Hunter Statement on the Implications of Globalization & Foreign Ownership on the Defense Industrial Base

April 16, 2008

Contact: Josh Holly; 202.226.3988

Hunter Statement on the Implications of Globalization & Foreign Ownership on the Defense Industrial Base

Washington D.C.

- House Armed Services Committee Ranking Republican Duncan Hunter (R-CA) released the following opening statement for the committee's hearing on the National Industrial Security Program (NISP) and the implications of globalization and foreign ownership on the defense industrial base:

"Thank you Mr. Chairman for holding this hearing on a program that, to date, has received little Congressional attention, but addresses a subject that goes to the heart of an issue this Committee cares 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 military 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 ‘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, a program which essentially imposes a set of requirements upon a contractor in exchange for a Facility Security Clearance that allows the 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 obligated 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’ve 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 cannot create this culture of compliance on their own. These companies need the support and guidance of the Department. It’s unreasonable 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 (DSS) has struggled in recent years in this regard, and I’m curious to hear from DSS on the steps they are taking to ensure that industry has a partner in government that aids and supports industry as they carry out their NISP obligations.

Finally, Mr. Chairman, I’d like to take this Committee back to a hearing we held in this room on March 2, 2006. On that day, over two years ago, we examined the national security implications 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 more complicated and difficult task, and in my view, requires no less attention by the Congress than what was given to Dubai Ports case and the subsequent CFIUS legislation.”

###


2340 Rayburn House Office Building, Washington, DC 20515  Phone: (202) 226-8980  Fax: (202) 225-0858