United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Thursday, June 4, 2009

MILITARY AND DUAL-USE TECHNOLOGY

Covert Testing Shows Continuing Vulnerabilities of Domestic Sales for Illegal Export

Statement of Gregory D. Kutz, Managing Director
Forensic Audits and Special Investigations

GAO
Accountability * Integrity * Reliability

GAO-09-725T

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
Accountability • Integrity • Reliability

Highlights

Highlights of GAO-09-725T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

June 4, 2009

MILITARY AND DUAL-USE TECHNOLOGY

Covert Testing Shows Continuing Vulnerabilities of Domestic Sales for Illegal Export

Why GAO Did This Study

Terrorists and foreign governments regularly attempt to obtain sensitive dual-use and military technology from manufacturers and distributors within the United States. Although the Department of State (State) or Department of Commerce (Commerce), or both, must grant approval to export sensitive military and dual-use items, publicly reported criminal cases show that individuals can bypass this requirement and illegally export restricted items such as night-vision goggles. In the wrong hands, this technology poses a risk to U.S. security, including the threat that it will be reverse engineered or used directly against U.S. soldiers.

Given the threat, the subcommittee asked GAO to conduct undercover tests to attempt to (1) purchase sensitive dual-use and military items from manufacturers and distributors in the United States; and (2) export purchased items without detection by domestic law-enforcement officials.

To perform this work, GAO used fictitious individuals, a bogus front company, and domestic mailboxes to pose as a buyer for sensitive items. GAO, in coordination with foreign law-enforcement officials, also covertly attempted to export dummy versions of items. GAO interviewed relevant agencies to gain an understanding of which items were in demand by terrorists and foreign governments. GAO actions were not designed to test controls of other countries. Relevant agencies were also briefed on the results of this work.

View GAO-09-725T or key components.
For more information, contact Gregory Kutz at (202) 512-6722 or kutzg@gao.gov.

What GAO Found

GAO found that sensitive dual-use and military technology can be easily and legally purchased from manufacturers and distributors within the United States and illegally exported without detection. Using a bogus front company and fictitious identities, GAO purchased sensitive items including night-vision scopes currently used by U.S. soldiers in Iraq and Afghanistan to identify targets, triggered spark gaps used to detonate nuclear weapons, electronic sensors used in improvised explosive devices, and gyro chips used in guided missiles and military aircraft. Interviews with cognizant officials at State and Commerce and a review of laws governing the sale of the types of items GAO purchased showed there are few restrictions on domestic sales of these items.

GAO was also able to export a number of dummy versions of these items using the mail to a country that is a known transshipment point for terrorist organizations and foreign governments attempting to acquire sensitive technology. Due to the large volume of packages being shipped overseas, and large volume of people traveling overseas, enforcement officials within the United States said it is impossible to search every package and person leaving the United States to ensure sensitive technologies are not being exported illegally. As a result, terrorists and foreign governments that are able to complete domestic purchases of sensitive military and dual-use technologies face few obstacles and risks when exporting these items. The table below provides details on several of the items GAO was able to purchase and, in two cases, illegally export without detection.

Sensitive Items Purchased by GAO Using Fictitious Identities

Item	Use	Notes
Gyro chip	Dual-use – Used in advanced aircraft, missile, space and commercial systems for stabilization, control, guidance, and navigation	• In 2006, company paid a $15 million civil penalty for the export of civil aircraft containing a gyro chip to China • The gyro chip is fully self contained, lightweight, and has a virtually unlimited life • GAO exported without detection
Night-vision monocular	Military – Used by U.S. troops to identify targets in nighttime operations	• In 2006, criminal convictions for two people involved in export of night-vision devices to the terrorist group Hezbollah • GAO's bogus company became a certified distributor for the item, gaining access to an unrestricted quantity. • Contains an image intensifier tube made to military specifications
Accelerometer	Dual use – Accelerometers are suitable for use in "smart" bombs and for measuring motions generated by nuclear and chemical explosives	• Item is in high demand by foreign countries and was the subject of a 2007 U.S. Immigration and Customs Enforcement investigation • In 2007, an individual was sentenced for conspiracy to smuggle military-grade accelerometers from the United States to China • GAO exported without detection

Source: GAO.

Mr. Chairman and Members of the Subcommittee:

Terrorists and foreign governments regularly attempt to obtain sensitive dual-use[1] and military technology from manufacturers and distributors within the United States. Recently the Department of Justice (DOJ) reported that, on a daily basis, foreign states as well as criminal and terrorist groups seek arms, technology, and other material to advance their technological capacity. With the United States producing advanced technology, it has become a primary target of these illegal technology-attainment efforts. For fiscal year 2008, DOJ publicly reported more than 145 defendants faced criminal charges for violations of export-control laws. Roughly 43 percent of the defendants charged in these cases were attempting to illegally transfer items to Iran or China. For example, a 2007 undercover investigation by the U.S. Immigration and Customs Enforcement (ICE) agency revealed that an individual in Connecticut attempted to purchase and illegally export an accelerometer to China. According to the indictment, this accelerometer is suitable for use in smart bombs and for measuring motions generated by nuclear and chemical explosives. In another example, in 2008, various individuals and companies were indicted on federal charges for purchasing items capable of being used to construct Improvised Explosive Devices (IED), including inclinometers, and exporting these items to multiple transshipment points, with Iran being the final destination. These types of items have been, and may continue to be, used against U.S. soldiers in Iraq and Afghanistan. In addition, we have identified weaknesses in the effectiveness and efficiency of government programs designed to protect critical technologies while advancing U.S. interests. Since 2007, we have included ensuring the effective protection of technologies critical to U.S. national security interest as a high-risk area.[2]

