INVESTIGATION INTO THE SALE OF SENSITIVE, IN-DEMAND MILITARY EQUIPMENT AND SUPPLIES ON THE INTERNET

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY
AND FOREIGN AFFAIRS

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

APRIL 10, 2008

Serial No. 110–178

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.oversight.house.gov

U.S. GOVERNMENT PRINTING OFFICE

50–350 PDF WASHINGTON : 2009

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HENRY A. WAXMAN, California, *Chairman*

EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
BRIAN HIGGINS, New York
JOHN A. YARMUTH, Kentucky
BRUCE L. BRALEY, Iowa
ELEANOR HOLMES NORTON, District of Columbia
BETTY MCCOLLUM, Minnesota
JIM COOPER, Tennessee
CHRIS VAN HOLLEN, Maryland
PAUL W. HODES, New Hampshire
CHRISTOPHER S. MURPHY, Connecticut
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont

TOM DAVIS, Virginia
DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
JOHN J. DUNCAN, JR., Tennessee
MICHAEL R. TURNER, Ohio
DARRELL E. ISSA, California
KENNY MARCHANT, Texas
LYNN A. WESTMORELAND, Georgia
PATRICK T. MCHENRY, North Carolina
VIRGINIA FOXX, North Carolina
BRIAN P. BILBRAY, California
BILL SALI, Idaho
JIM JORDAN, Ohio

PHIL SCHILIRO, *Chief of Staff*
PHIL BARNETT, *Staff Director*
EARLEY GREEN, *Chief Clerk*
LAWRENCE HALLORAN, *Minority Staff Director*

SUBCOMMITTEE ON NATIONAL SECURITY AND FOREIGN AFFAIRS

JOHN F. TIERNEY, Massachusetts, *Chairman*

CAROLYN B. MALONEY, New York
STEPHEN F. LYNCH, Massachusetts
BRIAN HIGGINS, New York

CHRISTOPHER SHAYS, Connecticut
DAN BURTON, Indiana
JOHN M. MCHUGH, New York
TODD RUSSELL PLATTS, Pennsylvania

DAVE TURK, *Staff Director*

CONTENTS

INVESTIGATION INTO THE SALE OF SENSITIVE, IN-DEMAND MILITARY EQUIPMENT AND SUPPLIES ON THE INTERNET

THURSDAY, APRIL 10, 2008

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY AND FOREIGN AFFAIRS,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m. in room 2154, Rayburn House Office Building, Hon. John F. Tierney (chairman of the subcommittee) presiding.

Present: Representatives Tierney, McCollum, Hodes, Welch, and Shays.

Staff present: Dave Turk, staff director; Andrew Su, professional staff member; Davis Hake, clerk; Andrew Howell, intern; A. Brooke Bennett, minority counsel; Nick Palarino, minority senior investigator and policy advisor; Chris Espinoza, minority professional staff member; and Mark Lavin, minority Army fellow.

Mr. TIERNEY. Good morning, and thank you for being here.

Most Members, as you know, have multiple conflicting items on their schedule, and they will be in and out as the morning goes on. Mr. Shays is on his way over, but you folks are kind enough to be here in a timely fashion and we want to get started so that your day is put to good use.

The Subcommittee on National Security and Foreign Affairs hearing entitled, "Investigation into the Sale of Sensitive, In-Demand Military Equipment and Supplies on the Internet," will come to order.

There is unanimous consent that only the chairman and ranking member will be allowed to make opening statements. Mr. Shays will be allowed to make his when he arrives.

There is unanimous consent that the hearing record will be kept open for five business days so that all members of the subcommittee will be allowed to submit a written statement for the record.

Last summer the subcommittee, on a bipartisan basis, asked the special investigators at the Government Accountability Office to begin an undercover operation into whether sensitive and stolen military equipment and supplies were being sold on the Internet on such sites as eBay and Craigslist—obviously, not exclusively those sites. We also asked GAO to investigate how such items were acquired and able to be put for sale online.

We were concerned, first, about the possibility that sensitive military equipment was being sold to would-be terrorists or criminals or hostile nations to the harm of our troops abroad, as well as the rest of us here in the United States.

Second, we were concerned about taxpayer-funded equipment being stolen or otherwise accounted for and sold for profit, especially with respect to any items currently in demand by our service members fighting abroad.

Today we will hear and we will see with our own eyes what the GAO was able to buy online. Unfortunately, the undercover investigators found not only significant amounts of stolen goods being sold for profit; they also were able to buy sensitive technology and equipment we wouldn't want to fall into the hands of our enemies.

GAO was able to buy, for example, F–14 aircraft parts; sophisticated night vision goggles; infrared tabs worn by our troops to differentiate friend from foe; a complete current issue of a U.S. military uniform; nuclear, biological, and chemical protective gear; and body armor currently worn by our troops—just to name a few items.

It doesn't take a whole lot of imagination to understand the troubling nature of some of these items being sold online. For instance, Iran is the only country currently operating F–14s.

The type of night vision goggles purchased on eBay, because of its ability to read infrared tabs worn by our soldiers, could be used by our enemies to easily locate U.S. troops on the battlefield. A leading manufacturer was previously fined $100 million for selling sensitive technologies found in night vision goggles to China.

Just over a year ago, insurgents dressed in American combat uniforms raided a security post in Karbala, Iraq, killing five American soldiers.

And what are the ramifications of having for sale online body armor and nuclear, biological, and chemical protective gear our troops are currently using? What are the homeland security concerns? Could an enemy who buys these items probe them for weaknesses and countermeasures?

What the undercover GAO special investigator found, and the ease by which they were able to buy these items caused us to call this hearing today. We wanted to bring everyone together in the same room who has a role to play, all in the spirit of constructive oversight, to focus on what we can all do to fix the problem going forward.

We will soon hear from the head of the GAO special investigations unit about the undercover efforts here and their followup investigatory work. We will also get an update from the law enforcement arm of the Department of Defense on their own investigations.

