United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on National Security and Foreign Affairs, Committee on Oversight and Government Reform, U.S. House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
April 10, 2008

INTERNET SALES

Undercover Purchases on eBay and Craigslist Reveal a Market for Sensitive and Stolen U.S. Military Items

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

DRAFT

DRAFT

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-08-644T, a testimony before the Subcommittee on National Security and Foreign Affairs, Committee on Oversight and Government Reform, House of Representatives

INTERNET SALES

Undercover Purchases on eBay and Craigslist Reveal a Market for Sensitive and Stolen U.S. Military Items

Why GAO Did This Study

Unauthorized individuals, companies, terrorist organizations, and other countries continue their attempts to obtain sensitive items related to the defense of the United States. The Internet is one place that defense-related items can be purchased, raising the possibility that some sensitive items are available to those who can afford them. In addition to the risk that sensitive defense-related items could be used to directly harm U.S. service members or allies on the battlefield, these items could be disassembled and analyzed (i.e., reverse engineered) to develop countermeasures or equivalent technology.

Given the risks posed by the sale of sensitive defense-related items to the public, and the Internet's international reach and high volume of commerce, the Subcommittee asked GAO to conduct undercover testing to determine whether the general public can easily purchase these items on the Internet, including on the Web sites eBay and Craigslist.

To perform this work, GAO investigators used undercover identities to pose as members of the general public, meaning that they conducted their work with names, credit cards, and contact information that could not be traced to GAO. Investigators interviewed sellers where possible and referred cases to the appropriate law enforcement entities for further investigation.

To view the full product, including the scope and methodology, click on GAO-08-644T. For more information, contact Gregory D. Kutz at (202) 512-6722 or kutzg@gao.gov.

What GAO Found

GAO found numerous defense-related items for sale to the highest bidder on eBay and Craigslist. A review of policies and procedures for these Web sites determined that there are few safeguards to prevent the sale of sensitive and stolen defense-related items using the sites. During the period of our investigation, GAO undercover investigators purchased a dozen sensitive items on eBay and Craigslist to demonstrate how easy it was to obtain them. Many of these items were stolen from the U.S. military. According to the Department of Defense (DOD), it considers the sensitive items GAO purchased to be on the U.S. Munitions List, meaning that there are restrictions on their overseas sales. However, if investigators had been members of the general public, there is a risk that they could have illegally resold these items to an international broker or transferred them overseas.

Examples of Sensitive Items Purchased by Undercover Investigators

No.	Item	Web site	Notes
1	F-14 antenna waveguide	eBay	▪ F-14 parts are in demand by Iran, the only country with operating F-14s ▪ Winning bidders on other auctions held by the seller were located in countries such as Bulgaria, China (Hong Kong), and Russia
2	Nuclear biological chemical gear	Craigslist	▪ Could be reverse engineered to develop countermeasures or produce equivalent technology ▪ Stolen military property
3	Enhanced small arms protective inserts	eBay	▪ Body armor plates manufactured in June 2007 and currently in use by troops in Afghanistan and Iraq ▪ Winning eBay bidders on similar military body armor items included individuals in China (Hong Kong), Taiwan, and Singapore ▪ Stolen from either the U.S. military or the manufacturer

Source: GAO.

GAO investigators also identified numerous examples of U.S. government property that was stolen and sold for a profit rather than being utilized by DOD. For example, GAO found two civilian store owners who acted as conduits for defense-related property that was likely stolen from the military. According to records, they purchased gear from service members—including Kevlar helmets, flak jackets, and flight suits—and sold it through eBay to the general public. GAO also purchased stolen military meals, ready-to-eat (MRE) and found a robust market for stolen military MREs on eBay and Craigslist.

Advertisements for the sensitive and stolen military items GAO purchased were not removed by Web site administrators, allowing investigators to buy the items. Both Web sites maintain lists of items that are prohibited from sale, including stolen items, but only eBay contains warnings related to overseas sales and the improper sale of sensitive defense-related items.

DRAFT

Mr. Chairman and Members of the Subcommittee:

Unauthorized individuals, companies, organizations, and other countries continue their attempts to obtain sensitive items related to the defense of the United States. For example, a 2003 undercover investigation by Immigrations and Customs Enforcement (ICE) revealed that an individual in Florida attempted to purchase and illegally export roughly $750,000 worth of U.S. F-14 fighter jet components to the Iranian military. According to the indictment, the individual planned to ship these components through other countries, including Italy, to conceal Iran as the ultimate destination. As we have reported before, Iran's acquisition of F-14 parts could threaten national security. In another example, ICE agents arrested a Columbian national in 2005 for attempting to illegally export 80 AK-47 assault rifles, an M-60 machine gun, and an M-16 machine gun to the Autodefensas Unidas de Colombia, a U.S.-designated terrorist organization.

Although it is not illegal to buy and sell some defense-related items domestically, many sensitive items are manufactured strictly for military purposes and were never meant to be a part of everyday American life. The Department of Defense (DOD) assigns demilitarization codes (demil codes) to some items so that, when they are no longer needed by the military, the items can be recognized and rendered useless for their intended purpose prior to leaving government control. We are defining *sensitive defense-related items* as those items that, if acquired by DOD, would have to demilitarized before disposal—a process that could involve everything from removing a sensitive component to destroying the item entirely. Our prior reports found that control breakdowns at DOD allowed members of the general public to acquire sensitive defense-related items, including F-14 parts, from the Government Liquidation Web site; these items had not been demilitarized properly.[1] Although DOD has made improvements in the management of its excess property system, saving millions of dollars and reducing the likelihood that

[1]The Government Liquidation Web site is the mechanism the Defense Logistics Agency (DLA) uses to sell items from its excess property system to the general public. See GAO, *Sales of Sensitive Military Property to the Public*, GAO-07-929R (Washington, D.C.: July 6, 2007); GAO, *DOD Excess Property: Control Breakdowns Present Significant Security Risk and Continuing Waste and Inefficiency*, GAO-06-943 (Washington, D.C.: July 25, 2006); GAO, *DOD Excess Property: Management Control Breakdowns Result in Substantial Waste and Inefficiency*, GAO-05-227 (Washington, D.C.: May 13, 2005); and GAO, *DOD Excess*

sensitive items are improperly sold, concerns remain that members of the general public can acquire sensitive defense-related items through additional weaknesses involving the government's acquisition, use, storage, and sale of these items.

The Internet is one place that defense-related items can be purchased, raising the possibility that some sensitive items are available to those who can afford them. In addition to the Government Liquidation Web site, many military surplus stores across the United States have Web pages with online ordering capability. Furthermore, Web sites such as eBay and Craigslist are popular because they allow sellers to advertise individual items and appear to provide some element of anonymity. For the most part, these Web sites have an international reach—meaning that it is possible for sellers to identify buyers in foreign countries and quickly export purchased items. Sellers use eBay to auction goods or services, receive bids from prospective buyers, and finalize a sale. eBay also features "store fronts" in which property is listed and bought without going through a bidding process. In contrast, Craigslist functions as an automated version of the newspaper classifieds, listing jobs, housing, goods, services, personals, activities, advice, and just about anything users wish to sell, advertise, or promote. The service is community-based and moderated, operating in 450 cities worldwide, and is largely free of charge.

While potential buyers for some sensitive items certainly include hobbyists, military enthusiasts, and emergency response or law enforcement units, the ICE cases clearly show the real risk that illegal weapons brokers, terrorists, and unauthorized agents of foreign governments also number among potential buyers. In addition to the risk that sensitive defense-related items could be used directly against U.S. interests, some items could be disassembled and analyzed to determine how they work. This technique, known as reverse engineering, could allow the creation of (1) countermeasures to defeat or minimize the military significance of the item or (2) the development of an equivalent item that could be used against U.S. interests.

