 1993, established NISP for the protection of information classified under Executive Order 12958, as amended.

States, and include manufacturing plants, laboratories, and universities. Industrial security representatives work out of DSS field offices across the United States and serve as the primary points of contact for these facilities. Representatives' oversight involves educating facility personnel on security requirements, accrediting information systems that process classified information, approving classified storage containers, and assisting contractors with security violation investigations. DSS representatives also conduct periodic security reviews to assess whether contractor facilities are adhering to NISPOM requirements and to identify actual and potential security vulnerabilities.

Contractors are required to self-report foreign business transactions on a Certificate Pertaining to Foreign Interests form.[3] Examples of such transactions include foreign ownership of a contractor's stock, a contractor's agreements or contracts with foreign persons, and whether non-U.S. citizens sit on a contractor's board of directors. Contractors are required to report changes in foreign business transactions and to update this certificate every 5 years. Because a U.S. company can own a number of contractor facilities, the corporate headquarters or another legal entity within that company is required to complete the certificate.[4]

When contractors declare foreign transactions on their certificates and notify DSS, industrial security representatives are responsible for ensuring that contractors properly identify all relevant foreign business transactions. They are also required to collect, analyze, and verify pertinent information about these transactions. For example, by examining various corporate documents, the industrial security representatives are to determine corporate structures and ownership and identify key management officials. The representatives may consult with DSS counterintelligence officials, who can provide information about threats to U.S. classified information. If contractors' answers on the certificates indicate that foreign transactions meet certain DSS criteria or exceed thresholds, such as the percentage of company stock owned by

[3]In this testimony we refer to information reported by contractors on the Certificate Pertaining to Foreign Interests as foreign business transactions.

[4]Each business structure has its own set of legal requirements. Within the NISP, the most common type of business structure is the corporation. A corporation may be organized as a single corporate entity, a multiple facility organization with divisions, or a parent-subsidiary relationship. Under a multiple facility organization, the home office is the legal entity, while the divisions are extensions of the legal entity. In a parent-subsidiary relationship, the parent and the subsidiary are separate legal entities.

foreign persons, the representatives forward these cases to DSS headquarters. DSS headquarters works with contractors to determine what, if any, protective measures are needed to reduce the risk of foreign interests gaining unauthorized access to U.S. classified information. Field staff are then responsible for monitoring contractor compliance with these measures.

DSS Did Not Systematically Collect and Analyze Information to Identify Weaknesses and Institute Corrective Actions

In overseeing contractor facilities and contractors under FOCI, DSS did not systematically collect and analyze information to assess the effectiveness of its operations. Without this analysis, DSS was limited in its ability to detect trends in the protection of classified information across facilities, to determine sources of security vulnerabilities, and to identify those facilities with the greatest risk of compromise. In addition, DSS was unable to determine whether contractors were reporting foreign business transactions as they occurred or how much time a contractor facility with unmitigated FOCI[5] had access to classified information.

In overseeing contractor facilities, we found DSS evaluated its performance in terms of process factors, such as the

- percentage of security reviews completed,
- percentage of security reviews that covered all pertinent areas of contractors' security programs,
- length of time needed to clear contractor facilities for access to classified information, and
- length of time needed to clear contractor personnel for access to classified information.

While such indicators are important, they alone cannot measure where the greatest risks are, the types of violations that are occurring, and by whom. Performance indicators such as the ratings[6] and number of findings[7] that resulted from security reviews would have provided an indication as to

[5]Unmitigated FOCI refers to situations in which contractors with facility clearances are under FOCI and protective measures are needed but not yet implemented.

[6]After a security review, an industrial security representative was to rate that facility's security program in terms of how well it met NISPOM requirements and ensured the protection of classified information.

[7]DSS defined a finding as the failure to comply with the NISPOM. Findings were either administrative or serious. Serious findings could lead to the loss or compromise of classified information.

whether DSS was achieving its mission. However, there were no such indicators to determine overall facility ratings, the sources of the violations, and their frequency. Without such information, DSS cannot ensure facilities are protecting the classified information entrusted to them.

Similarly, DSS did not know how many contractors under FOCI were operating under all types of protective measures and, therefore, was unaware of the magnitude of potential FOCI-related security risks. Although DSS tracked information on contractors operating under some types of protective measures, it did not centrally compile data on contractors operating under all types of protective measures. Specifically, DSS headquarters maintained a central repository of data on contractors under voting trust agreements, proxy agreements, and special security agreements—protective measures intended to mitigate majority foreign ownership. However, information on contractors under three other protective measures—security control agreements, limited facility clearances, and board resolutions—were maintained in paper files in the field offices. DSS did not aggregate data on contractors for all six types of protective measures and did not track and analyze overall numbers. Such analysis would allow DSS to target areas for improved oversight.