While the U.S. State Department (State) and Commerce Department (Commerce) each have jurisdiction over the export of certain items to countries outside the United States, many of these same items can be purchased legally within the United States. In a testimony before another congressional committee in 2008, we described how our undercover agents were able to purchase sensitive items such as F-14 Tomcat aircraft parts, night-vision goggles currently being used by U.S. forces, and

[1]Dual-use items refer to items that have commercial uses as well as military or nuclear proliferation uses.

[2]See GAO, *High-Risk: Series an Update*, GAO-09-271 (Washington, D.C.: Jan, 22, 2009).

current-issue military body armor on commercial internet sites such as eBay and Craigslist.[3] Given the ease at which we were able to buy those items, and the continued attempts by foreign governments and terrorist groups to obtain sensitive technologies from within the United States, the committee asked us to conduct proactive testing to attempt to (1) purchase sensitive dual-use and military items from manufacturers and distributors in the United States; and (2) export purchased items without detection by domestic law-enforcement officials.

To perform this investigation, we spoke with relevant agencies to gain an understanding of which dual-use and military items were in demand by terrorists and foreign governments. Furthermore, we identified publicly disclosed enforcement cases regarding the sale and illegal export of sensitive dual-use and military items. We searched for dual-use and military technology being sold on manufacturers' and distributors' Web sites. We then made domestic purchases of dual-use and military items either through e-mail or the seller's Web site. We did not purchase items from individual persons or commercial auction sites such as eBay or craigslist. We used a bogus front company and fictitious identities when purchasing these items, meaning that we conducted our work with fictitious names and contact information that could not be traced back to GAO. We also established a Web site related to our bogus company and rented domestic commercial mailboxes used to receive purchased items. In some cases, no information other than a name and credit card were used when purchasing a sensitive item. When possible, we obtained written price quotes from manufacturers and distributors for purchases of additional quantities of items we successfully purchased. After purchasing these items in an undercover capacity, we contacted the distributors and manufacturers of the items and informed them of our operation. We then interviewed company officials and performed additional follow-up investigative work. In addition, we coordinated with foreign government officials to covertly export a number of dummy versions of the items we purchased. We discussed the results of our work with officials at State and Commerce, as well as law-enforcement officials within the Department of Defense, DOJ, and the Department of Homeland Security (DHS).

[3]See GAO, *Internet Sales: Undercover Purchases on eBay and Craigslist Reveal a Market for Sensitive and Stolen U.S. Military Items*, GAO-08-644T (Washington, D.C.: Apr. 10, 2008).

We conducted our investigation from May 2008 through June 2009 in accordance with quality standards for investigations as set forth by the Council for Inspectors General on Integrity and Efficiency (CIGIE).

Background

Commerce and State are principally responsible for regulating the export of sensitive dual-use and military items, respectively. Under the authority of the Export Administration Act of 1979,[4] Commerce is responsible for regulating the export of dual-use items that are included in the Commerce Control List (CCL).[5] Specifically, Commerce's Bureau of Industry and Security (BIS) is responsible for regulating the export and reexport of most commercial items. The commercial items BIS regulates are referred to as dual-use items that have both commercial and military or proliferation applications. BIS's export enforcement activities target the most significant threats facing the United States such as the proliferation of weapons of mass destruction and missile delivery systems, terrorism and state sponsors of terror, and diversions of dual-use goods to unauthorized military end uses.

Under the authority of the Arms Export Control Act of 1976,[6] State regulates the export of military items, which are included in the U.S. Munitions List.[7] Generally, items regulated by State require an export license, while items regulated by Commerce do not necessarily require an export license. Whether an export license is required depends on multiple factors including the item being exported, country of ultimate destination, individual parties involved in the export, parties' involvement in proliferation activities, and the technical characteristics and planned end use of the item. Any person or company in the United States that engages

[4]Pub. L. 96-72, 93 Stat. 503, codified as amended at 50 U.S.C. app. §§ 2401–2420. The Act has lapsed and been reauthorized by statute and Executive Order several times. Currently, the Act is in force pursuant to Executive Order 13,222, 66 Fed. Reg. 44,025 (Aug. 22, 2001), which extended the application of the Act under the authority of the International Emergency Economic Powers Act (IEEPA), Pub. L. 95-223, Title II 91 Stat. 1626, codified as amended at 50 U.S.C. §§ 1701–1707. IEEPA provisions are renewed yearly through a presidential determination, the most recent occurring on July 25, 2008 (73 Fed. Reg. 43,603).

[5]The CCL is contained in Supplement No. 1 to Part 774 of the Export Administration Regulations (EAR), 15 C.F.R. § 774.1.

[6]Pub. L. 94-329, Title II, § 212(a)(1), 90 Stat. 744, codified as amended at 22 U.S.C. § 2778.