We will then hear from eBay and Craigslist about their respective current efforts to prevent and detect the sale of sensitive stolen military equipment on their Web sites. eBay and Craigslist are certainly different types of organizations. eBay is a for-profit company with thousands of employees and serves as an international marketplace. Craigslist, on the other hand, has a self-described public service mission, with only 25 employees, and maintains city-specific sites.

The subcommittee also, of course, understands that eBay and Craigslist are only part of the e-marketplace, and that there are thousands of other sites out there, many of which operate in the shadows.

We will also hear from the logistics and supply chain experts within the Defense Department and the U.S. Army. The very nature of our global marketplace underscores the vital importance of keeping a very close hold on sensitive military technologies and equipment in the first place.

In other words, we need to ensure that we have robust controls in place, as robust as possible, to minimize the opportunities for items to be siphoned off beyond our control, whether by negligence or by criminal activity.

Of course, if an item does slip through the cracks, we need to have swift and rigorous response to recapture the materiel and punish the wrongdoers.

We also want to make sure that the Defense Department and companies like eBay and Craigslist coordinate as much as possible. We will be asking if there are ways to improve our public/private partnerships with the companies who want to do the right thing to better differentiate between sensitive or stolen items versus those allowed to be sold.

Finally, I should add that today's hearing builds off the oversight work that Mr. Shays spearheaded during his time as chairman of the subcommittee. Through the previous impressive work of the GAO special investigative team, this subcommittee was able to identify and play a helpful role in correcting weaknesses in Defense Department controls regarding excess property.

I want to thank our ranking member for leading those past hearings and for working with me on this current bipartisan and constructive oversight.

We come to this hearing without attributing blame to any single entity and without any cure-all fixes; rather, we felt it was important to bring all the relevant actors and stakeholders together to discuss GAO's investigation and, most importantly, to strategize on what possible actions we can take individually and cooperatively going forward to strengthen our controls.

[The prepared statement of Hon. John F. Tierney follows:]

FROM THE OFFICE OF JOHN F. TIERNEY
Representing Massachusetts's 6th District

For Immediate Release
April 10, 2008

Contact: Catherine Ribeiro
(202) 225-8020

NATIONAL SECURITY SUBCOMMITTEE HEARING

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

WASHINGTON, DC —Today, the Subcommittee on National Security and Foreign Affairs investigated the sale of sensitive, in-demand military technologies and supplies on Internet sites such as eBay and Craigslist. Specifically, the Subcommittee heard the results of an undercover investigation Chairman Tierney tasked the Special Investigations Unit of the Government Accountability Office (GAO) with undertaking. The GAO team showed the Subcommittee the items they were able to purchase on-line and explained how the deals were consummated. Representatives from the Department of Defense and eBay, among others, discussed whether controls should be tightened and what possibilities there are for conducting better screening to discover stolen or sensitive equipment and supplies.

A copy of Chairman Tierney's opening statement as prepared for delivery is below:

Statement of John F. Tierney
Chairman
National Security and Foreign Affairs Subcommittee
"Investigation into the Sale of Sensitive, In-Demand Military Equipment and Supplies on the Internet"
As Prepared for Delivery
April 10, 2008

Good morning, and welcome.

Last summer, this Subcommittee – on a bipartisan basis – asked the special investigators at the Government Accountability Office to begin an undercover operation into whether sensitive and stolen military equipment and supplies were being sold on the Internet on such sites as eBay and Craigslist. We also asked GAO to investigate how such items were acquired and able to be put for sale on-line.

We were concerned, first, about the possibility of sensitive military equipment being sold to would-be terrorists, criminals, or hostile nations to the harm of our troops abroad as well as the rest of us here in the United States.

Second, we were concerned about taxpayer-funded equipment being stolen or otherwise accounted for and sold for profit, especially with respect to any items currently in-demand by our service-members fighting abroad.

Today, we will hear – and we will see for our own eyes – what the GAO was able to buy on-line.

Unfortunately, the undercover investigators found not only significant amounts of stolen goods being sold for profit, they also were able to buy sensitive technology and equipment we wouldn't want to fall into the hands of our enemies.

GAO was able to buy, for example, F-14 aircraft parts; sophisticated night vision goggles; infrared tabs worn by our troops to differentiate friend from foe; a complete, current-issue U.S. military uniform; nuclear, biological, and chemical protective gear, and body armor currently worn by our troops; just to name a few.

And it doesn't take a whole lot of imagination to understand the troubling nature of some of these items being sold on-line.

For instance, Iran is the only country currently operating F-14s.

The type of night vision goggles purchased on eBay, because of its ability to read infrared tabs worn by our soldiers, could be used by our enemies to easily locate U.S. troops on the battlefield. A leading manufacturer was previously fined $100 million for selling sensitive technologies found in night-vision goggles to China.

Just over a year ago, insurgents dressed in American combat uniforms raided a security post in Karbala, Iraq, killing five American soldiers.

And what are the ramifications of having for sale on-line body armor and nuclear, biological, and chemical protective gear our troops are currently using? What are the homeland security concerns? Or, could an enemy who buys these items probe them for weaknesses and countermeasures?

What the undercover GAO special investigators found – and the ease by which they were able to buy these items – caused us to call this hearing today. We wanted to bring everyone together in the same room who has a role to play, all in the spirit of constructive oversight focused on what we can all do to fix this problem going forward.

We'll soon hear from the head of GAO's Special Investigations Unit about their undercover efforts here and their follow-up investigatory work. We'll also get an update from the law enforcement arm of the Department of Defense on their own investigations.

We'll then hear from eBay and Craigslist about their respective, current efforts to prevent and detect the sale of sensitive and stolen military equipment on their websites. EBay and Craiglist are certainly different types of organizations. Ebay is a for-profit company with thousands of employees and serves as an international marketplace. Craigslist, on the other hand, has a self-described "public service mission" with only 25 employees and maintains city-specific sites.