The NISPOM requires contractors with security clearances to report any material changes of business transactions previously notified to DSS. DSS is dependent on contractors to self-report transactions by filling out the Certificate Pertaining to Foreign Interests form. However, this form did not ask contractors to provide specific dates for when foreign transactions took place. Consequently, DSS did not know if contractors were reporting foreign business transactions as they occurred and lacked knowledge about how much time a contractor facility with unmitigated FOCI had access to classified information. In addition, DSS did not compile or analyze how much time passed before it became aware of foreign business transactions. DSS field staff told us that some contractors reported foreign business transactions as they occurred, while others reported transactions months later, if at all. During our review, we found a few instances in which contractors were not reporting foreign business transactions when they occurred. One contractor did not report FOCI until 21 months after awarding a subcontract to a foreign entity. Another contractor hired a foreign national as its corporate president but did not report to DSS, and DSS did not know about the change until 9 months later, when the industrial security representative came across the information on the contractor's Web site. In another example, DSS was not aware that a

foreign national sat on a contractor's board of directors for 15 months until we discovered it while conducting our audit work.

DSS also did not determine the time elapsed between the reporting of foreign business transactions by contractors with facility clearances until the implementation of protective measures or when suspensions of facility clearances occurred. Without protective measures in place, unmitigated FOCI at a cleared contractor increases the risk that foreign interests can gain unauthorized access to U.S. classified information. We found two cases in which contractors appeared to have operated with unmitigated FOCI before protective measures were implemented. For example, officials at one contractor stated they reported to DSS that their company had been acquired by a foreign entity. However, the contractor continued operating with unmitigated FOCI for at least 6 months. According to the NISPOM, DSS shall suspend the facility clearance of a contractor with unmitigated FOCI, and DSS relies on field office staff to make this determination. Contractor officials in both cases told us that their facility clearances were not suspended. Because information on suspended contractors with unmitigated FOCI is maintained in the field, DSS headquarters did not determine at an aggregate level the extent to which and under what conditions it suspends contractors' facility clearances due to unmitigated FOCI.

Many Determinations of Information Compromise either Did Not Occur or Were Done Inappropriately

Industrial security representatives often failed to determine whether security violations by facilities resulted in the loss, compromise, or suspected compromise of classified information or made determinations that were not in accordance with approved criteria. Determinations of loss, compromise, or suspected compromise are important because the affected government customer must be notified so it can evaluate the extent of damage to national security and take steps to mitigate that damage. Even when representatives made an appropriate determination, they often took several weeks and even months to notify the government customer because of difficulties in identifying the customer. As a result, the customer's opportunity to evaluate the extent of damage and take necessary corrective action was delayed.

The NISPOM requires a facility to investigate all security violations. If classified information is suspected of being compromised or lost, the facility must provide its DSS industrial security representative with information on the circumstances of the incident and the corrective actions that have been taken to prevent future occurrences. The industrial security representative is to then review this information and, using the

criteria specified in DSS's Industrial Security Operating Manual, make one of four final determinations: no compromise, suspected compromise, compromise, or loss.

If a determination other than no compromise is made, the Industrial Security Operating Manual directs the representative to inform the government customer about the violation so a damage assessment can be conducted. However, for 39 of the 93 security violations that we reviewed, industrial security representatives made no determination regarding the compromise or loss of classified information. For example, in two cases involving one facility, the representative made no determination of compromise even though the facility reported the improper transmission of classified information via e-mail. In another eight cases at another facility, the representative made no determination despite employees' repeated failure to secure a safe room to ensure the protection of classified information. In the absence of a determination, the government customers were not notified of these violations and therefore were unable to take steps to assess and mitigate any damage that may have occurred.

For the remaining 54 violations that we reviewed, representatives made determinations regarding the compromise or loss of information, but many were not consistent with the criteria contained in DSS's Industrial Security Operating Manual. Representatives made 30 inappropriate determinations, such as "compromise cannot be precluded" or "compromise cannot be determined." For example, in nine cases, the same facility reported that classified material was left unsecured, and the facility did not rule out compromise. In each of these cases, the industrial security representative did not rule out compromise but used an alternative determination. Senior DSS officials informed us that industrial security representatives should not make determinations other than the four established in the Industrial Security Operating Manual because the four have specific meanings based on accepted criteria. By not following the manual, representatives introduced variability in their determinations and, therefore, their decisions of whether to notify the government customer of a violation.