[7]The U.S. Munitions List is contained in Part 121 of the International Traffic In Arms Regulations (ITAR), 22 C.F.R. §§ 121.1 - .16.

in manufacturing, exporting, or importing U.S. Munitions List items must register with State.[8]

Commerce and State require exporters to identify items that are on the CCL and U.S. Munitions list and, if required, obtain license authorization from the appropriate department to export these items unless an exemption applies. Exporters are responsible for complying with export-controls laws and regulations. When shipping a sensitive dual-use or military item that requires a license, exporters are required to electronically notify DHS's Customs and Border Protection (CBP) officials at the port where the item will be exported, including information on the quantity and value of the shipment, the issued export license number, or an indication that the item is exempt from licensing requirements. Export enforcement agencies including CBP, ICE, the Federal Bureau of Investigation (FBI), Commerce's Office of Export Enforcement (OEE), U.S. Attorney's Office and the Defense Criminal Investigative Service, are involved with inspecting items to be shipped, investigating potential violations of export-control laws, and punishing export-control violators.

U.S. regulations are designed to keep specific military and dual-use items from being diverted to improper end users. However, current regulations focus on the export of these items and do not address the domestic sales of these items. The seller of a U.S. Munitions List item or a CCL item may legally sell the item within the United States, and is under no legal duty to perform any type of due diligence on a buyer. However, if the seller of an item knows or has reason to know that the buyer is representing a foreign government or intends to export the item, then the seller may be liable.[9]

[8]Export often involves the actual shipment of goods or technology out of the United States. Under ITAR, transfers of Munitions List "technical data" to foreign persons within the United States is also considered to be an export. 22 C.F.R. § 120.17(a)(4). Under EAR, release of CCL "technology" to foreign nationals within the United States is considered to be an export to the home country of the foreign national and thus may require an export license. 15 C.F.R. § 734.2(b).

[9]An otherwise legal transaction is prohibited if the seller knows an export violation will occur, pursuant to 15 C.F.R. § 736.2(b)(1) for CCL items and 22 C.F.R. § 127.1(2) for U.S. Munitions List items. Criminal liability may attach under 50 U.S.C. app. § 2410, 50 U.S.C. § 1705, 22 U.S.C. § 2778(c), or general statutes such as 18 U.S.C. § 371.

Sensitive Dual-Use and Military Items Can Be Easily Purchased within the United States Using a Bogus Front Company and Fictitious Identities

We found that sensitive dual-use and military technology can be easily purchased from manufacturers and distributors within the United States. Using a bogus front company and fictitious identities, we purchased[10] sensitive dual-use and military items from the sellers of the items. Based on our legal analysis of the applicable laws and regulations over the domestic sale of sensitive dual-use and military technology, we determined that companies are allowed to make domestic sales of sensitive items with little or no restrictions. Some of the manufacturers and distributors of items we purchased stated that they independently instituted procedures to document the sales of sensitive items, such as requiring buyers to fill out end-user agreements.[11] However, the sellers were not legally required to conduct any research to validate the authenticity of the identification used or the final use of the item. In addition, many of the distributors and manufacturers have received warning letters from Commerce for exporting sensitive items without the required export license.

Items obtained by our fictitious individuals included a night-vision monocular, electronic components used in IEDs, and secure military-grade radios used by U.S. Special Operations personnel. Items we obtained were not only sensitive in nature, but were also in demand by foreign governments and terrorist organizations. Specifically, seven of the sensitive dual-use and military items we obtained during our investigation have been the center of criminal indictments and convictions for violations of export control laws. All items, except the F-16 engine computer, were new and unused. The F-16 engine computer was purchased from a distributor who had obtained the item from the Department of Defense. Table 1 below summarizes the sensitive items we

[10]For several items, we obtained written price quotes in lieu of purchasing the items due to their costs. After obtaining the price quotes, we confirmed with the sellers of the items that our attempted purchases would have been successful once we had made payment arrangements for the items.

[11]End-user agreements refer to documents submitted by the buyer in which the buyer self-certifies the proposed use for the item being purchased, whether the buyer plans to export the item, and whether the buyer plans to resell the item.

obtained during our investigation, followed by detailed case-study narratives.[12]

Table 1: Sensitive Dual-Use and Military Items

Case	Items	Dual-use	Military	Nuclear	IED
Dual-use items					
1	Triggered spark gap	✓		✓	
2	Oscilloscope	✓		✓	
3	Accelerometer	✓	✓	✓	
4	Quadruple differential line receiver	✓	✓		✓
5	Inclinometer	✓	✓		✓
6	Gyro chip	✓	✓		
7	Ka-band power amplifier	✓	✓		
Military items					
8	Infra-red flag		✓		
9	Modular tactical vest (MTV) / enhanced small arms protective inserts (ESAPI)		✓		
10	Night-vision monocular / Night-vision goggles (NVG)		✓		
11	Secure personal radio		✓		
12	F-16 engine computer		✓		

Source: GAO.