Given the risks posed by the sale of sensitive defense-related items to the public, and the Internet's international reach and high volume of commerce, you asked us to conduct undercover testing to determine whether the general public can easily purchase these items on the Internet, including on the Web sites eBay and Craigslist.

To perform this investigation, we searched for certain target items on eBay and Craigslist. When these items were identified, investigators attempted to purchase them—either through bidding or a direct purchase (eBay) or by contacting the seller and arranging an in-person meeting or sale via U.S. mail (Craigslist). Investigators used undercover identities to pose as members of the general public when purchasing these items, meaning that they conducted their work with names, credit cards, and contact information that could not be traced back to GAO. In the case of eBay purchases, investigators worked with eBay's Fraud Investigation Team (FIT) to obtain information regarding the identity and account history of the sellers. We also searched the DOD Employee Interactive Data System (DEIDS) database to determine whether sellers were active members of the U.S. military. Where applicable and feasible, investigators interviewed the sellers and performed additional follow-up investigative work or, in some instances, made immediate referrals of the cases to field agents of the appropriate law enforcement entities.

After purchasing a questionable item, our investigators matched the National Stock Number (NSN) on the item to those listed in DOD's Federal Logistics System (FedLog) to validate that it met our definition of a sensitive defense-related item.[2] We also spoke with officials from the Defense Criminal Investigative Service (DCIS), Demilitarization Coding Management Office (DCMO), the Air Force Office of Special Investigations (Air Force OSI), and the Army Criminal Investigation Division (Army CID) regarding the sale of U.S.

Agents, GAO-04-15NI (Washington, D.C.: Nov. 19, 2003).

[2]An NSN is a 13-digit number that identifies standard use inventory items. The first 4 digits of the NSN represent the Federal Supply Classification, such as 8430 for men's footwear, followed by a 2-digit North Atlantic Treaty Organization (NATO) code and a 7-digit designation for a specific type of boot, such as cold weather boot. FedLog is the logistics information system published by the Defense Logistics Information Service (DLIS). FedLog lists demil codes that should be taken for each property item, which differ by property type.

military property. We referred pertinent information to DCIS, Army CID, and Air Force OSI for further investigation. We also spoke with officials from eBay and Craigslist about the policies and procedures governing commerce on their Web sites and performed legal research.

We conducted our investigation from January 2007 through March 2008 in accordance with quality standards for investigations as set forth by the President's Council on Integrity and Efficiency. It is important to note that our investigation does not represent a comprehensive assessment of all sensitive defense-related items sold through these Web sites during this period. Rather, our report provides only a "snapshot" of some items that investigators identified and purchased. Further, we did not attempt to perform a comprehensive audit or analysis to determine whether systemic property-management problems at DOD ultimately resulted in the sale of these items on the Internet during this period. As a result, our investigation of sellers was limited, in most cases, to their claims regarding how they obtained the items. We also did not test the government's enforcement of export controls by attempting to transfer what we purchased overseas, or validate whether eBay and Craigslist sellers we identified actually exported items to other countries.

Summary of Investigation

We found numerous defense-related items for sale to the highest bidder on eBay and Craigslist from January 2007 through March 2008. A review of eBay and Craigslist policies and procedures determined that, although these Web sites have taken steps to regulate their user communities and define items that are prohibited from sale, there are few safeguards to prevent sensitive and stolen defense-related items from being sold to either domestic or foreign users of these sites. During the period of our investigation, undercover investigators purchased a dozen sensitive items to demonstrate how easy it was to obtain them. The items were shipped to us "no questions asked." Many of these items were stolen from the U.S. military. According to DOD, it considers the sensitive items we purchased to be on the U.S. Munitions List, meaning that there are restrictions

on their overseas sales. However, if investigators had been members of the general public, there is a risk that they could have illegally resold these items to an international broker or transferred them overseas. Many of the sensitive items we purchased could have been used directly against our troops and allies, or reverse-engineered to develop countermeasures or equivalent technology. For example, we purchased:

- Two F-14 components from separate buyers on eBay. Given that the United States has retired its fleet of F-14s, these components could only be used by the Iranian military. By making these parts available to the general public, the eBay sellers provided an opportunity for these parts to be purchased by an individual who could then transfer them to Iran. The continued ability of Iran to use its F-14s could put U.S. troops and allies at risk. We were unable to determine where the sellers obtained the F-14 parts, and we found that ICE had an open investigation of one of the sellers.

- Night vision goggles containing an image intensifier tube made to military specifications (milspec) that is an important component in the U.S. military's night-fighting system. Although night vision goggles are commercially available to the public, the milspec tube in the pair of goggles we purchased on eBay is a sensitive component that allows U.S. service members on the battlefield to identify friendly fighters wearing infrared (IR) tabs. We also purchased IR tabs from a different Internet seller. These IR tabs work with the goggles we purchased, giving us access to night-fighting technology that could be used against U.S. troops on the battlefield.

- An Army Combat Uniform (ACU) and uniform accessories that could be used by a terrorist to pose as a U.S. service member. After a January 2007 incident in which Iraqi insurgents, dressed in U.S. military uniforms, entered a compound in Karbala and killed five U.S. service members, DOD issued a bulletin declaring that all ACUs should be released only "to Army, Navy, Air Force, Marines and their Guard or Reserve components." We purchased the ACU on eBay in April 2007, after

DOD's bulletin had been issued. The ACU we purchased also came with IR tabs, which could have allowed an enemy fighter to pose as a "friendly" during night combat. The seller represented to us that he obtained the ACU at a flea market near Fort Bragg, North Carolina. This ACU appears to be stolen military property.

- Body armor vests and Small Arms Protective Inserts (SAPI), including advanced Enhanced SAPI (E-SAPI) plates that are currently used by our troops in Iraq and Afghanistan. Unauthorized individuals, companies, terrorist organizations, or other countries could use reverse engineering on this body armor to develop countermeasures, equivalent technology, or both. Body armor could also be used domestically by a violent felon to commit crime. The body armor vests, SAPIs, and E-SAPIs, which we purchased from eBay and Craigslist sellers, appear to have been stolen from DOD.

In addition to the above case studies, our investigators identified numerous examples of U.S. government property that was stolen and sold for personal profit rather than being utilized by DOD (i.e., conversion of government property). According to DOD officials, U.S. military personnel are not authorized to sell certain items that have been issued to them, such as body armor; doing so is considered theft of government property. Although not all of the stolen property items available on eBay and Craigslist were sensitive, each item was purchased with taxpayer money and represents a waste of resources because it was not used as intended. For example, we found two civilian store owners who acted as conduits for defense-related property that was likely stolen from the military. According to records they gave us, these store owners purchased gear from service members—including Kevlar helmets, flak jackets, gas masks, and ACUs—and sold it through eBay to the general public. We also investigated sales of military meals, ready-to-eat (MRE) and found a robust market for stolen military MREs on eBay and Craigslist. Both civilians and service members sold us numerous cases of new/unused military MREs despite the fact that they were marked "U.S. Government Property, Commercial Resale Is Unlawful." Because the military MREs we bought had been originally purchased by the government for use by U.S. troops, we conclude that these

MREs were stolen from DOD. For example, we found that an active duty Army Private First Class stationed in South Korea stole military MREs from a warehouse and sold them to us on eBay. After our referral, Army CID executed a search warrant of the seller's residence and discovered a substantial amount of stolen U.S. military property, as well as nearly $2,000 in cash. The seller was subsequently linked to a string of larcenies on the base and is currently serving over 3 years in prison.