The failure of representatives to always make determinations consistent with the Industrial Security Operating Manual was at least partially attributable to inadequate oversight. The Standards and Quality Branch is the unit within DSS responsible for ensuring that industrial security representatives properly administer the NISP. Branch officials regularly test and review field office chiefs and representatives on NISP requirements, particularly those related to granting clearances and conducting security reviews. However, the Standards and Quality Branch

did not test or review how representatives responded to reported violations and made determinations regarding compromise. As a result, DSS did not know the extent to which representatives understood and were consistently applying Industrial Security Operating Manual requirements related to violations and, therefore, could not take appropriate action.

While the Industrial Security Operating Manual did not specify a time requirement for notifying government customers when classified information had been lost or compromised, DSS was often unable to notify customers quickly because of difficulties in identifying the affected customers. DSS notified government customers regarding 16 of the 54 reported violations for which representatives made determinations. For 11 of these 16 violations, DSS did not notify the customer for more than 30 days after the contractor reported that information was lost, compromised, or suspected of being compromised. In one case, 5 months passed before an industrial security representative was able to notify a government customer that its information was suspected of being compromised. This delay was a result of the facility's inability to readily determine which government customer was affected by the compromise. DSS relied on the facility to provide this information. However, facilities that were operating as subcontractors often did not have that information readily available.

DSS Did Not Always Provide Adequate Guidance, Training, and Tools to Field Staff

DSS industrial security representatives faced several challenges in carrying out their FOCI responsibilities, largely due to complexities in verifying FOCI cases, limited tools to research FOCI transactions, insufficient FOCI training, staff turnover, and inconsistencies in implementing guidance on FOCI cases.

For industrial security representatives, verifying if a contractor is under FOCI is complex. Representatives are required to understand the corporate structure of the legal entity completing the Certificate Pertaining to Foreign Interests form and to evaluate the types of foreign control or influence that exist for each entity within a corporate family. For example, representatives are required to verify information on stock ownership by determining the distribution of the stock among the stockholders and the influence or control the stockholders may have within the corporation. This entails identifying the type of stock and the number of shares owned by the foreign person(s) to determine authority and management prerogatives. Some industrial security representatives told us they did not always have the tools needed to verify if contractors

are under FOCI. They conducted independent research using the Internet or returned to the contractor for more information to evaluate the FOCI relationships and hold discussions with management officials, such as the chief financial officer, treasurer, and legal counsel. DSS headquarters officials told us additional information sources, such as the Dun and Bradstreet database of millions of private and public companies were not available in the field.

In addition, industrial security representatives stated they lacked the training and knowledge needed to better verify and oversee contractors under FOCI. For example, DSS did not require its representatives to have financial or legal training. While some FOCI training was provided, representatives largely depended on DSS guidance and on-the-job training to oversee a FOCI contractor. In so doing, representatives worked with more experienced staff or sought guidance, when needed, from DSS headquarters.

Despite DSS efforts to provide training on FOCI, we found that the training needs on complex FOCI issues were still a concern to representatives. In fact, many said they needed more training to help with their responsibility of verifying FOCI information, including how to review corporate documents, strategic company relationships, and financial reports. In addition, officials from one-third of the field offices we reviewed noted staff retention problems. DSS officials at two of these field offices said that in particular they have problems retaining more experienced industrial security representatives.

Compounding these challenges are inconsistencies among field offices in how industrial security representatives said they understood and implemented DSS guidance for reviewing contractors under FOCI. For example, per DSS guidance, security reviews and FOCI meetings should be performed every 12 months for contractors operating under special security agreements, security control agreements, voting trust agreements, and proxy agreements. However, we found that some industrial security representatives did not follow the guidance. One representative said a contractor under a special security agreement was subject to a security review every 18 months because the contractor did not store classified information on-site. In addition, two industrial security representatives told us they did not conduct annual FOCI meetings for contractors that were operating under a proxy agreement and security control agreement, respectively. We also found that industrial security representatives varied in their understanding or application of DSS guidance for when they should suspend a contractor's facility clearance when FOCI was

unmitigated. The guidance indicates that when a contractor with a facility clearance is determined to be under FOCI that requires mitigation by DSS headquarters, the facility security clearance shall be suspended until a protective measure is implemented. However, we were told by officials in some field offices that they rarely suspend clearances when a contractor has unmitigated FOCI as long as the contractor is demonstrating good faith in an effort to provide documentation to DSS to identify the extent of FOCI and submit a FOCI mitigation plan to DSS. Officials in other field offices said they would suspend a contractor's facility clearance once they learned the contractor had unmitigated FOCI.