Sensitive Dual-Use Items

Using a bogus front company, fictitious identities, and a domestic mailbox we rented, we were able to purchase sensitive dual-use items from distributors and manufacturers. Items that we purchased have commercial applications, but can also be used for other purposes such as in the development of nuclear weapons, guided missiles, and IEDs. The items listed below are subject to export restrictions under either the CCL or

[12]For item 2 (Oscilloscope) we obtained a written price quote in lieu of purchasing the item due to its cost. For the NVG in item 10, we found we could have purchased this same item from the same seller of the Night Vision Monocular. However, since we had purchased this item on previous work, we choose not to purchase this same item again. For item 9 (ESAPI) we found we could have purchased this item from the same seller as the MTV however, since we had purchased this item in previous work we choose not to purchase this same item again. After obtaining the price quotes, we confirmed with the sellers of the items that our attempted purchases would have been successful once we had made payment arrangements for the items.

State's U.S. Munitions List. Many of the items we purchased have also been the center of previously identified unlawful exports to foreign nations.

Sensitive Dual-Use Items with Nuclear Applications

- **Case 1: Triggered Spark Gap.** Triggered spark gaps are versatile high-voltage switches used for medical applications that can also be used as nuclear weapons detonators. Triggered spark gaps have been the center of unlawful exports to Pakistan and India. However, they are completely legal to buy and sell within the United States.

Figure 1: Triggered Spark Gap

Source: GAO.

In January 2009, using a bogus company and a domestic mailbox as a business address, we purchased, via e-mail, a triggered spark gap for the amount[13] of $735 from a manufacturer that is registered in the federal Central Contractor Registration (CCR) database, an approved government supplier via the General Services Administration (GSA) schedule, and a previous target for attempted purchases by foreign nationals. After

[13]Total amounts may include taxes, shipping and handling fees, and service fees.

obtaining the triggered spark gap, we notified the manufacturer of our undercover purchase. During our interview with the manufacturer, company personnel stated they believed that they had sufficient protocols in place to document the sale of their items. The manufacturer requires new customers to complete a certification form where the customer provides their name and the end use of the product they are purchasing. However, because sales of this item are legal domestically, we were able to purchase it with a fictitious name and bogus company, and by providing a valid credit card. With no requirement to do so, the manufacturer did not question our fictitious identity or bogus company and did not inquire further about the end use for our product. While purchasing the triggered spark gap, we also obtained a price quote for up to 100 additional triggered spark gaps. In addition, in 2005, an individual was sentenced to 3 years in prison for conspiring to violate and violating U.S. export restrictions after exporting, using an air freight company, items including triggered spark gaps. Another individual was indicted for conspiring to violate and violating U.S. export restrictions. The two individuals arranged to purchase, and export to Pakistan, several U.S.-origin triggered spark gaps. In order to obtain the triggered spark gaps the individuals falsely indicated that the items were intended for medical use.

- **Case 2: Oscilloscope.** Oscilloscopes are used for displaying the timing, voltages, frequency, and other attributes of electrical signals. In addition, certain oscilloscope versions are capable of being utilized in weapon of mass destruction development and are also export-controlled for antiterrorism reasons. However, oscilloscopes are legal to buy and sell within the United States. During our investigation, we determined that CCL versions of oscilloscopes can be purchased on the Internet from a distributor that is registered in CCR through an online purchase with a credit card. Because this item cost over $7,500, we chose not to purchase it. However, we confirmed with the distributor that we would have been able to purchase an oscilloscope domestically without any verification. In addition, a model of oscilloscope similar to the version we could have purchased was also illegally shipped overseas by the same seller in 2005. Specifically, this seller pled guilty to one felony count of violating the International Emergency Economic Powers Act by exporting an oscilloscope to Israel without a license. This distributor was sentenced to pay a criminal fine in the amount of $50,000, placed on 3 years' probation and ordered to serve 250 hours of community service. In recent years, the oscilloscope manufacturer has received several warning letters from Commerce for exporting oscilloscopes to Pakistan and India without the required license.

- **Case 3: Accelerometer.** Accelerometers are sensors and instruments used for measuring, displaying, and analyzing acceleration and vibration. They can be used on a stand-alone basis, or in conjunction with a data-acquisition system. The version of the accelerometer we purchased is suitable for use in "smart" bombs and for measuring motions generated by nuclear and chemical explosives and, although legal for domestic sale, is export-controlled under CCL restrictions. In January 2009, we purchased an accelerometer from a manufacturer for the amount of $2,766. The manufacturer is registered in CCR and is an approved government supplier through the GSA Schedule. We accomplished the purchase using a fictitious name, bogus company, and domestic mailbox as a business address. We also provided an end-user certification stating that we would use the item for research and development purposes and would not export the item. We met with the manufacturer after our purchase to discuss what we had done and to discuss whether the company implemented any voluntary restrictions over the domestic sales of sensitive items. The manufacturer of the item did not implement controls that are not required by law, and believed that documentation of the sale was appropriate. This type of item is in high demand by foreign countries. For example, a 2007 undercover investigation by ICE revealed that an individual attempted to purchase and illegally export the same type of accelerometer we purchased to China. Specifically, ICE used an undercover company to capture the individual. The individual was sentenced 12 months in prison for his role in conspiring to export the accelerometer.