Advertisements for the sensitive and stolen defense-related items we purchased were not removed by the administrators of these Web sites, allowing us to complete the transactions. Both Web sites maintain published lists of items that are prohibited from sale, including stolen items, but only eBay contains warnings related to the improper sale of sensitive defense-related items. Furthermore, only eBay contains warnings related to export control issues and overseas sales, even though both Web sites have an international reach. While eBay has an administrative staff and investigative teams that look into fraud and prohibited sales occurring on the site, Craigslist has a smaller staff and largely relies on its user community for identifying inappropriate advertisements or postings. For example, when we asked a Craigslist manager about whether his company had a Fraud Investigation Team (FIT), he said, "I am the FIT for Craigslist." Generally, neither eBay nor Craigslist can incur criminal liability for being the conduit through which stolen or sensitive defense-related items are sold, even if the items are sold overseas.

Background

DOD assigns demil codes to all military property to identify their required disposition when no longer needed. Demil codes are contained in the Defense Demilitarization Manual, which implements DOD policy to apply appropriate controls and prevent improper use or release of these items outside of DOD. Demil codes indicate whether property is available for public use without restriction or whether specific restrictions apply, such as removal of classified components, destruction, or trade security controls. For example, if an item is designated as demil D, DOD requires this item to be totally

destroyed "so as to preclude restoration or repair to a usable condition" rather than allowing a member of the general public to purchase the item.

According to information in DOD's FedLog system, it considers sensitive defense-related items to be U.S. Munitions List items. This list, which is maintained by the State Department, identifies defense-related items that require government approval prior to export or temporary import. There are 20 categories of items on the U.S. Munitions List, including firearms and ammunition; aircraft and associated components; protective personnel equipment (such as body armor); nuclear weapons and related items; and directed energy weapons. Some of these items are also defined as significant military equipment, which are items for which special export controls are warranted because of their capacity for substantial military utility or capability. Any person or company in the United States that engages in either manufacturing or exporting U.S. Munitions List items must register with the State Department. Prior to exporting these items, a State Department-issued license is generally required.

The table below defines the DOD demil codes, their associated designation as U.S. Munitions List items or Significant Military equipment, and DOD's approach to disposing of the item under each code.

Table 1: DOD Demil Codes

Demil code	U.S. Munitions List item[a]	Significant Military Equipment	Required disposal action
A	No	No	Demilitarization not required
B	Yes	No	Demilitarization not required; trade security controls required at disposition
C	Yes	Yes	Remove and/or demilitarize installed key point(s) as prescribed (e.g., partial destruction)
D	Yes	Yes	Total destruction of item and components so as to preclude restoration or repair to a usable condition by melting, cutting, tearing, scratching, crushing, breaking, punching, neutralizing, etc.
E	Yes	No	Remove and/or demilitarize installed key point(s) as prescribed (e.g., partial destruction)[b]
F	Yes	Yes	Demilitarization instructions furnished by DOD item specialist
G	Yes	Yes	Demilitarization required and, if necessary,

			declassification and/or removal of sensitive marking or information
P	Yes	Yes	Declassification, and any other required demilitarization and removal of sensitive markings or information
Q	No	No	Demilitarization not required; dual use items under the jurisdiction of the U.S. Department of Commerce

Source: Defense Logistics Information Service.

[a]These designations as U.S. Munitions List items are according to DOD rather than the State Department, which maintains the U.S. Munitions List.
[b]This demil code is now obsolete according to the Defense Logistics Information Service.

Despite the use of demil codes and other safeguards, our prior reports show that DOD faces significant challenges in properly disposing of sensitive military property. For example, in our May 2005 report on excess property, we found that some sensitive defense-related items in the DOD excess property system were lost, stolen, or damaged before DOD could decide what to do with them. Losses included nearly 150 chemical and biological protective suits, over 70 units of body armor, and 5 guided missile warheads. Because 43 percent of the reported losses involved military and commercial technology requiring demilitarization, we reported that these losses posed a security risk. In follow-up work reported in July 2006, we found that the Government Liquidation Web site sold over 2,500 sensitive-defense related items to nearly 80 individuals between November 2005 and June 2006. We also reported that our undercover investigators purchased items from the Government Liquidation Web site that should not have been sold to the public, including SAPIs (which were in demand by U.S. service members in Iraq and Afghanistan); a time-selector unit used to ensure the accuracy of computer-based equipment, such as global positioning systems and system-level clocks; digital microcircuits used in F-14 fighter aircraft; and numerous other items. In our most recent July 2007 report, we found that DOD has made significant improvements in preventing the sale of sensitive defense-related items through the Government Liquidation Web site. Throughout our investigation, we detected items that were potentially sensitive, but DOD or Web site employees regularly identified the same property items and removed them from the site before they were sold.

In addition to the improper sale of sensitive defense-related items, we have also reported that the sale of demil code A and other nonsensitive military items can result in waste and reduces the efficiency of DOD operations. For example, in our May 2005 report, we

found that DOD sold new and unused items to the general public for pennies on the dollar through the Government Liquidation Web site at the same time other DOD agencies requested these items. Rather than allocate its resources effectively, DOD simply paid the full acquisition cost again to purchase the same new and unused items. We determined that, from fiscal years 2002 through 2004, $3.5 billion in new, unused, and excellent condition items were being transferred or donated outside of DOD, sold on the Internet for pennies on the dollar, or destroyed rather than being reutilized. DOD has made progress in this area, with improved utilization of property resulting in millions of dollars in recent savings. Another area involving waste where we have performed investigative work involves the sale of military MREs. Although military MREs are nonsensitive items and are not on the U.S. Munitions List, we have identified civilians and service members selling military MREs on eBay for commercial gain.[3] We concluded that military MREs are procured by government entities using taxpayer dollars, and consequently, if they are sold to the general public on eBay, they are clearly not reaching their intended recipients.

Sensitive and Stolen Defense-Related Items Available on the Internet to the Highest Bidder

We found numerous defense-related items for sale to the highest bidder on eBay and Craigslist from January 2007 through March 2008. Undercover investigators purchased a dozen sensitive items to demonstrate how easy it was to obtain them. The items were shipped to us "no questions asked." Many of these items were stolen from the U.S. military. According to DOD, it considers the sensitive items we purchased to be on the U.S. Munitions List, meaning that there are restrictions on their overseas sales. However, if investigators had been members of the general public, there is a risk that they could have illegally resold these items to an international broker or transferred them overseas. Some items we purchased were assigned demil code D, meaning that, if the items were in DOD's possession, the item should be destroyed rather than made available to members of the general public. Our investigators also identified numerous examples of U.S.

[3]See GAO, *Military Meals, Ready-to-Eat sold on eBay,* GAO-06-410R (Washington, D.C.: Feb. 13, 2006).

government property—both sensitive and nonsensitive items—being stolen and sold for personal profit rather than being utilized by DOD (i.e., conversion of government property). In addition to being cases of probable theft, these examples represent a waste of resources because DOD is effectively purchasing items that are subsequently not used for their intended purpose.

While some sellers were active-duty members of the military, other sellers included retired or reserve status military members and civilians. Our investigation of the sellers found that they obtained the sensitive defense-related items in various ways, though in most cases theft from DOD was involved. According to DOD officials, U.S. military personnel are not authorized to sell certain items that have been issued to them, such as body armor; doing so is considered theft of government property. Moreover, if a civilian (such a surplus store owner) receives military property that they know has been stolen from the government, they are in violation of the law.[4] See figure 1 for a photograph of the defense-related items we purchased from eBay and Craigslist sellers during our investigation.

[4]An individual may be in violation of 18 U.S.C. § 641 if he or she "receives, conceals, or retains [property of the United States] with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted."

Figure 1: Defense-Related Items Purchased from eBay and Craigslist Sellers

Source: GAO.

The sale of sensitive defense-related items over the Internet can have serious consequences, both abroad and here in the United States. In addition to the threat that sensitive items could be used directly against U.S. troops or allies, criminals could take advantage of some sensitive items to commit domestic crime. Sensitive defense-related items could also be reverse-engineered to develop countermeasures or equivalent technologies.