In conclusion, we believe that the weaknesses identified in the NISP and other programs designed to protect technologies critical to U.S. national security present significant challenges and need to be addressed. Although in its initial response to our reports, DOD did not agree with many of our recommendations or the need for corrective actions, we understand that DSS has subsequently begun to address some of the issues we raised. While we have not reviewed any of these actions and therefore can not address their potential effectiveness, we welcome DSS's recognition that action is needed.

Mr. Chairman this concludes my statement. I would be happy to answer any questions you or other members of the committee may have.

For information about this testimony, please contact Ann Calvaresi Barr, Director, Acquisition and Sourcing Management, at (202) 512-4841 or calvaresibarra@gao.gov. Other individuals making key contributions to this product include Thomas J. Denomme, Brandon Booth, John Krump, Karen Sloan, Lillian Slodkowski, and Suzanne Sterling.

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

APRIL 16, 2008

RESPONSE TO QUESTION SUBMITTED BY MR. BARTLETT

Ms. WATSON. The National Industrial Security Program (NISP) (established by Executive Order 12829, January 6, 1993) authorizes firms to receive classified contracts, and authorizes security clearances for their personnel under specific conditions. The NISP Operating Manual (NISPOM), DoD 5220.22-M, defines those conditions. The first condition is that the "company must need access to the classified information in connection with a legitimate U.S. Government or foreign government requirement" (NISPOM para. 2-102.a.). This threshold condition is met when a Federal government contracting activity or an already cleared company, usually acting as a prime contractor, sponsors a company for a facility clearance (FCL). The NISPOM states that "a contractor or prospective contractor cannot apply for its own FCL." (NISPOM para 2-102)

When a company is sponsored for an FCL, the Defense Security Service (DSS) inspects and evaluates the company's security qualifications. Key management personnel would also have to be eligible for a personnel security clearance in order for the company to be granted a FCL. Only a company that has a FCL or is in process for receiving a FCL may submit requests for personnel security clearances.

The lack of a FCL does not preclude a company from bidding on contract opportunities that may involve classified work or companies without a FCL being awarded classified contracts, subject to their being eligible for a FCL when the classified work on the contract is to begin. In addition, DSS will process a firm for a facility security clearance if a contracting activity requires the firm to access classified information in order to prepare a contract bid. [See page 23.]

RESPONSE TO QUESTION SUBMITTED BY MRS. BOYDA

Ms. WATSON. Airbus Americas is currently involved in commercial sales (aircraft design and construction, parts, tools, engineering services, etc.) and does not have any U.S. Defense contracts at this time. As of August 2008, the Defense Security Service did not have a request for a facility clearance for Airbus Americas. Airbus Americas is a European Aeronautics Defense and Space (EADS) company. EADS has five facilities in the United States; four with facility clearances and one in process for a facility clearance.

The Boeing Company has 25 cleared divisions and 15 cleared subsidiaries. The Boeing Company in Wichita, Kansas is cleared to the Top Secret level.

Further information on details of any contract awards should be directed to the appropriate Government Contracting Activity. The Defense Security Service is not involved in the contract award process. Further, DSS only has oversight of companies cleared under the National Industrial Security Program that are performing on government contracts requiring access to classified information. DSS has no oversight responsibility of companies performing on government contracts that do not require access to classified information. [See page 26.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

APRIL 16, 2008

QUESTIONS SUBMITTED BY MR. SAXTON

Mr. SAXTON. In 2007 DSS reported 647 FOCI cases. What constitutes a FOCI case? Of these 647 cases, were they all a result of self-reporting? How much are you missing because the system relies upon self reporting or holes in the reporting requirements?

Mr. SULLIVAN and Ms. WATSON. According to the NISPOM, a U.S. company is considered to be under Foreign Ownership, Control, or Influence (FOCI) "whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts." A company that is under FOCI is not eligible for access to classified information unless the FOCI can be mitigated. A FOCI case is an action, conducted at HQ or in the Field, analyzing affirmative response(s) on the SF 328, "Certificate Pertaining to Foreign Interests". Affirmative responses on the SF 328 indicate potential FOCI.