Dual-Use Items with IED applications

- **Case 4: Quadruple Differential Line Receiver.** The quadruple differential line receiver is used for balanced or unbalanced digital data transmission. The product supports defense, aerospace, and medical applications. In addition, certain versions of quadruple differential receivers have military applications. This item may be legally bought and sold within the United States. In April 2009, we purchased 10 military-grade quadruple differential line receivers from a distributor for the amount of $248. The transaction was accomplished through the company's Internet Web site using a bogus company, fictitious identity, and domestic mailbox as a business address. Because the law did not mandate it, no verification of our identity or description of the use of the product was required. After the purchase we notified the distributor of our undercover purchase. As a result of our undercover purchase, the distributor stated it will consider implementing voluntary controls for the online transactions, but did not provide details on what additional controls it would implement. In addition to our purchase, other individuals have attempted to export a similar item to Iran. Specifically, in 2008, various individuals and companies were indicted on federal charges for purchasing items for IEDs including items similar to a quadruple differential line receiver. The individuals allegedly arranged to export items to multiple transshipment

points, with Iran being the final destination. In addition, we spoke with a Department of Defense official who confirmed similar U.S.-made technology is being found in IEDs. The official stated that terrorist groups are using more advanced IEDs with easy access to this type of technology.

- **Case 5: Inclinometer.** An inclinometer is an instrument used for measuring angles of slope and inclination of an object with respect to its center of gravity. Inclinometers, which are export-controlled but legal to buy and sell within the United States, are suitable for use in the military, medical, optical, range-finder, and robotics fields, and have applications in IEDs. In February 2009, we purchased an inclinometer from a manufacturer for the amount of $548. The manufacturer is registered in CCR and has recently been the target for purchases by individuals shipping inclinometers to Iran. Because it was a domestic purchase, the manufacturer was not required to request an end-user agreement, or question our identity, company, or that our business address was a mailbox. While purchasing the inclinometer, we also obtained a price quote for up to 40 additional inclinometers. In addition, after the purchase we notified the manufacturer of our undercover purchase. When interviewed, the manufacturer correctly stated that he did not identify any Commerce-identified red flags from the undercover transaction.[14] In addition, in 2008, various individuals and companies were indicted on federal charges for purchasing items for IEDs and exporting inclinometers to Iran. Specifically, in 2007, the individuals allegedly purchased inclinometers from the same manufacturer we purchased inclinometers from, and shipped them to multiple transshipment points, with Iran being the final destination.

Other Dual-Use Items

- **Case 6: Gyro Chip.** Gyro chips are sensitive dual-use items used in advanced aircraft, missile, space, and commercial systems for stabilization, control, guidance, and navigation. The gyro chip's original intent was for commercial use; however, this same item is also used to stabilize and steer guided missiles. For this reason, the item is export-controlled, but may be legally bought and sold within the United States without restriction. The device is fully self-contained, extremely small, lightweight, and has virtually unlimited life.

[14]Commerce's BIS publishes a list of "Red Flag Indicators" that may indicate a transaction could lead to a violation of the Export Administration Regulations. A seller who finds a red flag is encouraged to report it to Commerce. Examples of red flags include situations where the item purchased does not fit with the buyer's line of business, the buyer is willing to pay cash for an expensive item where financing is the norm, or the buyer has little or no business background. The full list is available at http://www.bis.doc.gov/enforcement/redflags.htm.

Figure 2: Gyro Chip

Source: GAO.

In February 2009, we purchased a gyro chip from a manufacturer that is registered in CCR for the amount of $3,146. During the purchase process the manufacturer made it clear that the item is subject to ITAR, and if exported would be subject to export restrictions. During the undercover purchase we provided our bogus company's Web site address, listed a domestic mailbox as a business address, and completed a falsified end-user agreement. While purchasing the gyro chip, we also obtained a price quote for an additional 10 gyro chips. In addition, after the purchase we notified the manufacturer of our undercover purchase. We then interviewed the manufacturer, which stated that it conducts extensive training of its personnel on export regulations of items it sells, attends export-regulation conferences, hires export consultants, and conducts internal training to sales representatives on specific procedures to follow while quoting or selling products. However, no validation procedures are required when a domestic sale is made, and therefore the manufacturer did not identify our fictitious identity and company. In addition, in a previous case, State charged a different company with shipping 85 commercial jets overseas many of which went to countries including

China with a gyro chip embedded in the flight control systems. In April 2006, the company agreed to pay $15 million to settle the allegations.[15]

- **Case 7: Ka-Band Power Amplifier.** Ka-band power amplifiers are suited for military radar systems, ground terminals for Ka-band satellite communications systems, and point-to-point communication systems. Ka-band power amplifiers are export-controlled for national security reasons, but legal to buy and sell within the United States. In March 2009, we purchased two Ka-band power amplifiers from a distributor for the amount of $227. The distributor is registered in CCR and was a previous target for purchases by individuals shipping amplifiers to China. Our purchase was made via e-mail and the Internet using a fictitious identity, bogus company, and domestic mailbox as a business address, and by providing an end-user agreement. We completed the agreement using bogus information and stating we would not export the item without obtaining an export license. Because there are no restrictions on the domestic sale of this item, no additional documentation procedures or validation was performed by the distributor prior to our purchase. While purchasing the Ka-band power amplifiers, we also obtained a price quote for up to 99 additional amplifiers. In addition, after the purchase we notified the distributor of our undercover purchase. When we interviewed distributor personnel, they stated their documentation procedures require the customer to complete an end-user agreement; however, they correctly stated they are not required to do this for domestic sales. In 2009, an individual was indicted for exporting several controlled items including this Ka-band power amplifier to China without an export license. Specifically, on three occasions the individual allegedly had someone in the United States ship several controlled items to China, and in one occasion the individual hand-carried the items when flying from the United States to China. In recent years, Commerce issued warning letters to the manufacturer for exporting electronics to China, failure to comply with a license condition, and exporting amplifiers to Germany for sale to China without the required export license.