Sensitive and Stolen Defense-Related Items Purchased on the Internet

Our investigators purchased a dozen sensitive defense-related items from Internet sellers during the period of our review. According to DOD, these items are on the U.S. Munitions List, meaning that there are restrictions on their overseas sales. Table 1 summarizes the majority of the items we purchased, followed by detailed case-study narratives.

Table 2: Sensitive and Stolen Defense-Related Items Purchased on the Internet

Case	Item	Seller location	Web site	Case details

1	F-14 antenna waveguide	Loveland, Colo.	eBay	○ Item in demand by Iran, the only country with operating F-14s ○ Winning bidders on other auctions held by the seller were located in countries such as Bulgaria, China (Hong Kong), Malaysia, Russia, and Thailand ○ The seller told us that he obtained the part, along with other aircraft components, from an individual in the Denver area whose name and address he could not remember ○ We could not determine how this part became available to the general public
2	Helicopter antenna	The Colony, Tex.	eBay	○ Item currently used in the AH-1 Cobra, AH-64A Apache, and CH-47D Chinook helicopters ○ Parts that can be used in the Chinook helicopter are in demand by Iran ○ Winning bidders on other auctions held by the seller were located in countries such as Cyprus, the Czech Republic, Malaysia, and Slovenia ○ We could not determine how this part became available to the general public
3	Night-vision goggles	Tequesta, Fla.	eBay	○ These night vision goggles contain a milspec image intensifier tube, making them demil F when owned by DOD ○ In combination with IR tabs (see cases 4 and 5 below), these goggles are components in a night-fighting system that allows U.S. service members to identify friendly warfighters ○ These goggles could be used to identify U.S. troops on the battlefield
4	IR tabs	Marlboro, N.Y.	Internet storefront	○ Enemies could use IR tabs to pose as a friendly fighter during night combat, creating confusion on the battlefield and putting troops at risk ○ Seller claimed that he always verifies the identification of IR tab buyers to ensure that only military and law enforcement officials obtain the tabs ○ Our undercover investigators ordered tabs using the seller's online store front and obtained the tabs without any type of verification check
5	ACU and accessories	Fayetteville, N.C. and other locations	eBay	○ In combination with accessories purchased from other sellers (e.g., patches, boots, a beret), item could allow anyone to look like a U.S. service member ○ ACU came with IR tabs, meaning that the enemy could also use this ACU to pose as a friendly fighter during night combat, creating confusion on the battlefield and putting troops at risk ○ Seller is a civilian who claimed to obtain the ACU at a flea market near Fort Bragg, N.C.

				○ Property appears to be stolen
6	Kevlar helmet	Bloomingdale, Ill.	eBay	○ Demil B item that cannot be exported without a license from the State Department, which the seller said he did not have ○ According to eBay records, winning eBay bidders for other Kevlar helmets included buyers in countries such as Costa Rica, the Czech Republic, Hungary, and Thailand ○ Seller represented to us that he cancelled transactions when auctions were won by overseas bidders ○ Seller is a civilian who said he legitimately obtained the helmets from the Government Liquidation Web site
7	Nuclear biological chemical gear	Oxnard, Calif.	Craigslist	○ Item that could be reverse engineered to develop countermeasures or produce equivalent technology ○ Craigslist ad identified the seller as a Marine who was selling gear he had been issued ○ When we interviewed the seller, he stated that, contrary to what he wrote in his advertisement, an acquaintance had given him the gear ○ Stolen government property
8	E-SAPIs	Arlington, Tex.	eBay	○ Item that could be reverse engineered to develop countermeasures or produce equivalent technology ○ According to eBay records, winning eBay bidders on similar military body armor items included individuals in China (Hong Kong), Poland, Taiwan, and Singapore ○ Stolen from government or manufacturer
9	Body armor/SAPIs	Fayetteville, N.C.	Craigslist	○ Item that could be reverse engineered to develop countermeasures or produce equivalent technology ○ Seller is an Army Special Forces Staff Sergeant assigned to Fort Bragg, N.C. ○ The seller stated that he purchased these items at a yard sale and paid cash ○ He said that he thought it was "OK" to sell the body armor on Craigslist because he had seen other body armor for sale there ○ Stolen government property
10	Body armor/SAPIs	Minot, N.D.	eBay	○ Item that could be reverse engineered to develop countermeasures or produce equivalent technology ○ Seller was a Senior Airman with the Air Force Reserve at the time of our investigation ○ Minot Air Force Base security police and the county sheriff's office investigated the matter and determined that the body armor was stolen from the base ○ Seller knew he was selling government property

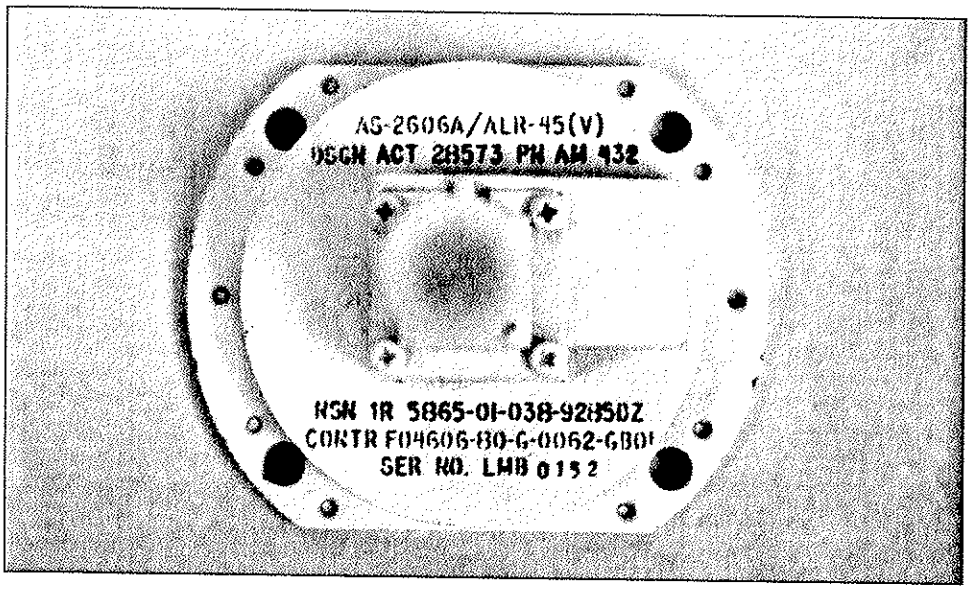
Source: GAO.

In addition to the items in the above table, we also purchased other items including an F-14 radio receiver and a body armor vest with SAPI plates. According to DOD, these are U.S. Munitions List items. We also purchased nonsensitive defense-related items such as boots, berets, patches, and an ACU chest rig.

Case 1: F-14 Antenna Waveguide

On October 10, 2007, we purchased a new antenna for the F-14 Tomcat from an eBay seller located in Loveland, Colorado. The seller lives about 60 miles from Buckley Air Force Base in Colorado. The antenna has a demil designation of D, which requires DOD to destroy it when no longer needed. Our past work identified the control of excess F-14 components as a major challenge for DOD. The only country with operational F-14s, Iran, is known to be seeking such parts. We interviewed the seller, who told us that he sells industrial electronic surplus items. He said he purchases these items from individuals, Internet sales sites, other eBay sellers, manufacturers, and occasionally the Government Liquidation Web site. The seller told us that he obtained this antenna waveguide from an individual located in the Denver, Colorado, area, whose name and address he could not remember. We were unable to determine how this part became available to the general public. We referred the seller to DCIS for criminal investigation. See figure 2 for a picture of the antenna waveguide.

Figure 2: F-14 Antenna Waveguide Purchased from eBay Seller



Source: GAO.

