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.