Sensitive Military Items

Using a bogus front company, fictitious identities, and a domestic mailbox as our business address, we were able to purchase or otherwise obtain sensitive military items from distributors and manufacturers without

[15]Specific gyro chips are subject to the export licensing jurisdiction of State's Directorate of Defense Trade Controls, unless these specific gyro chips are integrated into and included as an integral part of a commercial primary or standby instrument system. If included as an integral part of a commercial primary or standby instrument system, these specific gyro chips are subject to the CCL.

detection. Some of the items we obtained are subject to State's U.S. Munitions List and have been at the center of unlawful export plots by foreigners. After purchasing and receiving the sensitive military items, we interviewed the sellers regarding the controls they have in place for the sales of their respective items.

- **Case 8: Infra-Red (IR) Flag.** IR flags[16] are currently in use by U.S. military forces to help identify friendly soldiers during nighttime operations. Several of the IR flags we purchased appear as a black material with no identifying markers. However, with the use of U.S. military night-vision technology (such as the monocular we purchased in case 10 below), the patches reveal a U.S. flag, and are the same IR flags used on U.S. military combat uniforms. An enemy fighter wearing these IR flags could potentially pass as a friendly service member during a night combat situation, putting U.S. troops at risk. Nevertheless, these items are completely legal to buy and sell within the United States.

Figure 3: IR Flags

Source: GAO.

[16]The IR flags are also known as IFF (identification of friend or foe) IR U.S. flags.

In September 2008, we purchased various U.S. IR flags from a distributor for the amount of $78. The company's Internet storefront states it specializes in designing modified battle dress uniforms and other military uniform accessories used by modern-day warriors. Specifically, the company's Web site states that Special Forces in Iraq and Afghanistan currently use many of their products. Although there is no legal requirement to do so, the distributor's Internet site stated that the company checks for military identification; however, the seller failed to request identification from our undercover investigator. In the end, our fictitious buyer was only required to provide a name, credit card, and domestic address for shipment to purchase these items. After purchasing and receiving the IR flags, we also obtained a price quote for an additional 400 IR flags. In addition, after the purchase we notified the distributor of our undercover purchase. When interviewed, the distributor of the IR flags stated that it always requests for a copy of a military ID as part of his own voluntary policy and has minimal voluntary controls in place over the sale of the IR tabs. However, the distributor did not request a copy of a military ID as part of our purchase. In addition, we interviewed the distributor's supplier (manufacturer); the manufacturer stated that the distributor is required by their distributorship agreement to ask for a military ID. As a result of this lapse, the manufacturer stated that the distributor will no longer be authorized to sell the IR flags.

- **Case 9: Modular Tactical Vest (MTV) and Enhanced Small Arms Protective Inserts (ESAPI).** The MTV we purchased is a type currently being used by U.S. military personnel and have been tested to National Institute of Justice[17] Level IIIA[18] 9mm velocity. Enemies of the United States could use the vest during attacks against American and coalition forces, and they could also be used by criminals within the United States and on the United States–Mexico border. However, the item is completely legal to sell, buy, or possess within the United States, except by certain violent felons. ESAPIs are ceramic plates that are thicker than the normal SAPIs and increase the protection. These types of ESAPIs are suited for use in the MTV we purchased. The combination of these items could give terrorists or criminals an advantage and protection in combat situations. In September 2008, we purchased an MTV of the type currently in use by

[17]The U.S. Justice Department has created standards of body armor known as the N.I.J. (National Institute of Justice) Standard 0101.06.

[18] Level IIIA is usually the highest threat level in soft body armor. It is usually worn as overt-style armor because of the weight and thickness of the ballistic panels.

the U.S. Marine Corps in Iraq and Afghanistan from a distributor for the amount of $2,417. The distributor is an approved government supplier through the GSA schedule. We purchased the MTV from the distributor's Internet Web site. Although legally not required to do so, the distributor's Web site states that it requires a military ID and completes a verification process before the sale of the equipment. However, we were able to bypass their voluntary requirements using a fictitious military ID. After purchasing and receiving the MTV, we also obtained a price quote for an additional 20 MTVs. In addition, we found that we could have purchased new ESAPI plates, from the same distributor through the same process, which fit into the MTV we purchased. The addition of the e-SAPI plates would have increased the effectiveness of our vest. We chose not to purchase the ESAPI plates because we had purchased similar plates in our prior work.[19] After the purchase, we notified the distributor of our undercover purchase. The distributor stated that it has several voluntary controls in place. Specifically, for our transaction it noticed that the shipping address and billing address were different; therefore, it called the credit card company to verify that the credit card was valid, thinking that would be sufficient to verify that the undercover customer was not bogus. In the past, this distributor has received a warning letter from Commerce for exporting police equipment without the required export license. In addition, the MTV manufacturer was fined $65,000 for the export of military items to Kuwait, Chile, Oman, Trinidad and Tobago, and Saudi Arabia without the required export license.