Case 2: Helicopter Antenna

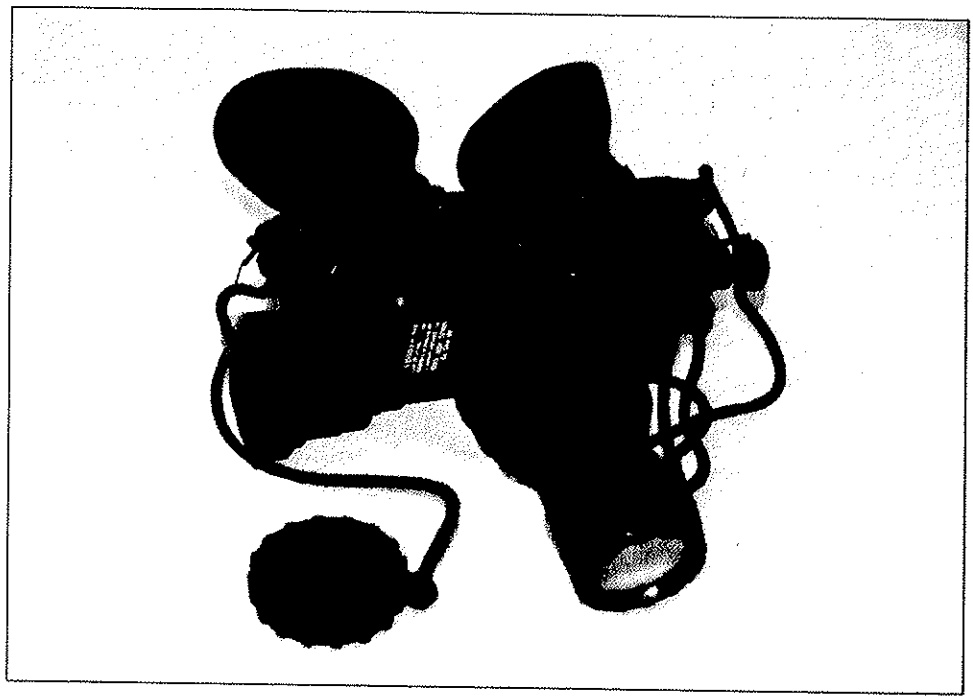
On September 19, 2007, we purchased a used flush-mount antenna, which is currently in use by the military in the AH-1 Cobra, AH-64A Apache, and CH-47D Chinook helicopters, from an eBay seller located in The Colony, Texas. This city is located about 130 miles from Sheppard Air Force Base. The antenna is assigned demil code D, which requires DOD to destroy it when no longer needed. Chinook components are reportedly in demand by Iran, making this a national security issue. We interviewed the seller, who told us that he buys aircraft components from auctions and companies that are going out of business (not from Government Liquidation). He explained that he targets specific aircraft parts that can be used in both military and commercial aircraft because he can better market these items to collectors. For example, he said that if he buys a Boeing 707 part he will resell it and advertise the part as belonging to a KC-135 Stratotanker (a midair refueling aircraft) because it would better pique the interest of a collector. According to eBay records, winning eBay bidders for other auctions held by this seller were located in Cyprus, the Czech Republic, Malaysia, and Slovenia. The seller did not recall the sale of this particular part, and it is unclear how it became available to the general public. We referred the seller to DCIS for criminal investigation.

Cases 3 and 4: Night Vision Equipment

We obtained both milspec night vision goggles and IR tabs on the Internet. Although night vision goggles are commercially available to the public, the milspec tube in the goggles we purchased is a sensitive component that allows U.S. service members on the battlefield to identify friendly fighters wearing infrared (IR) tabs. These tabs are known as an IFF (identification friend or foe) element and can be detected at night by both ground troops and airborne combat pilots equipped with night-vision equipment. Obtaining either of these two items could give enemies an undue advantage in night combat situations, either by using the night vision goggles to detect U.S. troops or by posing as U.S. troops (or friendly forces) with the IR tabs. We purchased these items directly from distributors who could sell these products domestically without violating any laws. However, officials representing the manufacturer of the night vision goggles told us that the goggles should not be sold on eBay and that, consequently, a violation of its distribution policies had occurred at some point in the distribution process. Officials told us they would conduct an investigation into where the violation of policy occurred and would remove the offending distributor from its list of authorized distributors.

Case #3: Night Vision Goggles. On March 29, 2007, we purchased new/unused milspec night-vision goggles from an eBay seller located in Tequesta, Florida. The fully operational goggles have a demilitarization code of F, meaning that, if the goggles are part of DOD inventory, they cannot be sold to the general public unless the milspec image intensifier tube has been removed. The image intensifier tube was included in the goggles we purchased. See figure 3 for a picture of the night-vision goggles.

Figure 3: Night-Vision Goggles Purchased on eBay



Source: GAO.

Our investigators determined that the seller is a retired U.S. Marine Corps Colonel. The seller is the manager of business development for a General Services Administration scheduled business that distributes tactical, surveillance, and force protection equipment. According to the retired Colonel, he originally obtained 28 night-vision goggles from an authorized distributor and sold most of them to active-duty military units, the U.S. Fish and Wildlife Service, U.S. Department of Homeland Security, U.S. Bureau of Land Management, and a number of municipal and state law enforcement agencies. The retired Colonel told us that, when he was unable to sell all 28 goggles, he used his personal eBay account to sell the remaining goggles to 10 individuals across the United States. He represented to us that he asked all potential clients for the goggles whether they were U.S. citizens as part of the eBay sales process. However, he did not ask our undercover investigator this question. Based on interviews with the goggle manufacturer and our legal research, we determined that the seller did not violate the law by selling these goggles domestically to members of the general public. However, it does appear the sale and distribution of these goggles violated the manufacturer's policy. Officials representing the goggle manufacturer told us they would conduct an investigation into where the violation of policy occurred and would remove the offending

distributor from its list of authorized distributors. We referred this matter to DCIS and DLA for investigation.

Case #4: IR tabs. We purchased new/unused IR tabs from an Internet store front (not eBay or Craigslist) maintained by a business owner in Marlboro, New York. We were alerted to this seller through his eBay advertisements and located the associated online store front. An enemy fighter wearing these IR tabs could pass as a friendly service member during a night combat situation, putting U.S. troops at risk. Prior to this purchase, our investigators had visited the physical store location, which is near the U.S. Military Academy at West Point. The physical store sells a variety of military items ranging from parachute cords to military patches. Our investigators identified themselves as GAO investigators and asked the store owner, a retired Army Captain, whether he sells IR tabs to the general public. The store owner stated that he only sells the tabs to U.S. military personnel and that he always obtains proof of employment before completing an order. Several days after the interview, our investigator ordered and received several tabs from the seller's online store front. The validity of the order was never questioned, and the owner did not attempt to verify the employment of our investigator, as he stated during the interview. These tabs are not standard U.S. military issue and therefore do not have a demil code assigned to them. However, according to the manufacturer, they have the same properties as the IR tabs used by the military and are a comparable product. Our own in-house tests confirmed that the tabs had IR properties and appeared to function the same way. We referred this matter to DCIS for investigation.

Case 5: ACU and Accessories

During the course of this investigation, we purchased all the items necessary to build a complete, current U.S. military uniform—from boots to beret—using only the Internet Web sites eBay and Craigslist. Our intent was to demonstrate that the general public can purchase, over the Internet, all the gear necessary to dress and look like a U.S. service member. DOD has recognized the security risk associated with a member of the general

public being able to acquire a full uniform. In January 2007, Iraqi insurgents dressed in U.S. military uniforms were allowed to pass through a police checkpoint in Karbala, Iraq. They subsequently broke into a secure compound using percussion bombs and killed five U.S. service members. After this incident, DOD issued a Demil Bulletin noting that ACUs "...will only be released to Army, Navy, Air Force, Marines and their Guard or Reserve components."