DSS primarily relies upon information provided by the company to make a determination of the company's eligibility for access to classified information. In this regard, DSS is in a position similar to many other government agencies that rely upon company self-reporting, such as the SEC. When DSS initially processes a firm for a facility security clearance, DSS reviews and attempts to validate FOCI information provided by the firm. DSS inspects cleared companies, and requires them to correct, supplement and update information which was not accurate when submitted or is out of date. Should DSS determine that the company has failed to provide required and accurate FOCI information, DSS can invalidate its facility security clearance, which precludes the firm from being awarded new classified contracts, or, if warranted, revoke its facility security clearance. Historically, situations where the company failed to report accurate and complete information have been rare, however DSS has not measured the extent to which information reported is incomplete or inaccurate.

Mr. SAXTON. Do companies with Government Security Committees do a better job of self-reporting? How does the Government Security Committee improve a company's compliance with NISPOM?

Mr. SULLIVAN. Government Security Committees (GSCs) are a part of the company governance structure required by Voting Trusts, Proxy Agreements, Special Security Agreements, and Security Control Agreements. These are mitigation measures put in place to protect classified information when there are significant Foreign Ownership, Control, or Influence (FOCI) concerns associated with the company. Companies with these agreements have additional reporting requirements because of the FOCI concerns at the company. They represent approximately two percent of the cleared contractor population of approximately 12,000 cleared facilities.

DSS has not noted that self-reporting or NISPOM compliance by companies with a GSC is any different than by companies that do not have a GSC.

Mr. SAXTON. In 2007 DSS reported 647 FOCI cases. What constitutes a FOCI case? Of these 647 cases, were they all a result of self-reporting? How much are you missing because the system relies upon self-reporting or holes in the reporting requirements?

Dr. SCHNEIDER. The Defense Science Board has not addressed the specific question asked and therefore I can not respond to your inquiry.

Mr. SAXTON. Do companies with Government Security Committees do a better job of self-reporting? How does the Government Security Committee improve a company's compliance with NISPOM?

Dr. SCHNEIDER. The Defense Science Board has not addressed the specific question asked and therefore I can not respond to your inquiry.

Mr. SAXTON. In 2007, DSS reported 647 FOCI cases. (a) What constitutes a FOCI case? (b) Of these 647 cases, were they all a result of self-reporting? (c) How much are you missing because the system relies upon self-reporting or holes in the reporting requirements?

Ms. CALVARESI BARR.

- DSS, industrial security representatives (ISR) are responsible for ensuring that contractors properly identify all relevant foreign business transactions. The ISR is required to collect, analyze, and verify the pertinent information about these transactions to determine whether foreign ownership, control, or influence (FOCI) exists. If contractors' indicate that foreign transactions meet certain DSS criteria [1] or exceed thresholds, such as the percentage of company stocked owned by foreign persons, the ISR forwards the case to DSS headquarters. DSS headquarters works with the contractor to determine what, if any, protective measures are needed to reduce the risk of foreign interests gaining unauthorized access to U.S. classified information. Then, DSS field staff monitor contractor compliance with these measures.
- Identification of FOCI is generally the result of self reporting on the part of the contractor. However, we can not say whether all 647 cases resulted only from self reporting.
- While we are not able to say how much is being missed, our work found that ISR's lacked the training and knowledge needed to verify complex FOCI cases. Further, we found that DSS headquarters did not know the universe of all contractors operating under all types of protective measures used when FOCI is present.

Mr. SAXTON. (a) Do companies with Government Security Committees (GSC) do a better job of self-reporting? (b) How does the Government Security Committee improve a company's compliance with NISPOM?

Ms. CALVARESI BARR.

- A GSC is established after FOCI has been identified to help ensure that the company under FOCI maintains policies and procedures to safeguard classified information and sensitive but unclassified information in the possession of the. The GSC is also to help ensure that the company complies with U.S. export control laws and regulations and does not take action deemed adverse to performance on classified contracts.
- By following through and effectively carrying out its responsibilities under the NISPOM, the GSC increases the likelihood that the company will comply with the NISPOM.