- **Case 10: Night-Vision Monocular and Night-Vision Goggles (NVG).** The night-vision monocular is a lightweight, self-contained, image-intensification system capable of being either hand-held, mounted to a small arms weapon mounting rail, or mounted to a head mount or helmet mount. Night-vision monoculars are used in nighttime operations by U.S. forces to provide a tactical advantage on the battlefield. They are legal to buy and sell within the United States.

[19] GAO-08-644T.

Figure 4: Night-Vision Monocular

Source: GAO.

In November 2008, we purchased a night-vision monocular of a type that is currently in use by the U.S. military from a distributor that is registered in CCR, for $3,600. The purchase was made using a fictitious identity, bogus company, and domestic mailbox as a business address. During our undercover purchase, the seller certified our bogus company to be a distributor of the item by signing a dealer/reseller agreement. This allowed us to circumvent the seller's voluntary restrictions on only selling the items to military and law-enforcement agencies. As a result, we could have obtained a substantial number of night vision monoculars as part of this agreement. In addition, we also found that we could have purchased new military-specification NVGs, from the same distributor through the same process. We chose not to purchase the NVG because we had purchased a similar NVG in our prior work.[20] After the purchase we notified the distributor of our undercover purchase. When we interviewed distributor personnel, they stated that they have controls in place that are required for the sale of night-vision technology as a part of the distributor agreement. The distributor correctly stated that it is the reseller/dealer's

[20]GAO-08-644T.

responsibility, if exporting an item, to request and obtain export licenses for the subject items and to ensure that the requirements of all applicable export laws and regulations are met. Night-vision technology has been in demand by entities in countries like China, Singapore, Indonesia, Iran, and Hong Kong. For example, on November 14, 2006, BIS issued a Section 11(h) Denial Order against two individuals in connection with their criminal convictions for conspiring to export Commerce- and State-controlled night-vision devices to the terrorist group Hezbollah in Lebanon.

- **Case 11: Secure Personal Radio (SPR).** According to the SPR distributor, the SPR model we obtained, which is being used by U.S. Special Forces personnel, is the latest model with enhanced digitally encrypted capability that has a low probability of detection without the aid of high-tech military radio-interception equipment. The SPR provides secure communications between battlefield personnel with an encryption feature that makes communicating with the radio virtually undetectable. Nevertheless, the item is legal to buy and sell within the United States. In November 2008, we obtained two SPRs with headsets and accessories along with one microphone headset on a loan from a distributor. Specifically, the company loaned, at no cost, our bogus company the two radios for demonstration purposes with the possibility for the undercover company to become a distributor of the SPR radios. The company also offered our undercover investigator a job selling the equipment on a commission basis. Because there are no domestic restrictions on these radios, the company only asked for a copy of a driver's license prior to loaning the radios. After the transaction, we made the distributor aware of the fictitious identity. The distributor acknowledged that it should have shown more voluntary due diligence prior to loaning the radios to our undercover investigator. The distributor stated that it requires an end-user agreement and a copy of identification for documentation purposes, but it performs no other voluntary verification checks. The distributor stated it often receives inquiries from foreign individuals and estimated as much as 30 percent of individuals that register on its Web site are foreign. The distributor told us that it informs these individuals it only sells domestically to military and law-enforcement entities.

- **Case 12: F-16 Engine-Monitoring System Computer (EMSC).** F-16 EMSC processes digital engine-performance signals from the digital electronic-control module. This EMSC is used in more than 75 percent of the USAF's single-engine F-16 Block 50/52 aircraft. Furthermore, the engine that uses this monitoring system is also qualified for use on the F-15 Strike Eagle aircraft and was recently chosen by South Korea to power its new F-15K fighters. This item is export-controlled under ITAR, but is

legal to buy and sell within the United States. In April 2009, using a fictitious identity and bogus company, we purchased, through e-mail, a used F-16 EMSC from an online distributor for the total amount of $570. The distributor had obtained this item from DOD. During the purchase process, we provided a bogus company name, a domestic mailbox as a business address, a copy of our fictitious person's driver license, and a falsified end-user agreement. After obtaining the F-16 EMSC, we notified the seller of our undercover purchase. During our interview with the seller, the official correctly stated that the seller is not required to have any controls in place for the domestic sale of this item; however, for its own voluntary due diligence the seller ran a public-records check on our fictitious person, but did not identify the purchase as suspicious. In recent years, several individuals and companies have been sentenced to probation and received fines in connection with illegal exports of aircraft components to Iran and Libya. In addition to the United States and its allies' fleets of F-16 aircraft, Venezuela's military also has a fleet of F-16s and has recently issued public statements suggesting the country may want to sell its fleet of F-16s to Iran.

Sensitive Dual-Use and Military Items Can Be Easily Exported

We were able to export, without detection by U.S. enforcement officials, a number of dummy versions of sensitive dual-use and military items to a country that is a known transshipment point for terrorist organizations and foreign governments attempting to acquire sensitive technology. Due to the large volume of packages being shipped overseas, large volume of people traveling overseas, and various agencies[21] involved in enforcing export controls, U.S. enforcement officials stated it is impossible to search every package and person leaving the United States to ensure sensitive dual-use and military items are not being exported illegally. The combined effect of the lack of restrictions over domestic sales and the ease of illegal export of these items is that sensitive dual-use and military items can be easily purchased and exported by terrorists or foreign governments without detection.

