April 10, 2008

Expected Release
10:00 a.m.

Charles W. Beardall

Deputy Inspector General for Investigations
Department of Defense

before the

Subcommittee on National Security
and Foreign Affairs
United States House of Representatives

on

"Investigation into the Sale of Sensitive, In-Demand Military Equipment and Supplies on the Internet"

Chairman Tierney, Congressman Shays, and distinguished members of the Subcommittee on National Security and Foreign Affairs, thank you for the opportunity to appear before you and discuss the DoD Office of the Inspector General's efforts to stem the theft and sale of sensitive military equipment and supplies on the Internet.

Consistent with its mission of "Protecting America's Warfighters by conducting investigations in support of crucial National Defense priorities," the Defense Criminal Investigative Service (DCIS), the law enforcement arm of the DoD Inspector General, has been actively engaged in investigating the theft, diversion, and sale of sensitive military technologies since the early 1990s. These technology protection investigations join terrorism, major procurement fraud, corruption, and protection of the Global Information Grid as our top five investigative priorities.

Subsequent to the terrorist attacks of September 11, 2001, DCIS recognized the need to place increased emphasis upon investigations involving diversion of sensitive technologies to countries and subversive groups that could potentially utilize our technology against our Armed Forces, our allies, or even our citizens. To this end, DCIS senior leaders in the field were instructed to prioritize investigations involving the illegal transfer of sensitive DoD technology, systems, and equipment. Theft and export enforcement investigations (collectively referred to as "technology protection" investigations) have grown to encompass approximately twenty percent of DCIS' active caseload. Noteworthy is the fact that 90% of DCIS' active undercover operations focus upon technology protection.

DCIS currently employs approximately 340 special agents who are assigned to 57 offices located throughout the United States, and in Europe and Southwest Asia. Pursuant to the Inspector General Act of 1978, DCIS has broad criminal investigative jurisdiction regarding DoD programs and operations. However, effectively countering the illegal sale of sensitive DoD equipment requires the cooperative efforts of other DoD investigative agencies and Federal law enforcement partners. DCIS is currently recognized by the FBI, Immigration and Customs Enforcement (ICE), the U.S. Department of Commerce, and various members of the Intelligence Community as a significant partner in the on-going battle against counter-proliferation and illicit technology transfer. DCIS is also a charter member of the Department of Justice's National Counter-Proliferation Initiative. Despite our broad commitment, manpower limitations restrict DCIS from becoming involved in all investigations involving theft and sale of DoD equipment. As a result, we must be selective in the investigations we undertake, and focus upon the more serious or threatening offenses. Lesser offenses which we discover are often referred to the Military Criminal Investigative Organizations (MCIOs – which include the U.S. Army Criminal Investigation Command, the U.S. Air Force Office of Special Investigations, and the Naval Criminal Investigative Service) or Defense agencies for investigation.

As mentioned above, DCIS has established as one of our top five priorities those investigations involving the illegal sale and export of controlled Defense technologies and U.S. Munitions List Items in violation of International Traffic in Arms Regulations. The majority of our investigations involve foreign nationals who contact U.S. Defense

contractors seeking to obtain controlled technology for export to various countries. These foreign nationals include terrorists, arms dealers, foreign counterintelligence officers, members of foreign militaries, and arms brokers. Defense items being sought by these individuals include missiles; Man-Portable Air Defense Systems (sophisticated shoulder-fired rockets used to bring down aircraft); Unmanned Aerial Vehicles; M-16 and M-4 rifles and other weapons; night vision goggles; communication equipment; aircraft parts; and components used in making weapons of mass destruction.

DCIS also gives priority to investigations involving the sale of items which are not appropriately "demilitarized." The Defense Reutilization and Marketing Service, a component of Defense Logistics Agency (DLA), disposes of excess property received from the military services. Some of this property was built strictly for military purposes. This type of property must be rendered useless for its intended purpose ("demilitarized") prior to sale or removal from government inventory. Demilitarization prevents offensive and defensive military equipment from being released to the public. It also prevents battlefield-related property from being unnecessarily rendered useless. For instance, tanks and rocket launchers are candidates for sale as scrap after demilitarization; tents and combat boots can be reused or sold to the public. Many items that enter the supply system receive a "no demilitarization required" code, such as office furniture, tools, or appliances. On the other hand, items such as arms or munitions must be rendered useless prior to sale, and require destruction. Certain items requiring demilitarization can be legally sold to the public depending on inventory status; however, certain articles cannot be legally possessed by the public. In some cases, items are improperly released to the public prior to

demilitarization (this typically occurs when the item is incorrectly classified as not requiring demilitarization). In such instances, DCIS will determine if the item can be utilized against United States interests or is export controlled and undertake an investigation. One limitation to our efforts is that DCIS agents have no statutory authority to seize items that were legally sold to the public, but were not appropriately de-militarized. Unless we can establish the goods were stolen, we often have to rely upon the "owner" to voluntarily forfeit the items. Complicating matters further is the fact that suspects who obtained the items legally sometimes seek compensation from the Government.

The following are examples of controlled item investigations that DCIS pursues:

- A citizen of the Democratic Socialist Republic of Sri Lanka was convicted and sentenced to 57 months incarceration for conspiring to provide material support to a designated foreign terrorist organization and attempted exportation of arms and munitions. The individual conspired to illegally export machine guns, ammunition, surface-to-air missiles, night vision goggles, and other military equipment to the Liberation Tigers of Tamil Eelam (Tamil Tigers).

- U.S. and Austrian authorities thwarted a plot by Iranian agents to buy 3,000 U.S.-made helmet-mounted military night vision systems. Two Iranian nationals were taken into custody in Vienna, Austria, as the result of a two-year joint investigation by ICE, DCIS, and the Austrian Federal Agency for State Protection and Counter-Terrorism

- A citizen of the Republic of Indonesia was convicted and sentenced to 37 months incarceration for conspiring to provide material support to a foreign terrorist organization, money laundering, and attempted exportation of arms and munitions. The individual sent an itemized list to a Maryland undercover business requesting 53 military weapons, including sniper rifles, machine guns, and grenade launchers destined for the Tamil Tigers.

- An Iranian citizen pled guilty and was sentenced to 57 months incarceration for attempting to export aircraft parts and gunnery system components for the F-4 and F-14 fighter aircraft to Iran and for money laundering. One of the components the individual attempted to export was an M61A1 Vulcan six-barrel rotary action inner drum, which feeds ammunition into a multi-barrel "Gatling gun" used in military aircraft. The weapon is capable of firing 6,000 rounds of 20mm ammunition per minute.

- Agents from DCIS and ICE received information that an individual, who was later identified as a covert agent of the People's Republic of China, was seeking to procure 70 Blackhawk helicopter engines. Over a two-year period, numerous meetings, faxes, emails, and consensual recorded conversations detailed negotiations involving the purchase of F-16 fighter aircraft jet engines, MH-60 Blackhawk helicopter engines, AIM-120 Air-to-Air missiles, and AGM-129 Air to Ground missiles. The subject of the investigation traveled to the U.S. and met with DCIS and ICE undercover agents and was shown the aircraft engine. Two days later the subject sent a wire transfer of

$140,000, to an undercover bank account. He was subsequently arrested. While in custody, he attempted to bribe an Assistant United States Attorney for $500,000. He was ultimately charged with violations of the Arms Export Control Act, conspiracy, money laundering, failure to register as a foreign agent, bribery, and obstruction of justice. In May 2006, the individual pled guilty to being a covert agent of the People's Republic of China, export violations, and bribery of a public official. In July 2006, the individual was sentenced to serve 78 months confinement, followed by 36 months supervised probation, and ordered to pay $1,000,000 in fines.

As these examples illustrate, our efforts to combat the illegal export of U.S. Defense technology have primarily focused on items that could potentially be used against our soldiers, sailors, airmen, and marines or deny them the advantage that American technology should provide them.

It is important to note that many of the investigations we initiate stem from cooperative relationships with our DoD partners, to include the Defense Security Service (DSS). DoD contractors are required to report any "suspicious" contacts they receive to DSS. DSS conducts open source database searches on the individuals and then makes a formal referral to the FBI, ICE, DCIS, MCIOs, and appropriate members of the Intelligence Community.

In addition to DSS referrals and information derived from confidential sources, DCIS and partner agencies utilize undercover operations to actively search Internet websites such as eBay, Craig's List, and the Inventory

Locator Service, in an attempt to identify controlled U.S. military items. Since it is nearly impossible to review every Internet sale, agents focus on identifying sellers who appear to intend to export controlled items or sell large quantities of specialized items. When investigations identify relatively minor offenses (for example, potential sale of individual items not associated with weapon systems or controlled technologies), they are typically referred to appropriate MCIOs or DLA for action deemed appropriate.

One example of a particularly significant undercover operation which targeted illegal sales of controlled items on the Internet was DCIS' Operation High Bidder. Operation High Bidder was initiated based on a referral from Defense Supply Center Philadelphia. The Defense Supply Center informed DCIS that DoD property, to include small arms protective insert (SAPI) body armor components and outer tactical vests, were being sold on eBay. DCIS initiated an investigative project on April 2003. The operation identified numerous persons throughout the U.S selling military grade body armor on eBay. High Bidder resulted in the generation of approximately 183 information reports which were referred to various DCIS offices throughout the country for follow-up investigation. One hundred thirty nine cases were initiated. Investigations resulted in issuance of 11 arrest warrants and 34 search warrants. Fifty-one criminal charges were filed, which resulted in 44 individuals being convicted and sentenced to a total of over 48 years. Additionally, over $400,000 in fines were collected. In addition to these results, there are two unquantifiable benefits to High Bidder that are still visible today, and those are the reduced number of sales of certain controlled items and greater public confidence, through publicity, that DoD is policing these illegal sales.

One case that received nation-wide exposure identified a U.S. Marine Corps staff sergeant assigned to Camp Pendleton, CA, as an eBay subscriber who sold a body armor outer tactical vest for $202. In 2003, similar vests cost the Government up to $1,400. The staff sergeant confessed to the theft of 50 sets of body armor. The case was referred to the Marine Corps for prosecution under the Uniform Code of Military Justice. The staff sergeant was sentenced to 10 years in prison and received a dishonorable discharge.

Operation High Bidder generated a DCIS fraud vulnerability report which concluded that lack of appropriate internal control mechanisms and inadequate tracking systems at Defense depots and military installations throughout the U.S. contributed towards diversion of controlled property from intended end-users. The vulnerability report concluded that, in some cases, DLA was unable to trace SAPIs once they left the manufacturer's plant. Identifying the means by which individuals obtained items was therefore often impossible to ascertain, since the SAPIs could not be traced via DLA. The vulnerability report was provided to the Director of DLA, and the Assistant Deputy Undersecretary of Defense, Supply Chain, for their action.

Operation High Bidder also resulted in issuance of a DCIS Criminal Intelligence Report which was distributed to thousands of military components as well as State, local, and Federal law enforcement organizations throughout the U.S. The bulletin notified recipients of the potential availability of stolen body armor, SAPIs, and related military equipment to the general public, and alerted law enforcement officers to the possibility that the equipment could be obtained and utilized by criminal

elements. The bulletin provided points of contact within DCIS that could assist should the equipment be encountered in the field.

It should be noted that eBay was supportive of law enforcement efforts related to Operation High Bidder. The operation resulted in installation of filters on eBay which use key words to identify body armor and related items. While effective, these filters are not 100% successful in identifying controlled items. DCIS undercover operations continue to identify the sale of sensitive DoD technologies via eBay and other Internet sites, in addition we continue to pursue other preventive measures.

DCIS worked with eBay to draft language for inclusion on the website which informs sellers and buyers that "eBay does not permit sale of equipment and supplies issued to and formerly used by United States Armed Forces that have not been disposed of in accordance with Department of Defense demilitarization policies."

DCIS also is a strong participant in the ICE-sponsored Project Shield America which is an industry outreach initiative developed to prevent the illegal export of sensitive U.S. munitions and strategic technology to terrorists, criminal organizations, and foreign adversaries.

I would like to conclude by emphasizing the fact that the DoD Office of the Inspector General remains steadfastly committed to aggressively countering the illegal sale of sensitive DoD equipment and technologies on the Internet. We will continue to prioritize technology protection investigations and place special emphasis upon investigations involving the theft and sale of weapon systems, munitions, and related items which could

be utilized against our men and women in the Armed Forces, our allies, and our citizens. We will continue to keep Congress and DoD leadership fully and promptly informed regarding our efforts.