
Undercover Purchases on eBay and Craigslist Reveal a Market for Sensitive and Stolen United States Military Items

By
Gregory D. Kutz
Managing Director Forensic Audits and Special Investigations
Government Accountability Office

[The following are excerpts from the Government Accountability Office-08-644T (GAO), a report before the Subcommittee on National Security and Foreign Affairs, Committee on Oversight and Government Reform, House of Representatives. To view the full report, including the scope and methodology, visit <http://www.gao.gov/new.items/d08644t.pdf>.]

Highlights

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.

What the Government Accounting Office Found

The 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 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* (USML), 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			
Number	Item	Web Site	Notes
1	F-14 antenna	eBay	<ul style="list-style-type: none"> F-14 components 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	<ul style="list-style-type: none"> Could be reverse engineered to develop countermeasures or produce equivalent technology Stolen military property
3	Enhanced small arms protective inserts	eBay	<ul style="list-style-type: none"> Body armor plates manufactured in June 2007 and currently in use by troops in Afghanistan and Iraq Winning eBay bidders on other body armor items offered by this seller included individuals in China (Hong Kong), Taiwan, and Singapore Stolen from U.S. military or manufacturer

Examples of Sensitive Items Purchased by Undercover Investigators

GAO investigators also identified 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. The store owners told GAO they purchased gear from service members, including Kevlar vests, flak jackets, and gas masks, and sold it through eBay to the general public. GAO also purchased stolen military Meals, Ready-to-Eat (MREs) and found a robust market for stolen military MREs on eBay and Craigslist.

Advertisements for the sensitive defense-related 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.

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 components could threaten national security. In another example, ICE agents arrested a Colombian 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 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 be 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 components, 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 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.

In addition to the Government Liquidation web site, many military surplus stores across the U.S. 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 classified:

- Listing jobs
- Housing
- Goods
- Services
- Personals
- Activities
- Advice
- 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.

1. The Government Liquidation web site, which is run by a DoD contractor, 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 Risks 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-05-277 (Washington, D.C.: May 13, 2005); and GAO, *DoD Excess Property: Risk Assessment Needed on Public Sales of Equipment That Could Be Used to Make Biological Agents*, GAO-04-15N1 (Washington, D.C.: Nov. 19, 2003).

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. [As mentioned previously,] 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 the following:

- Countermeasures to defeat or minimize the military significance of the item
- The development of an equivalent item that could be used against U.S. interests

To perform [our internet] 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). [As stated before,] 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 Investigations Team 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. 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

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 the demil code associated with each item in the system.

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—F-14 components are in demand by Iran. 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 components available to the general public, the eBay sellers provided an opportunity for these components 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 components, 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 [the] DOD.

In addition to the above case studies, our investigators identified examples of USG property that was likely 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. The store owners told us they 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 (MREs) 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 three years in prison.

Advertisements for the sensitive defense-related items we purchased were not removed by the administrators of these web sites, allowing us to complete the transactions. [As stated previously,] 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 Investigations 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.