In order to export our items, we first obtained nonfunctional "dummy" versions of the items through cooperation with the manufacturers. Next, in cooperation with foreign law-enforcement officials, we shipped the items, using commercial mail, in nondescript boxes that did not disclose the true contents of the items contained within the package. The boxes passed

[21]See GAO, *Export Controls: Challenges Exist in Enforcement of an Inherently Complex System,* GAO-07-265 (Washington, D.C.: Dec. 20, 2006).

through U.S. customs controls without being inspected. The location we shipped the items to was a known transshipment point for items being sent to terrorist organizations and other foreign governments. After receiving the unopened packages, the foreign law-enforcement officials shipped the items back to the United States.

When we discussed our covert shipments with State, Commerce, and various law-enforcement agencies responsible for monitoring packages, vehicles, and persons exiting the United States, they were not surprised by our success. Officials from several agencies stated that there is no practical way to ensure that otherwise unsuspicious people, vehicles, or packages leaving the United States that carry or contain export-controlled items can be identified and searched consistently. Officials from Commerce stated that they were aware of similar schemes used by real individuals attempting to illegally export controlled items. In addition, officials from State stated they have programs in place, working in coordination with other government agencies such as ICE, designed to educate manufacturers and distributors about laws and common risks associated with sales of sensitive technology. However, State agreed that it is difficult to prevent items from leaving the country after they are legally sold to an individual within the United States.

Conclusions

A comprehensive network of controls and enforcement is necessary to ensure sensitive technology does not make it into the hands of unauthorized individuals. However, the lack of legal restrictions over domestic sales of these items, combined with the difficulties associated with inspecting packages and individuals leaving the United States, results in a weak control environment that does not effectively prevent terrorists and agents of foreign governments from obtaining these sensitive items. The key to preventing the illegal export of these sensitive items used in nuclear, IED, and military applications is to stop the attempts to obtain the items at the source, because once sensitive items make it into the hands of terrorists or foreign government agents, the shipment and transport out of the United States is unlikely to be detected.

Mr. Chairman, this completes my prepared statement. I would be happy to respond to any questions you or other Members of the subcommittee may have at this time.

Appendix I: Scope and Methodology

To perform the undercover test of purchasing sensitive dual-use and military items from manufacturers and distributors in the United States we spoke with relevant agencies and used publicly disclosed enforcement cases regarding the sales and illegal exports of sensitive dual-use and military items. GAO used the information obtained from these sources to determine which sensitive items were in demand by terrorists and foreign governments. We also reviewed the export regulations to determine that manufacturers and distributors are not required to have controls for the domestic sales of sensitive items. We searched for dual-use and military technology being sold on manufacturers' and distributors' Web sites. We then made domestic purchases of dual-use and military items either through e-mail, personal contact, or the seller's Web site. We used a bogus front company, fictitious identities, and domestic mailboxes as our business address when purchasing these items, meaning that we conducted our work with fictitious names and contact information that could not be traced back to GAO. We also established a Web site related to our bogus company and rented domestic commercial mailboxes used to receive purchased items. The bogus company used was incorporated to add more credibility. In some cases, during the purchase process, no information other than a name and credit card were used to purchase a sensitive item. In other cases, we submitted falsified end-user agreements stating the end use of the product and agreeing not to export the sensitive item. On one occasion, we provided a local military unit as the end use of the item and a fictitious military ID we created using commercial computer software. After we purchased the sensitive items, when possible, we obtained written price quotes from manufacturers and distributors for purchases of additional quantities of items we successfully purchased. After successfully purchasing these items in an undercover capacity, we contacted the distributors and manufacturers of the items and informed them of our operation. We did not attempt to purchase items from individual persons or commercial auction sites such as eBay or craigslist. Of the sensitive items disclosed we did not purchase the oscilloscope, enhanced small arms protective inserts, and the night-vision goggles. For these items we obtained written price quotes in lieu of purchasing the items due to their costs or due to the fact we had purchased the item in previous work. After obtaining the prices quotes, we confirmed with the seller of the items that our purchases would have been successful once we had made payment arrangement for the items.

To attempt to export purchased items without detection by domestic law-enforcement officials, we coordinated with foreign government officials to covertly export items out of the United States. We shipped the items to a destination known to be a transshipment point for terrorist organizations

and other foreign governments. We were able to export a number of items. The export process consisted of mailing the dummy versions of items from the United States through commercial package shipment. We falsified the shipment documents provided with the package. When the foreign government officials received the shipment they received specific instructions on how to inspect the shipment to verify that the package was sealed and was not opened or inspected by any U.S. officials. The foreign government officials also received special instructions on how to mail the package to GAO. GAO successfully received all items back from foreign law enforcement officials. We briefed officials at the Departments of State and Commerce, as well as law-enforcement officials within the Departments of Defense, Homeland Security, and Justice on the results of our work and incorporated their comments concerning controls over exported items.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper