

Testimony of
Peter C.W. Flory
Assistant Secretary of Defense for International Security Policy
Before the
Senate Committee on Banking, Housing, and Urban Affairs
on the Impact of Exon-Florio on National Security
October 20, 2005

Chairman Shelby, Congressman Sarbanes, Members of the Committee:

Thank you for the opportunity to appear before you today to discuss the impact of section 721 of the Defense Production Act (50 U.S.C. App. §2170 and also known as the Exon-Florio amendment) on national security. We in the Department of Defense (DoD) take very seriously our role in protecting technology, the defense industrial base and the security of those critical infrastructures we depend upon to accomplish our mission. Foreign investment in the United States generally is desirable. In terms of the defense sector, foreign investment has been helpful in maintaining the viability and diversity of the defense industry.

When it comes to reviewing a foreign acquisition of a US company, there are a number of factors which we in the DoD consider before taking a position. These include five major areas of interest:

First, the significance of the technologies possessed by the firm to be acquired (e.g., are they “state of the art” or otherwise militarily critical? Are they classified, export controlled, or otherwise security sensitive?);

Second, the importance of the firm to the US defense industrial base (e.g., is it a sole-source supplier and if so, what security and financial costs would be incurred in finding and /or qualifying a new supplier, if required?);

Third, possible security risks or concerns that might be posed by the particular foreign acquiring firm (e.g., is it controlled by a foreign government? Does the firm have a record of export control violations?);

Fourth, whether the company to be acquired is part of the critical infrastructures that the Defense Department depends upon to accomplish its mission; and

Fifth, can any potential national security concerns posed by the transaction be eliminated by the application of risk mitigation measures either under the Department’s own regulations or through negotiation with the parties?

DoD Participants and their Roles in CFIUS

Within the Department of Defense, there are a variety of DoD offices and agencies involved in the CFIUS review of each case. The Defense Technology Security Administration (DTSA) plays an important role as our representative to the Committee on Foreign Investment in the United States (CFIUS). DTSA is responsible for the

management, coordination and formulation of the Department's position for all CFIUS cases. DTSA is also the focal point within the Department for technology security policy as regulated by the Export Administration Regulation, International Traffic in Arms Regulation and the National Disclosure Policy. The Office of the Under Secretary, Acquisition, Technology and Logistics (USD/AT&L), determines if the US company involved in a CFIUS case provides a product or service that is a critical technology. That office also evaluates the transaction's impact on the defense industrial base, including whether the firm is a sole-source provider, and what the costs would be if we were required to find a new supplier.

The Office of the Assistant Secretary of Defense for Networks Information and Integration (ASD/NII), with input from subject matter experts such as the National Security Agency and the Defense Information Systems Agency, performs vital technical reviews of filings that involve critical information and telecommunications infrastructures. In its CFIUS review of cases involving defense contractors performing classified work, the Office of the Under -Secretary for Intelligence assesses whether the Defense Industrial Security Regulations are adequate to mitigate potential national security concerns of foreign control of US defense contractors. The National Industrial Security Program is a separate, but parallel process to the CFIUS review that protects classified information in US located firms owned/acquired by foreign companies.

The three military services (Army, Navy, and Air Force) identify and assess the impact of the transfer of technology relevant to the particular military service, especially when cases involve current or former defense contractors. Specifically, the services review cases to determine if commodities or technologies involved in a given transaction may affect warfighters' capabilities and technological advantages. The Defense Logistics Agency assesses the effect of the transaction on defense procurement and planning. The Defense Advanced Research Projects Agency evaluates the technology to be transferred, its relationship to defense programs, and its potential impact on future defense capabilities. The Defense Intelligence Agency prepares intelligence assessments and analyzes the risk of diversion. The Office of General Counsel provides positions on legal issues, including adequacy of other laws to protect national security, and other legal assistance.

Changing Nature of DoD Suppliers

I would now like to address an issue that is gaining increasing importance for DoD, that is, the growing role of non-traditional, commercial, and dual-use suppliers to the Department. As part of defense transformation, the Department is focusing on real-time communication between those systems and personnel responsible for finding enemy targets and those systems and personnel responsible for destroying or incapacitating those targets. This goes under the name of network-centric warfare or sensor-shooter integration, and is essential to the Department's transformational efforts. This

transformation increasingly involves the use of technologies from commercial markets in such fields as information technology, telecommunications and electronics, among others. Many of the suppliers are at the component and subsystem level and may not even have classified contracts.

Mitigation Measures and Security Agreements

Mitigation agreements, negotiated in conjunction with a CFIUS review, vary in scope and purpose, and are negotiated on a case-by-case basis to address the particular concerns raised by an individual transaction.

When we find potential national security concerns with a foreign acquisition, we normally use the risk mitigation measures available to us under the National Industry Security Program's Foreign Ownership, Control, and Influence Program (FOCI). The DoD imposes special mitigation/negation measures for companies that are cleared for access to classified information when they are acquired by a foreign source. These security agreements specify procedures to ensure protection of classified and export-controlled information. The Department's Defense Security Service enters into negotiations with the parties of such cases and develops specifically tailored agreements, which are designed to provide for the necessary level of security for such classified, export-controlled information and technologies.

The Department and other agencies occasionally negotiate risk mitigation measures for acquisitions where there are no classified contracts. As previously addressed, this is becoming more common as we increasingly rely on dual use and primarily commercial suppliers. As we review foreign acquisitions when FOCI does not apply, we have to enter a negotiation process with the parties to the transaction to develop appropriately tailored risk mitigation measures.

In the telecommunications sector, conditions have been imposed in the context of the Federal Communications Commission's (FCC) licensing process. Transactions involving the foreign acquisition of a US telecommunications company usually are subject to regulation by the FCC, which is an independent regulatory agency. The FCC has, in some cases, agreed to place conditions on the transfer of licenses to a foreign company subject to compliance with the Network Security Agreement that CFIUS member agencies have negotiated with that company before the transaction is finalized. The Network Security Agreement includes actions the commercial parties agree to undertake (during the initial review or during the investigatory period) in order to mitigate the national security risk. CFIUS members, in turn, agree to not object to the transaction if the companies have implemented the negotiated mitigation measures.

Conclusion

Mr. Chairman that concludes my formal statement. I would be happy to answer any further questions you may have regarding this subject.