QUESTIONS SUBMITTED BY MR. LOEBSACK

Mr. LOEBSACK. In an increasingly globalized world and defense industry, do you consider investment in U.S. defense firms, and a strong, competitive U.S. defense industry, to be important to our national security? a. How do you assure that, when U.S. contracts are awarded to foreign companies, U.S. defense and national security data, technology, expertise, and capabilities are not outsourced to such a degree that we lose them in this country all together? b. Could policy disagreements between the U.S. and nations in which U.S.-contracted companies are based result in a situation where critical, outsourced U.S. defense technology is not delivered or not available? Is such a possibility taken into account when assessing the awarding of a U.S. defense contract to a foreign company? c. The United States' aerial refueling fleet is the foundation of every mission undertaken by our men and women in uniform and is vital to the readiness of our Armed Forces. If the KC–X tanker award is outsourced, won't the United States lose our vital edge in this critical technology and capability? d. What is being done to guarantee that the United States would have not only the data, but the intellectual and real capital and capability to produce tankers for the U.S. military in the event that something unforeseen happens that is outside of our control—politically, militarily, or otherwise—that will enable the U.S. government to ensure that it could domestically develop, build and support tankers?

Mr. SULLIVAN and Ms. WATSON. The Office of the Under Secretary of Defense defers to the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics to respond to this question because the question is outside the oversight responsibilities of the Office of the Under Secretary of Defense for Intelligence.

---

[1] The following factors are considered in the aggregate in determining whether a company is under FOCI: a. Record of economic and government espionage against U.S. targets, b. Record of enforcement and/or engagement in unauthorized technology transfer, c. Type and sensitivity of information requiring protection, d. The source, nature and extent of FOCI, e. Record of compliance with pertinent U.S. laws, regulations and contracts, and f. Nature of bilateral and multilateral security and information exchange agreements.

Mr. LOEBSACK. In an increasingly globalized world and defense industry, do you consider investment in U.S. defense firms, and a strong, competitive U.S. defense industry, to be important to our national security? a. How do you assure that, when U.S. contracts are awarded to foreign companies, U.S. defense and national security data, technology, expertise, and capabilities are not outsourced to such a degree that we lose them in this country all together? b. Could policy disagreements between the U.S. and nations in which U.S.-contracted companies are based result in a situation where critical, outsourced U.S. defense technology is not delivered or not available? Is such a possibility taken into account when assessing the awarding of a U.S. defense contract to a foreign company? c. The United States' aerial refueling fleet is the foundation of every mission undertaken by our men and women in uniform and is vital to the readiness of our Armed Forces. If the KC–X tanker award is outsourced, won't the United States lose our vital edge in this critical technology and capability? d. What is being done to guarantee that the United States would have not only the data, but the intellectual and real capital and capability to produce tankers for the U.S. military in the event that something unforeseen happens that is outside of our control—politically, militarily, or otherwise—that will enable the U.S. government to ensure that it could domestically develop, build and support tankers?

Dr. SCHNEIDER. The Defense Science Board has not addressed the specific question asked and therefore I can not respond to your inquiry.

Mr. LOEBSACK. In an increasingly globalized world and defense industry, do you consider investment in U.S. defense firms, and a strong, competitive U.S. defense industry, to be important to our national security?

Ms. CALVARESI BARR. Defense trade not only helps support the U.S. industrial base but also provides the economic benefit of a positive trade balance. U.S. military strategy is premised on technological superiority on the battlefield. The Department of Defense spends billions of dollars each year for the development and production of high technology weaponry to maintain that superiority. Yet, the technologies that underpin U.S. military strength continue to be targets for theft, espionage, reverse engineering, and illegal export. At the same time, the programs the U.S. government has in place to protect critical technologies by weighing competing and sometimes conflicting national security, foreign policy, and economic interests have long been criticized by industry and allies for their inability to adapt to a changing world environment and their lack of efficiency.

In addition, as mentioned, the economy has become increasingly globalized as countries open their markets and the pace of technological innovation has quickened worldwide. The myriad of laws, regulations, policies, and processes intended to identify and protect critical technologies so they can be transferred to foreign parties in a manner consistent with U.S. interests include the national industrial security program, those that regulate U.S. defense-related exports and the investigation of proposed foreign acquisitions of U.S. national security-related companies. Responsibility for administering or overseeing the different programs is divided among multiple federal agencies and several congressional committees. However, we have found that these programs are often ill-equipped to weigh competing U.S. national security and economic interests. As a result, to address the issues you raise we believe a strategic reexamination of the existing programs is needed to ensure the advancement of U.S. interests.