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.