On April 17, 2007—after the Demil Bulletin had been issued by DOD—we purchased a new/unused ACU with IR tabs from an eBay seller located in Fayetteville, North Carolina. As discussed above, IR tabs allow U.S. service members to identify friendly fighters during night combat. In addition to the risk that an enemy could pose as a U.S. service member in this ACU, the readily available IR tabs would also allow an enemy fighter to pose as a friendly fighter during night combat. The DOD-issued IR tabs are demil code D, which requires DOD to destroy them when no longer needed. According to the Defense Logistics Agency, the ACU that we purchased from this seller is ineligible for resale or release to the general public. The seller told us that he purchased the ACU at a flea market near Fort Bragg, North Carolina, and added that, on many occasions, he has observed flea market vendors purchasing military items from individuals who arrive at the flea market. The vendors then sell the items to the general public at the flea market. After concluding the interview, our investigators visited the flea market and observed several vendors selling used ACUs and several new/unused ACUs (none contained IR tabs). The flea market vendors told our undercover investigators that they obtain the ACUs at yard sales in the area and from soldiers. This ACU appears to have been stolen from DOD. We referred this matter to DCIS for criminal investigation. See figure 4 for a picture of the ACU.

Figure 4: ACU Purchased on eBay

Source: GAO.

Case 6: Kevlar Helmet

On April 21, 2007, we purchased a used Kevlar helmet from a civilian eBay seller located in Bloomingdale, Illinois. Even though the eBay seller's ad indicated that the helmet could not be exported, our investigation of his eBay history indicated that buyers in countries such as Costa Rica, the Czech Republic, Hungary, and Thailand had won eBay auctions for the helmets. When we interviewed the seller, he told us that he had never shipped Kevlar helmets overseas and he canceled sales when overseas buyers won these auctions. He said he originally obtained the helmets from the Government Liquidation Web site, which required him to sign an end use certificate stating, among other things, that the helmets would not be exported without a license from the State Department. Further review of the seller's eBay records reveals that he had completed auctions for $21,000 worth of Kevlar helmets from February 2007 to July 2007. We referred this matter to DCIS for criminal investigation.

Case 7: Nuclear Biological Chemical Gear

On August 23, 2007, we purchased a used Nuclear Biological Chemical (NBC) protective suit, unused gas mask, used gloves and boots, and unused chemical-biological canister (containing the gas mask filter that is used to protect against chemical and biological warfare agents) from a Craigslist seller located in Oxnard, California. Although some of this gear was removed from packaging and therefore not usable to protect against an attack, according to a DOD Product Specialist with whom we spoke, the NBC suit is susceptible to reverse engineering and should not be sold to the public. The Craigslist advertisement stated that the seller was a former member of the military and that he was selling the gear because he needed money. When we interviewed the seller, he claimed that, despite what he wrote in the Craigslist advertisement, the gear was not his. He said that he left the Marines in 2002 and that the suit was given to him by an acquaintance who was also a Marine. He thought his Craigslist advertisement would be a good marketing ploy. Upon further questioning about the origin of the gear, the seller stated that (1) he did not remember his acquaintance's first name; (2) his acquaintance had not been issued the gear either, obtaining it at what he called a "swap meet" and; (3) his acquaintance had recently died in a motorcycle accident. This property was likely stolen from DOD. We referred this matter to DCIS for criminal investigation. See figure 5 for a picture of the NBC gear (worn by a GAO investigator).

Figure 5: NBC Gear Purchased on eBay

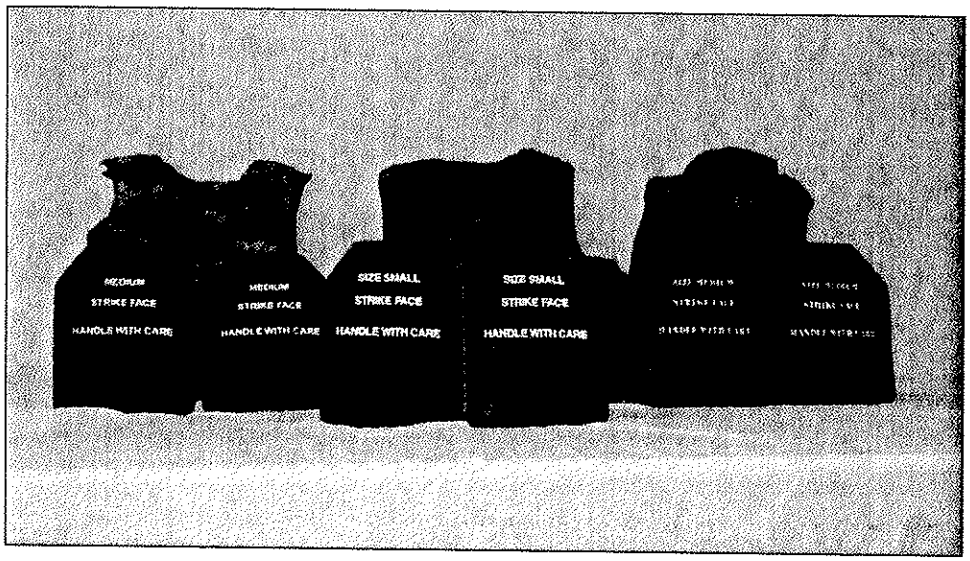
Source: GAO.

Cases 8 through 10: Body Armor and SAPIs

Our May 2005 and July 2006 work identified two types of body armor that DOD's excess property system did not manage adequately—body armor vests and SAPIs. SAPIs are ceramic plates designed to slide into pockets sewn into the front and back of body armor vests in order to protect the warfighter's chest and back from small arms fire. They are currently used by service members in Iraq and Afghanistan. According to DCIS, service members are not authorized to sell body armor vests or SAPIs, and selling these items is considered theft of government property. Moreover, body armor vests and SAPIs are designated demil code D, meaning that DOD should destroy them when no longer needed. We purchased three body armor vests and seven sets of SAPIs, including two current-issue E-SAPIs. Because service members are not authorized to sell these items,

we concluded that they were stolen from the military. See figure 6 for a picture of some of the stolen SAPIs and body armor vests we purchased.

Figure 6: Body Armor Vests with SAPIs Purchased on eBay and Craigslist



Source: GAO.

The availability of body armor and SAPIs to the general public has both national security and domestic safety implications. Regarding national security, reverse engineering could allow the creation of equivalent technology or the discovery of countermeasures based on potential weaknesses in the armor. On the domestic front, it is prohibited for violent felons to purchase, own, or possess body armor. Although sellers do not have a responsibility to determine whether they are selling body armor to a violent felon, and it is not illegal to do so, the wide availability of body armor online makes it easier for violent felons to break the law by obtaining body armor. The following case studies describe three of the four investigations we conducted into body armor we purchased online.

Case #8: E-SAPI. On September 13, 2007, we purchased two new/unused body armor inserts identified as E-SAPIs from an eBay seller located in Arlington, Texas. This city is about 120 miles from Sheppard Air Force Base. The E-SAPI plates were manufactured in June 2007 and are currently used by U.S. service members in Iraq and Afghanistan. We determined that, from September 2006 to February 2008, the seller, who did not appear

affiliated with the U.S. military, had completed eBay auctions of over 600 body-armor-related items totaling approximately $60,000. Most of the body armor appears to have been stolen from the military. In addition to domestic sales in the United States, the seller's eBay history indicates that the highest bidders on some auctions were located overseas in such countries as China (Hong Kong), Poland, Taiwan, and Thailand. We referred this matter to DCIS for criminal investigation

Case #9: Body Armor and SAPIs. On September 22, 2007, we purchased a used body armor vest and two SAPIs from a Craigslist seller located in Fayetteville, North Carolina. Our investigation determined that the seller is an active-duty Staff Sergeant in the U.S. Army stationed at Fort Bragg. We interviewed the Staff Sergeant about the purchase. He claimed that he purchased the body armor at a garage sale while he was stationed at Fort Stewart, Georgia. He could not recall the specific location of the sale or the name of the seller and said that he paid cash. He stated that he thought it was "OK" to sell body armor on Craigslist because he had seen other advertisements for it. This is another case of theft of government property, which we referred to DCIS for criminal investigation.

Case #10: Body Armor and SAPIs. On March 30, 2007, we purchased a used body armor vest and two SAPIs from an eBay seller located in Minot, North Dakota. The seller lives near Minot Air Force Base. Our investigation determined that the seller was a Senior Airman with the Air Force Reserve. Further, we determined that the individual had completed eBay auctions for 18 body armor vests and SAPIs from June 2006 to April 2007 for a total of over $3,300. According to eBay records, an individual in Japan was the highest bidder in one of the auction rounds. After we referred this matter to Air Force OSI, we learned that the Minot Air Force Base security police and the county sheriff's office had investigated the matter and determined that the body armor was stolen from the base. According to Air Force OSI, this individual knew that the items were government property when he sold them on eBay.

Other Defense-Related Items

Our investigators also identified numerous examples of U.S. government property—both sensitive and nonsensitive—being stolen and sold for personal profit rather than being utilized by DOD (i.e., conversion of government property). In addition to being cases of probable theft, these examples represent a waste of resources because DOD is effectively purchasing items that are subsequently not used for their intended purpose.

Civilian Sellers of Stolen Property

We identified two civilian sellers with eBay store fronts who bought defense-related items from service members and sold these items to the general public on eBay. These items could have been stolen from the military. If these sellers knew the property they bought from the service members was stolen, they too would be violating the law.[5]

Gun-Store Owner. This eBay seller owns a gun store in Barstow, California. He lists U.S. military items on his eBay store front, including sensitive defense-related items such as Kevlar helmets and NBC gear. When we asked the seller to identify the source of the items listed on his eBay store front, he told us that military personnel frequently arrive at his shop with the items for sale. He gave us a record of the military items he had purchased from military personnel. For each sale, the gun-store owner obtained the signature of the seller and photocopied their identification card—in some cases, sellers provided him with their military IDs. We cross-matched the names of the individuals who sold items to the gun-store owner with the DEIDS database to determine whether any of the sellers were currently serving in the military. Table 5 contains details about the service members who sold items to the gun-store owner and the nature of the items.

Table 3: Service Members Who Sold U.S. Military Property to a Gun-Store Owner in Barstow, California

No.	Rank	Branch	Current assignment	Items sold to gun shop owner
1	Staff Sergeant (E-6)	Army (active)	U.S. Army Recruiting Command, Ariz.	Helmets, knee pads, boots, and miscellaneous gear
2	Sergeant (E-5)	Army (active)	Fort Dix, N.J.	Flak vest and miscellaneous gear

[5]18 U.S.C. § 641.

3	Sergeant (E-5)	Army (reserve)	Fort Irwin, Calif.	Miscellaneous field gear
4	Specialist (E-4)	Army (active)	Fort Irwin, Calif.	Miscellaneous field gear
5	Specialist (E-4)	Not serving	N/A	Kevlar helmets, ACU, distress markers, and weapons-related gear
6	Specialist (E-4)	Not serving	N/A	Flak vest, gas mask
7	Specialist (E-4)	Army (reserve)	Portsmouth, Va.	Helmet, boots, miscellaneous gear
8	Private First Class (E-2)	Marine Corps (reserve)	Twenty-nine Palms, Calif.	Miscellaneous gear
9	Private (E-1)	Not serving	N/A	Flak vest

Source: Barstow, California gun-store owner.

We investigated this seller in 2005 in our report related to stolen MREs sold over eBay and referred him to the DOD Inspector General (IG) for review and criminal investigation.[6] We have not received any information from the DOD IG regarding their actions on this referral. We continue to believe this matter requires investigation and have made an additional referral to Army CID for criminal investigation.

Military Surplus Store Owner. This eBay seller owns a military surplus store in Abilene, Texas. Our investigators visited the physical store location associated with the eBay store and observed a number of new ACUs with IR tabs affixed to them. As discussed above, IR tabs are an IFF element that can be detected at night by both ground troops and airborne combat pilots equipped with night-vision equipment and represent one part of the night-fighting system discussed above. The IR tabs on the ACUs were likely demil code D items[7] and, if so, should be destroyed when no longer needed by DOD. When our investigators pointed this out to the store owner, he said he was unaware of the restriction and removed the ACUs from the sales rack. The store owner said he purchased the ACUs from service members. He added that many of the items in his store were acquired from local military personnel who arrive, unannounced, at his shop with items for sale. He said that he maintains a record of transactions and provided a copy to our investigators. We cross-matched information on these individuals with the DEIDS database to determine whether any of the sellers were currently serving in the

[6]GAO-06-410R.

[7]We did not test the IR properties of these tabs or confirm with DOD that they were military-issue.

military. Table 4 contains details about service members who sold items to the store owner and the nature of the items.

Table 4: Service Members Who Sold U.S. Military Property to an Abilene, Texas, Store Owner

No.	Rank	Branch	Current assignment	Items sold to store owner
1	Master Sergeant (E-7)	Air Force (retired)	N/A	Flight suits, flight jackets, battle dress uniforms (BDU), boots
2	Staff Sergeant (E-6)	Army National Guard (active)	Austin, Tex.	ACUs
3	Staff Sergeant (E-5)	Air Force (active)	Dyess Air Force Base	Kevlar vests, BDUs, boots
4	Staff Sergeant (E-5)	Air Force National Guard (active)	Nashville, Tenn.	Backpack
5	Staff Sergeant (E-5)	Air Force (active)	Kunsan Air Base (South Korea)	Helmet, miscellaneous gear
6	Senior Airman (E-4)	Air Force (active)	Dyess Air Force Base	BDUs
7	Senior Airman (E-4)	Air Force (active)	Dyess Air Force Base	BDUs, boots, gas mask and filters
8	Senior Airman (E-4)	Air Force (active)	Dyess Air Force Base	BDUs, boots, field jacket
9	Airman First Class (E-3)	Air Force (active)	Dyess Air Force Base	BDUs and boots

Source: Abilene, Texas, military surplus store owner.

We referred this matter to Air Force OSI for criminal investigation.

MREs

Military MREs are designed to sustain an individual engaged in strenuous activity, such as military training or actual military operations, when normal food service facilities are not available. In general, military MREs are boxed in cases of 12. Each MRE contains a full meal packet in a flexible bag. The cases and bags for military MREs are marked with the words "U.S. Government Property, Commercial Resale Is Unlawful." Although we do not consider MREs to be sensitive property, military MREs are procured by government entities using taxpayer dollars and are intended to be consumed by individuals from authorized organizations and activities. Consequently, if military MREs are sold to the general public on the Internet, they are clearly not reaching their intended recipients and

represent a waste of taxpayer dollars. Since service members are not authorized to take MREs and sell them for personal gain, the vast majority of the military MREs for sale on the Internet represent stolen military property

During our investigation, we purchased numerous cases of MREs from eBay and Craigslist sellers. The sellers were mostly civilians. Three examples of our investigative work related to military MREs follows:

- One civilian seller in Louisiana[8] indicated that she has been selling military MREs on eBay for a number of years. She said that she acquires the MREs from service members assigned to a nearby military base, and that they arrive at her home unannounced. She added that most of the service members have 2 or 3 MRE cases but that others have had as many as 10 to 12 cases. She told us that she does not know any of the service members or where they get the MREs, but suggested they are "left over" from field exercises. She said that she usually pays service members about $20 per case in cash and that she can sell the cases on eBay for about $55 per case. We reviewed eBay records and learned that, from September 2006 through February 2008, she completed eBay auctions totaling about $55,000 for MREs. These MREs were likely stolen from the nearby military base. We referred this case to Army CID for criminal investigation.

- A second seller living in Phenix City, Alabama, is employed as a civilian aircraft mechanic at Fort Benning, Georgia. She told us that she obtains military MREs from dumpsters at Fort Benning. She stated that she visits the dumpsters several times a week, removing unopened MREs from the dumpsters and cleaning, packaging, and mailing them to her eBay customers. According to sales data provided by eBay, from July 30, 2006, to February 6, 2008, this individual had completed approximately $54,000 in MRE auctions. If what this individual said was true, according to our calculations (using a sale price of $42 per case) this

[8]We have removed detailed information about the location of this seller because of an ongoing investigation by Army CID, which was based on our referral.

individual would have had to "dumpster dive" for about 15,428 individual MRE packages to have $54,000 in sales during this time period. Because of the volume of sales activity we referred this case to Army CID for criminal investigation.

- A third seller was a Private First Class in the U.S. Army stationed in Camp Casey, South Korea. Based on our referral, Army CID executed a search warrant at the seller's residence and discovered a substantial amount of stolen U.S. military property, as well as nearly $2,000 in cash. According to Army officials, the seller was charged with drug possession and use in the summer of 2006. He was demoted and placed in a supply clerk position in charge of MRE inventories while awaiting discharge from the military, which gave him the opportunity to steal MREs and sell them over eBay. Army CID linked the seller to a series of unsolved larcenies on base. The seller pled guilty and was sentenced to over 3 years in prison.

eBay and Craigslist Have Few Safeguards to Prevent the Sale of Stolen and Sensitive U.S. Military Items

Advertisements for the sensitive and stolen defense-related items we purchased were not removed by the administrators of these Web sites, allowing us to complete the transactions. Both Web sites maintain published lists of items that are prohibited from sale, including stolen items, but only eBay contains warnings related to sensitive defense-related or export-controlled items even though both Web sites have an international reach. eBay employs administrative staff and investigative teams intended to deter fraud and prohibited sales from occurring on the site. Meanwhile, Craigslist has a smaller staff and largely relies on its user community for identifying inappropriate advertisements or postings. Officials with both Web sites told us they cooperate with law enforcement agencies to stop the sale of illegal, counterfeit, or stolen items, and identify and deter individuals from using these Internet services for a fraudulent or improper purpose. Generally, neither eBay nor Craigslist can incur criminal liability for being the conduit through which stolen or export-controlled items are sold, even if the items are

sold overseas. Because the Web sites never take possession of the goods, do not set the price of transactions, and do not actually deliver the items, no relevant federal criminal statute applies to their activities. Table 5 summarizes the policies, proactive enforcement efforts, and penalties that each of these Internet companies maintain to deter the sale of prohibited items.

Table 5: eBay and Craigslist Policies and Procedures

Policy or procedure	eBay	Craigslist
Stolen items are prohibited from sale?	Yes, including explicit mention of items requiring demilitarization	Yes, no explicit reference to items requiring demilitarization
Prohibited items list includes export-controlled items?	Yes; contains information on international sales and provides a ink to http://www.export.gov	No; provides a link to Treasury's Office of Foreign Assets Control
Prevents the sale of property on its prohibited lists?	Prohibited Item Team attempts to detect prohibited items and delete prohibited postings. Additionally, users can report prohibited items being sold or other violations of policies.	Relies on users to detect and report advertisements for prohibited items
Works with law enforcement agencies?	Fraud Investigations Team cooperates with law enforcement to report information about sellers and makes proactive referrals	One individual at Craigslist is tasked to work with law enforcement and requires subpoena to disclose information about sellers
Have penalties for non-compliance with policies?	Penalties for violating policies include property listing cancellation, limits on account privileges, elimination of "Power Seller" status, and suspension of accounts	Penalties include deletion of user's account and other attempts to prevent the user from accessing the site

Source: GAO analysis of eBay and Craigslist policies and procedures, and information provided by respective Web site administrators.

eBay

Advertisements for the sensitive and stolen defense-related items we purchased were not removed by eBay administrators, allowing us to complete the transactions. According to its prohibited items list, eBay prohibits stolen property from being sold. eBay also provides extensive information about international trading on its prohibited items list, including a link to a government Web site on export controls. There are no explicit references to the sale of military MREs and other stolen military property on the

prohibited items list. However, eBay does discuss a prohibition on defense-related items that have not been disposed in accordance with DOD demilitarization policies. According to an eBay official with whom we spoke, his company has created two teams that inspect user sales—the Fraud Investigations Team and the Prohibited Items Team. The Fraud Investigations Team deals directly with law enforcement organizations and provides information on sales or seller activity. We received invaluable assistance from the Fraud Investigations Team during our investigation. The official stated that the Fraud Investigations Team also proactively refers cases to relevant law enforcement agencies for further investigation and prosecution. Meanwhile, the Prohibited Items Team has an automatic filtering system to identify potentially prohibited sales and responds to reports on prohibited activity. If the Prohibited Items Team discovers a prohibited item, its mandate is to remove the advertisement for the item, educate the seller, and suspend the seller's account if the activity continues. When we asked the eBay official about the sale of military body armor on eBay, he admitted that it was a difficult issue for eBay because some body armor can be sold legally. He said that the Fraud Investigations Team does not scan eBay sales to try to identify what body armor is illegal to sell, e.g., body armor that has been stolen from the military. Regarding the sale of military MREs, the official stated that "nobody has indicated to us that it's illegal to sell MREs." To penalize users who violate eBay policies, eBay officials can cancel listings, limit account privileges, eliminate users' "Power User" status, and suspend accounts.

Craigslist

Advertisements for the sensitive and stolen defense-related items we purchased were not removed by Craigslist administrators, allowing us to complete the transactions. Craigslist policies and procedures prohibit the sale of stolen property. However, its prohibited items list does not mention sensitive defense-related items, export controls, or international trading despite the fact that the Web site serves cities around the world. Further, there are no explicit references to the sale of military MREs and other stolen military property on the prohibited items list. Because these items are not included on the list, and there is no discussion of international trading, Craigslist officials and users

are unlikely to prohibit these sales. Craigslist maintains a much smaller staff than eBay (25 people according to its Web site). When we asked a Craigslist manager about whether his company had a Fraud Investigations Team (FIT), he said, "I am the FIT for Craigslist." This official added that Craigslist relies primarily on its user community to identify suspicious advertisements and report prohibited item sales. We observed this in several cases during our investigation, when questionable advertisements for weapons and other obviously prohibited sales we identified were also apparently noticed by Craigslist users, leading to removal of the items from the Web site. The Craigslist official with whom we spoke indicated that Craigslist works with law enforcement agencies but does not proactively call issues to their attention. The official said that Craigslist deletes advertisements for questionable items, such as body armor and night vision goggles, when contacted by law enforcement. However, unlike eBay, Craigslist will not provide seller information to a law enforcement agency without a subpoena. To penalize users who do not comply with Craigslist policies, company officials can delete the user's account or otherwise attempt to prevent the user from accessing the site.

Contacts and Staff Acknowledgments

For further information about this testimony, please contact Gregory D. Kutz at (202) 512-6722 or kutzg@gao.gov. Major contributors to this testimony include Mario Artesiano, Johana Ayers, Nabajyoti Barkakati, Norman Burrell, Shafee Carnegie, Bruce Causseaux, Thomas Denomme, Dennis Fauber, Richard Guthrie, Kenneth Hill, Jason Kelly, Barbara Lewis, Andrew McIntosh, James Murphy, Gertrude Moreland, and Richard Newbold.

192251