The Subcommittee also, of course, understands that eBay and Craigslist are only a part of the e-marketplace, and that there are thousands of other sites out there, many of which operate in the shadows.

We'll also hear from the logistics and supply chain experts within the Defense Department and the U.S. Army. The very nature of our global marketplace underscores the vital importance of keeping a very close hold on sensitive military technologies and equipment in the first place. In other words, we need to ensure that we have as robust controls in place as possible to minimize the opportunities for items to be siphoned off beyond our control, whether by negligence or by criminal activity.

And, or course, if an item does slip through the cracks, we need to have a swift and rigorous response to recapture the material and to punish those wrongdoers.

We also want to make sure that the Defense Department and companies like eBay and Craigslist coordinate as much as possible. We'll be asking if there ways to improve our public-private partnership so that companies who want to do the right thing can better differentiate between sensitive or stolen items versus those allowed to be sold.

Finally, I should add that today's hearing builds off of the oversight work that Mr. Shays spearheaded during his time as Chairman of this Subcommittee. Through the previous impressive work of the GAO special investigative team, this Subcommittee was able to identify and play a helpful role in correcting weaknesses in Defense Department controls regarding excess property. I want to thank our Ranking Member for leading those past hearings, and for working with me on this current bipartisan and constructive oversight effort.

We come to this hearing without attributing blame to any single entity and without any cure-all fixes. Rather, we felt it was important to bring all the relevant actors and stakeholders together to discuss GAO's investigation and, most importantly, to strategize on what possible actions we can take individually and cooperatively going forward to strengthen our controls.

I now turn to Mr. Shays for your opening remarks.

-30-

Mr. TIERNEY. I now turn to Mr. Shays for his opening remarks. Mr. Shays.

Mr. SHAYS. Thank you, Mr. Chairman, for continuing the work of this subcommittee concerning the Department of Defense's controls on sensitive military equipment.

In 2002 our subcommittee discovered DOD had been selling top-grade chemical protective suits to the public, while military units were waiting in line to acquire the same gear. In 2003 we determined DOD was selling items on the Internet that could be used to make a biological warfare laboratory. The equipment was being sold for pennies on the dollar.

At a June 2005 subcommittee hearing we learned DOD was transferring, donating, or selling excess property in new or good condition, while at the same time purchasing similar items for our soldiers.

At a July 2006 subcommittee hearing we confirmed, through a Government Accountability Office investigation, sensitive military equipment was being sold or given to the public.

As a direct result of this subcommittee's oversight, DOD has improved its procedures for processing and disposing of military equipment. A July 2007 entitled Sales of Sensitive Military Property to the Public confirmed these improvements. However, a recent GAO investigation discovered night vision goggles, F–14 parts, body armor, and infrared tape are being sold on the Internet.

Today's hearing focuses on the actions needed to prevent sensitive military equipment from being sold to the public. These items were not bought directly from DOD, as they had been in the past; they were provided by private citizens in legal possession of the equipment, by individuals who had stolen the equipment, or by authorized vendors not following established industrial guidelines.

We are pleased to have representatives from eBay and Craigslist at our hearing to help us better understand how we can prevent sensitive items from being sold on the Internet in the future.

I will be interested in hearing how they have cooperated with Government agencies and local law enforcement officials. For example, I am interested in learning how information channels can be streamlined and how this can be incorporated into an industrial standard. eBay and Craigslist are only two of many companies, but all must cooperate.

The military newspaper, "Stars and Stripes," published an article detailing the court martial proceedings for a soldier who stole and sold body armor, protective masks, and helmets on the Internet. The soldier is serving a 30-month sentence for these actions. Hopefully this will be a deterrent to others thinking about stealing unauthorized military equipment.

At this point I am not sure if we have a supply accountability problem, a law enforcement issue, or both. I look forward to the witnesses to sort this out, as well.

The July 2007 GAO report describes the comprehensive changes and programs implemented by the DOD, and they should be commended for these improvements. With this in mind, Mr. Chairman, I look forward to the testimony of our distinguished witnesses and thank each of them for being here today, and particularly thank

you for conducting this hearing and continuing this investigation on such a bipartisan basis.

Mr. TIERNEY. Thank you, Mr. Shays.

We will now receive testimony from our witnesses. I want to begin by introducing the witnesses on our first panel.

Mr. Greg Kutz is the Managing Director of the Forensic Audits and Special Investigations Team of the U.S. Government Accountability Office. Mr. Kutz joined GAO in 1991 and has served as point for countless previous investigations, including Hurricane Katrina fraud, waste, and abuse; military pay problems; credit card and travel fraud and abuse; and security issues such as airport security, border security, and security over the purchase and transportation of radioactive materials.

Mr. Kutz, the subcommittee thanks you and Rick Nobold and everybody else on your team for the conscientious work done here. Your efforts in helping to provide independent oversight are greatly appreciated and extremely important.

We also welcome Mr. Charles W. Beardall, who is the Deputy Inspector General for Investigations at the Department of Defense Office of the Inspector General. Prior to his appointment, Mr. Beardall served as the Director of the Defense Criminal Investigative Service, the criminal investigative arm of the Defense Department Inspector General.

Mr. Todd Cohen is the vice president and deputy general counsel for Government relations at eBay, Inc. Mr. Cohen joined eBay in 2000 as its first full-time public policy employee. Since 2004 he has led eBay's global government relations efforts.

And Mr. Jim Buckmaster is CEO of Craigslist.org. Mr. Buckmaster has led Craigslist since 2000. He has also served as chief technology officer and lead programmer.

Again, I want to welcome all of you and thank you for being here today.

It is the policy of this subcommittee to swear in people before they testify, so I would ask you to stand please and raise your right arm. If there is anybody else that is going to be testifying with you, I would ask them also to stand and be sworn.

[Witnesses sworn.]

Mr. TIERNEY. The record will please reflect that all of the witnesses answered in the affirmative.

Your full written statements will be placed on the record, so you don't have to feel compelled to be married to the written statement. But we would like you to put it in about a 5-minute block so that we can get some time to go back and forth with questions.

Mr. Kutz, we will begin with you. We are going to give you a little longer because, of course, your investigation is the subject of this hearing and we want you to feel free to make a complete presentation.

Thank you.

STATEMENTS OF GREGORY D. KUTZ, MANAGING DIRECTOR, FORENSIC AUDITS AND SPECIAL INVESTIGATIONS, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; CHARLES W. BEARDALL, DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS, U.S. DEPARTMENT OF DEFENSE; TOD COHEN, VICE PRESIDENT, GOVERNMENT RELATIONS, EBAY INC.; AND JIM BUCKMASTER, CHIEF EXECUTIVE OFFICER, CRAIGSLIST.ORG

STATEMENT OF GREGORY D. KUTZ

Mr. KUTZ. Mr. Chairman and members of the subcommittee, thank you for the opportunity to discuss the sales of military property on eBay and Craigslist. Previously I testified before this subcommittee that DOD was selling sensitive military property through its excess property system. Today's testimony responds to your request that we investigate the sales of military property on eBay and Craigslist.

My testimony has two parts. First, I will discuss what we did and provide you with some background; second, I will discuss the results of our investigation.

First, this investigation was done primarily as an undercover operation. For all of our purchases we posed as a bogus private citizen with only a credit card, mailbox, and a telephone necessary for this operation. Most of the purchases we made were on eBay. We appreciate the cooperation of eBay's fraud investigation team throughout this investigation.

Several of our purchases were also made on Craigslist, which serves as an Internet version of the newspaper classified ads.

Major criminal cases in the last year highlight the importance of protecting sensitive military property. For example, in April 2007 an individual pled guilty to selling night vision devices to a terrorist organization in Sri Lanka.

In May 2007 an individual was sentenced for illegally exporting F–14 parts to Iran. A search of his home led to the seizure of over 13,000 aircraft parts and a shopping list provided to him by a military officer from Iran.

And in September 2007 an Air Force staff sergeant pled guilty to charges of stealing military night vision goggles to sell overseas.

These are just a few of the hundreds of cases related to sales of sensitive military property to places such as Iran and China.

I provide this background because our undercover operation could have easily been financed by China, Iran, or a terrorist organization looking to acquire U.S. military property, which leads to the second part of my testimony: the results of our investigation.

Overall our undercover investigators purchased a dozen sensitive military items to show just how easy it was for anybody to obtain them. Once in possession of this property, we could have resold it to an international broker or shipped it overseas.

According to DOD, the sensitive items that we purchased are U.S. munitions list items. These items require Government approval before they can be exported. Some of these items could also be reverse engineered to develop similar technology or used, as the chairman said, to develop countermeasures. These items would also be useful to terrorists or criminals right here in the United States.

A recent Craigslist ad touted military body army as "a must-have for gangsters."

The majority of the items that we purchased are displayed on the table to my right. Let me discuss the items that are the most disturbing or troubling to me, which I will also show on the monitor as I go through this discussion.

First, I have in my hand this new, unused F–14 antenna wave guide. This item is part of the F–14 radar warning system. Iran is the only country with operational F–14 fighter jets.

Second, I have in my hand these new and unused night vision goggles. These goggles are a critical part of the U.S. night fighting system because of an image intensifier tube. This tube allows U.S. soldiers in Iraq and Afghanistan to distinguish friendly fighters wearing infrared tabs from the enemy at night.

Third, we have on the hanger to my right an Army combat uniform [ACU], and associated gear on the table. Why is this troubling? Because, as the chairman said, in January 2007 insurgents wearing U.S. military uniforms passed through security, entered a compound in Karbala and killed five U.S. soldiers. In addition, this ACU has the infrared tabs I mentioned, which would allow enemy fighters to pose as friendlies at night.

Fourth, we have the body armor on the table. The enhanced small arm protective inserts [ESAPIs], are currently used in body armor worn by our troops in Iraq and Afghanistan.

In addition to these purchases, we identified other sensitive military property that was also sold to the highest bidder. Examples include hundreds of sets of military body armor, dozens of aircraft and helicopter parts, additional night vision goggles, and ACUs. High bidders on some of these items were from places such as Hong Kong, Russia, Thailand, Costa Rica, Hungary, and Singapore.

Most of the military property that we purchased was stolen. For example, two sellers with eBay storefronts bought stolen property from service members and resold it on eBay. Examples of this property include kevlar helmets, gas masks, and additional ACUs.

I have in my hand this military meal ready to eat [MRE]. We identified a robust Internet market for the sales of these stolen MREs. For example, we identified two individuals that each sold over $50,000 of MREs stolen from nearby military bases.

We also identified a soldier at Camp Casey in South Korea who sold us MREs on eBay. After we referred him to the Army Criminal Investigative Division, they determined that he was responsible for numerous thefts at the camp. This eBay seller is now serving a 3½ year sentence in prison.

In conclusion, we believe that the technology used by our soldiers on the battlefield today should not be available to the highest bidder. Ironically, eBay prohibits the sales of used cosmetics, while at the same time the latest in military body armor is available to anybody with a credit card.

Our soldiers deserve better than to have our own technology used against them on the battlefield.

Mr. Chairman, that ends my statement. I look forward to your questions.

[The prepared statement of Mr. Kutz follows:]

United States Government Accountability Office

GAO

Testimony

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

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

GAO-08-644T

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

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.

April 10, 2008

INTERNET SALES

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

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 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	eBay	▪ 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	▪ 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 other body armor items offered by this seller included individuals in China (Hong Kong), Taiwan, and Singapore ▪ Stolen from U.S. military or manufacturer

Source: GAO.

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 (MRE) 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.

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 components 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 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,

[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 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-05-277 (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-04-15NI (Washington, D.C.: Nov. 19, 2003).

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.

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 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

[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.

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. 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 DOD.

In addition to the above case studies, our investigators identified examples of U.S. government 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 (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 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 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.

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 DOD's Defense Logistics Information Service, 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.

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

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 examples of U.S. 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 many 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 2 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	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 Blackhawk, Apache, and Chinook helicopters • Components 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

Case	Item	Seller location	Web site	Case details
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 gave 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 body armor offered by this seller included individuals in China (Hong Kong), Poland, Taiwan, and Singapore • Stolen from government or manufacturer
9	Body armor/SAPIs	Fayetteville, N.C.	Craigslist	• Items 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

Case	Item	Seller location	Web site	Case details
10	Body armor/SAPIs	Minot, N.D.	eBay	• Items 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

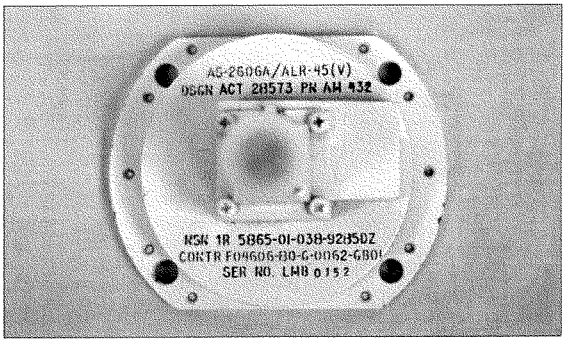
Source: GAO.

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 plate. 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

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 code 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 components. 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 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.

Figure 2: F-14 Antenna Purchased from eBay Seller



Source: GAO.

Case 2: Helicopter Antenna

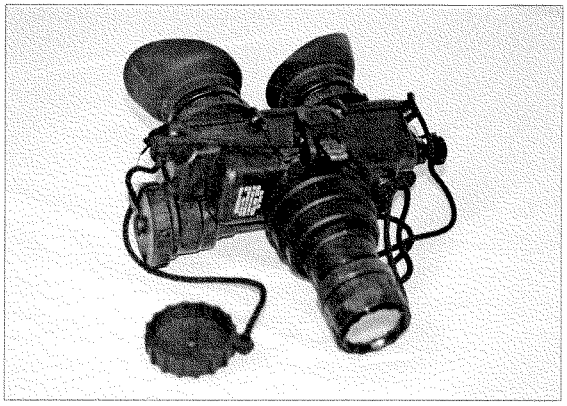
On September 19, 2007, we purchased a used flush-mount antenna, which is currently in use by the military in the Blackhawk, Apache, and Chinook helicopters, from an eBay seller located in The Colony, Texas. This city is located about 130 miles from Sheppard Air Force Base. The antenna is assigned demil 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 components 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 said he 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 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 former 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. According to the manufacturer, these tabs have the same properties as the IR tabs affixed to ACUs 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 (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, used 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 the NBC suit 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. 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 SAPIs, including two current-issue E-SAPIs, on

eBay and Craigslist. 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

to be affiliated with the U.S. military, had completed eBay auctions of over 600 body-armor-related items totaling approximately $60,000. Much 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 auctions for other body armor items 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 examples of U.S. government property—both sensitive and nonsensitive—that was likely 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 selected 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.	3 helmets and miscellaneous gear
2	Sergeant (E-5)	Army (active)	Fort Dix, N.J.	Flak vest and miscellaneous gear
3	Specialist (E-4)	Not serving	N/A	2 Kevlar helmets, distress markers, and weapons-related gear
4	Specialist (E-4)	Army (active)	Fort Irwin, Calif.	Flak vest and gas mask
5	Specialist (E-4)	Army (reserve)	Portsmouth, Va.	Helmet and miscellaneous gear
6	Private First Class (E-2)	Marine Corps (active)	Twenty-nine Palms, Calif.	27 head mounts (possibly for night vision goggles)
7	Private (E-1)	Not serving	N/A	Flak vest

Source: Barstow, California, gun-store owner; DEIDS.

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

[5]18 U.S.C. § 641.

review and criminal investigation.[6] We have not received specific 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 military's night-fighting system. IR tabs on ACUs are demil code D. 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 military. Table 4 contains details about selected 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 a Military Surplus Store Owner in Abilene, Texas

No.	Rank	Branch	Current assignment	Items sold to store owner
1	Master Sergeant (E-7)	Not serving	N/A	8 flight suits, 2 flight jackets, 15 battle dress uniforms (BDU)
2	Staff Sergeant (E-5)*	Air Force (active)	Dyess Air Force Base, Tex.	5 Kevlar vests
3	Staff Sergeant (E-5)	Air Force (active)	Kunsan Air Force Base, South Korea	Helmets
4	Senior Airman (E-4)*	Air Force (active)	Dyess Air Force Base, Tex.	9 BDUs
5	Senior Airman (E-4)	Air Force (active)	Dyess Air Force Base, Tex.	Gas mask and filters, BDUs

Source: Abilene, Texas, military surplus store owner; DEIDS.

*The records provided by the store owner listed the name of the service member's spouse. DEIDS includes the names of spouses.

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

[6]GAO-06-410R.

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[7] 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

[7]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.

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. 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 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 defense-related items we purchased were not removed by eBay and Craigslist Web site administrators, 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
Prohibited items list includes stolen items?	Yes	Yes
Prohibited items list includes items that have not been demilitarized (i.e., sensitive defense-related items)?	Yes, but is listed only under the "Firearms, Weapons, and Knives" category related to ordnance	Not explicitly mentioned
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; does not require subpoena to disclose seller information	One individual at Craigslist is tasked to work with law enforcement and requires subpoena to disclose seller information
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 officials.

eBay

Advertisements for the sensitive 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 Seller" status, and suspend accounts.

Craigslist

Advertisements for the sensitive 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, 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.

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, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."
Order by Mail or Phone	The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to: U.S. Government Accountability Office 441 G Street NW, Room LM Washington, DC 20548 To order by Phone: Voice: (202) 512-6000 TDD: (202) 512-2537 Fax: (202) 512-6061
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

Mr. TIERNEY. Again, thank you, Mr. Kutz, and your staff, as well, for that investigation and for the report.

Mr. Beardall.

STATEMENT OF CHARLES W. BEARDALL

Mr. BEARDALL. Chairman Tierney, Chairman Shays, distinguished members of the Subcommittee on National Security and Foreign Affairs, thank you for the opportunity to appear before you to discuss the DOD Office of the Inspector General's role in stemming the theft, diversion, and sale of sensitive military materiel, especially on the Internet.

Consistent with our mission of protecting America's war fighters, the Defense Criminal Investigative Service, the law enforcement arm of the DOD Inspector General, has been actively engaged in investigating the theft, diversion, and sale of sensitive military technologies since the early 1990's. These investigations joined terrorism, major procurement fraud, corruption, and the protection of the global information grid as DCIS' top five priorities.

DCIS technology protection investigations now comprise 20 percent of our caseload. Also, 90 percent of DCIS undercover operations focus on technology protection. DCIS comprises 340 of America's finest, most dedicated special agents. They are assigned to offices nationwide and in Europe and Southwest Asia. DCIS has broad investigative jurisdiction over DOD programs and operations, including technology protection. We are recognized as a major partner in the battle against proliferation and illicit technology transfers. Yet, despite broad commitment, manpower limitations restrict DCIS from becoming involved in all investigations involving theft and sale of DOD equipment; therefore, we focus on the most serious or threatening offenses.

Most investigations involve foreign nationals contacting Defense contractors to obtain control of technologies and U.S. munitions list items for export to proscribed nations. Popular items are missiles, UAVs, M–16 and M–4 rifles, night vision goggles, aircraft parts, and components for weapons of mass destruction.

DCIS also investigates disposal of military equipment that is not properly demilitarized, particularly items that threaten the U.S.'s interests or our export control.

A few example provide a vivid illustration of the investigation DCIS conducts in technology protection. In July 2005 an Iranian citizen was sentenced to 57 months confinement for attempting to export aircraft component parts for F–4 and F–14 fighters to Iran. One component the individual attempted to export was a Vulcan six-barrel drum which feeds ammunition into a Gatling gun used in military aircraft. The weapon can fire 6,000 rounds of ammunition per minute.

Also, over a 2-year period DCIS and the Immigration and Customs Enforcement agents investigated a covert agent of the People's Republic of China who was seeking to procure up to 70 Black Hawk helicopter engines, several F–16 engines, and air-to-air and air-to-ground missiles. The subject was induced to travel to the United States, where undercover agents showed him an F–16 engine. He wired $140,000 to an undercover bank account and was arrested. He was convicted of export violations, bribery of a public

official, and being a covert agent of the PRC. In July 2006 he was sentenced to 6½ years confinement and fined $1 million.

DCIS and partner agencies regularly use undercover operations to stop illegal technology transactions, including searching Internet Web sites for controlled military items. One significant undercover operation targeting illegal sales on the Internet was DCIS' Operation High Bidder, initiated in 2003, and, frankly, continuing today with other efforts. The operation identified numerous sales of military grade body armor on eBay. High Bidder resulted in 183 investigative reports, from which 139 cases were opened, 51 criminal charges were filed, that resulted in 44 persons being convicted and sentenced to a total of 48 years confinement and over $400,000 in fines.

The unquantifiable benefits of High Bidder are reduced number of sales of certain controlled items and greater public confidence that DOD is policing these illegal sales.

A DCIS High Bidder vulnerability report was provided to Defense Logistics Agency and the DOD Office of Supply Chain Integration. DCIS also prepared a criminal intelligence report warning military and law enforcement organizations of the availability of stolen body armor and other military equipment to potential terrorists and criminals.

We note that eBay supported High Bidder and the operation resulted in the installation of filters to identify body armor and related items, and we keep on trying to refine those filters.

I conclude by emphasizing that to protect America's war fighters, allies, and our citizens, the DOD Office of Inspector General remains steadfastly committed to aggressively countering the illegal sales of sensitive DOD equipment and technology, including those on the Internet. We will continue to keep Congress and the DOD leadership fully and promptly informed regarding our efforts.

I look forward to your questions.

[The prepared statement of Mr. Beardall follows:]

April 10, 2008

Expected Release
10:00 a.m.

Charles W. Beardall

Deputy Inspector General for Investigations
Department of Defense

before the

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

on

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Mr. TIERNEY. Thank you, sir.
Mr. Cohen.

STATEMENT OF TOD COHEN

Mr. COHEN. Chairman Tierney, Ranking Member Shays, members of the committee, my name is Tod Cohen, and I am vice president and deputy Government counsel for Government relations at eBay, Inc. I would like to thank the committee for giving eBay this opportunity to discuss the sale of military items on our site, and I ask that my full statement be entered into the record.

Mr. TIERNEY. It will be entered in, as I said.

Mr. COHEN. One of my focuses in my 8-year career at eBay has been to make sure that we work closely with governments around the world to keep our site as safe as possible for our community of users and for our communities, in general. We seek to achieve this goal by working with government experts to create clear, effective rules regarding what can and cannot be listed for sale on our site, and then aggressively enforce those rules.

We partner with law enforcement agencies proactively and reactively to make sure that sellers who break the law get prosecuted.

Since 1995, eBay has created prohibited and restricted item policies covering over 60 classifications of items, including firearms, prescription drugs, counterfeit goods, and drug paraphernalia, to name just a few. We have developed industry-leading advanced programs to identify suspicious items and user behaviors. We have teams of people in place around the world and around the clock to review and remove items that are flagged by our systems. We sanction and remove members who engage in harmful practices and we have, as mentioned, a global fraud investigations team that partners with law enforcement to make sure that criminals get prosecuted to the fullest extent of the law.

Let me provide some sense of scale to our efforts and our challenges. We have trading platforms in 39 markets, with over 82 million active users worldwide. At any one time, around 113 million items are listed for sale, with more than 6 to 7 million new items listed 24 hours a day, 7 days a week, 365 days a year. With such high volumes, we must work closely with regulatory and law enforcement agencies to police against abuses, both intentional and unintentional. We work with them to determine the key words and phrases that are commonly used to describe the goods that we would want to prevent from being available for sale.

One of our 60 prohibited item policies concerns the sale of military items. It essentially prohibits the sale of military items that have not been disposed in accordance with Department of Defense regulations. We have worked on these policies with national security experts at the Defense Criminal Investigative Service, the Government Accountability Office, the Department of Defense, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations, among others. We work with Government experts to build detection tools to flag listings for items such as body armor and MREs.

The goal is to identify items that cannot be sold commercially. We build the technology filters, test them, get extensive input and

followup from Defense agencies, and then use them to flag suspicious listings.

To give you just one example, in 2007 we reviewed 4,273 listings flagged by our body armor filters we developed with the help of DCIS and removed 1,278 listings from eBay. The nearly three-quarters that were not removed were deemed to be false positive, and the listings were allowed to remain active.

Our fraud investigative team has also assisted in a number of cases involving the illegal sale of body armor by providing seller information to DCIS and other enforcement agencies. When we receive a request for member records from GAO or one of the military investigative services, we respond quickly.

Our goal is to make it as easy as possible for these agencies to prosecute criminals, and we work tirelessly to attain this goal, including having investigators appear as witnesses to support prosecutions.

To sum up, we believe that eBay has the most proactive policies and tools to combat fraud and illegal activity of all the major Internet commerce companies. There are over 2,000 eBay, Inc. employees around the world working to combat all forms of harmful behaviors on our site, including the sale of illegal or stolen items.

As we have grown in business over the last 12 years, we have dedicated more and more resources to this fight. We believe our programs are not only best in class on the Internet; we also believe that they match up and surpass offline retailers and marketplace efforts.

Simply put, eBay is no place for the sale of stolen or illegal military goods. The transparency of our site, our rules, our enforcement tools, and our commitment to working with law enforcement makes it an unwelcome venue for criminals seeking to fence these goods.

We look forward to working with this committee and our partners in the military and Federal Government agencies on ways to more effectively prevent stolen or illegal military items from being listed on our site.

We very much appreciate the opportunity to participate in this important hearing, and thank you for your time and consideration.

[The prepared statement of Mr. Cohen follows:]

The Written Testimony of
Tod Cohen, Esq.
Vice President and Deputy General Counsel for Government Relations
eBay Inc.

Before the House Subcommittee on Government Oversight and Oversight Reform
Subcommittee on National Security and Foreign Affairs
April 10, 2008

Mr. Chairman Tierney, Ranking Member Shays, and members of the Committee,

My name is Tod Cohen, and I am Vice President and Deputy General Counsel for Government Relations at eBay Inc. I would like to thank the Committee for giving eBay this opportunity to discuss the sale of certain military items on our site, and I ask that my full statement be entered into the committee record.

My 8-year career at eBay has been focused on making sure that we work closely with government agencies to keep our site safe for our community of users. We seek to achieve this goal by working with government experts to create clear, effective rules regarding what can and cannot be listed for sale on our site and then aggressively enforcing those rules. We also partner with law enforcement agencies proactively and reactively to make sure that sellers who break the law get prosecuted. When eBay first emerged as a dynamic way for people to buy and sell items online back in 1995, there were really no rules in place for our users to follow and there was no team of investigators ready to help law enforcement prosecute criminals who abused our platform. The company realized in those early years that in order to become a truly safe and trusted e-commerce site we needed to put policies and tools in place to make sure that illegal items and harmful sellers were quickly identified and removed from our platform.

We created prohibited and restricted items policies and built tools using state-of-the art technology to enforce those policies. We developed advanced programs to identify suspicious behavior, remove members who engaged in harmful practices and take steps to keep them from coming back on the site. And we established a global Fraud Investigations Team to partner with law enforcement to make sure that criminals who seek to abuse our community of users get prosecuted to the fullest extent of the law. Largely as a result of these efforts, we now have trading platforms in 39 markets with over 82 million active users worldwide. At any one time, around 113 million items are listed for sale on eBay worldwide. Six to seven million new items get listed everyday. With such a high listing volume on our sites, it is a challenge to enforce our policies—but a challenge we must meet to be successful. The only way to meet that challenge is to work closely with regulatory and law enforcement agencies like the ones represented here today.

The "rules of the road" for sellers on eBay consists of over 60 separate prohibited and restricted items policies. These policies cover everything from firearms to prescription drugs to counterfeit goods to drug paraphernalia – all things that we do not allow to be listed on our site. We work with subject matter experts in the law enforcement and government agency communities to make sure these policies are accurate and that we enforce them effectively.

We have detection tools in place that flag listings that may violate one or more of our policies, and we have teams of agents all over the world that review these listings 24/7 and remove any listings that are found to be in violation. These tools utilize key words and phrases that are commonly used to describe the goods that we want to prevent from being sold on eBay.

In many cases, we obtain these words and phrases directly from the government agency that oversees a particular prohibited item, as those agencies have the latest and most useful information that we need to build effective detection tools. Once an item is flagged and deemed to violate one of our policies by the reviewing agent, we remove the item and take action against that seller ranging from a warning to a listing limitation to outright suspension of all eBay privileges, depending on the egregiousness of the violation. In some cases where a knowing violation of the law is apparent, we will refer a suspended seller to law enforcement for investigation.

One of our 60 prohibited items policies concerns the sale of military items—it is found within our policy on Firearms, Weapons and Knives. Any eBay user can find a link to our policy page at the bottom of every single page on the eBay site, our rules are not hard to find. I have copies of that policy should the Committee like to review it, but it essentially prohibits the sale of military items that have not been disposed of in accordance with Department of Defense regulations. It also prohibits the sale of all military ordnance, whether or not the item has been "demilled" or made "unserviceable." The policy also prohibits the sale of hand grenades. We have worked over the years with branches of the military as well as federal government agencies to effectively enforce this policy.

One example of this cooperative effort is our work to prevent the illegal sale of military body armor on eBay. Three years ago we started working with staff from the Defense Criminal Investigative Service (DCIS) in Raleigh, North Carolina after they brought it to our attention that some eBay sellers were listing body armor on our site that is not permitted to be resold under Department of Defense regulations. We have also worked with DCIS staff in Philadelphia on this issue.

We worked closely with both teams to build detection tools to flag listings of potentially illegal body armor while allowing the sale of certain types of armor that are legal to sell commercially and that can be found at any Army/Navy store. We necessarily depended on the DCIS staff to help us, as they are the true experts in this area and were able to give us the key words and terms that would most likely appear in a listing for body armor that cannot be sold commercially.

We established the filters, began a test phase with extensive input and follow-up from DCIS, and eventually developed highly effective tools to flag suspicious body armor listings for review by our agents. In 2007, we reviewed 4273 such listings that were flagged by our body armor filters and removed 1278 from eBay. The ones that were not removed were deemed to be "false positives." Our Fraud Investigations Team has also assisted in a number of cases involving the illegal sale of body armor by providing seller information to DCIS and other enforcement agencies.

Another good example of our efforts is in the area of Meals, Ready-to-Eat, commonly referred to as MREs. We worked with government officials several years ago, predominantly the Defense Supply Center in Philadelphia, to create an effective policy dealing with the sales of these meals to make sure that such transactions be conducted safely and legally. We do not allow the sale of the MREs that come with heating devices called "Flameless Ration Heaters," as those devices can be hazardous when not shipped correctly. We banned these heating devices at the request of the Defense Supply Center back in 2002. In 2007, we flagged 1,039 MRE listings based on the appearance that the meal came with a prohibited heating device and removed 202 listings after review. We also do not allow the sale of expired MREs and require our sellers to state in their listings when the meal will expire. Back in 2004, we set up messaging that appears to anyone that lists an MRE on eBay and puts them on notice of these obligations.

Along with our own internal enforcement efforts, we rely on members of our community as well as our partners in law enforcement and regulatory agencies to report items to us for review and possible removal. As we are dealing with millions of listings, we need a multi-pronged approach to flagging and removing listings that have no business being on eBay. Any eBay member can report an item to us instantly by simply clicking the "Report This Item" link at the bottom of every item listing on eBay. Our government and law enforcement relations teams also act on reports directly from regulatory and law enforcement personnel. In general, if an official from GAO or the Department of Defense contacts us and tells us an item is illegal and needs to be removed, it comes down as soon as possible. We depend on these agencies and our community to supplement our own enforcement efforts in this manner.

In addition to aggressively enforcing our rules and regulating our sellers' activities, our Fraud Investigations Team partners with government and law enforcement agencies to help them investigate and prosecute cases where sellers list illegal items on eBay. We conduct a great deal of outreach with law enforcement agencies in North American America and around the world to make sure they know that we stand ready to help them investigate any illegal practices that involve the use of the eBay platform. Our fraud investigations and outreach teams work closely with the Government Administration Office as well as several investigative units within the U.S. military.

When our team receives a request for member records from GAO or one of the military investigative services, they quickly receive the requested records. Our goal is to make it as easy as possible for these agencies to prosecute criminals that abuse our marketplace, and we work tirelessly to attain this goal. In addition to providing records to help make

the case, our investigators appear as witnesses to support prosecutions of sellers who list stolen or illegal military items.

Just last fall, for example, one of our fraud investigators testified in a court martial case brought by the Office of Special Investigation at Whitman Air Force Base involving the sale of stolen military items including night vision goggles and body armor by a Senior Airman. The defendant was dishonorably discharged and sentenced to 18 months of confinement. As is the case with our prohibited items policy enforcement, we can always do better when it comes to helping law enforcement agencies---military or civilian---bring these important enforcement actions, and we want to work with you and our government partners to do a better job.

We have the most pro-active policies and tools to combat fraud and illegal activity of all the major internet commerce companies. There are over 2,000 eBay Inc. employees around the world working to combat all forms of potentially harmful behavior on our sites, including the sale of illegal or stolen items. As we have grown as a business over the last 12 years, we have dedicated more and more resources to the fight against problematic activity that harms our users.

eBay is no place for the sale of stolen or illegal military goods. The transparency of our site, our rules, enforcement tools, and our commitment to working with law enforcement makes it an unwelcome venue for criminals seeking to "fence" these goods. We look forward to working with this Committee, and our partners in the military and the federal government on ways to more effectively prevent stolen or illegal items from being listed on our site. We very much appreciate the opportunity to participate in this important hearing, and thank you for your time and consideration.

Mr. TIERNEY. Thank you, Mr. Cohen.

Mr. Buckmaster, we appreciate that one-twentyfifth of your company is sitting before us and that you have made the time for us today. Please feel free to take your time.

STATEMENT OF JIM BUCKMASTER

Mr. BUCKMASTER. Chairman Tierney, Congressman Shays, good morning. As introduced, my name is Jim Buckmaster, and I am the CEO of Craigslist.

I would like to thank the subcommittee for inviting me here to participate in today's hearing, and look forward to working together with all of the organizations represented here to solve the problems identified in the GAO report.

Founded in 1995, Craigslist operates local community Web sites for 450 cities featuring classified ad services used by over 25 million Americans each month to find jobs, housing, for sale items, services, friendship, romance, and community information, generating almost 10 billion page views per month.

Nearly all Craigslist services are offered free of charge and without banner ads or text ads or other commercial impediments. Of our revenue, 100 percent comes from fees for job listings in 10 cities and a fee for brokered apartment listings in New York.

I would like to congratulate and thank the authors of the GAO report for their excellent work, but with all due respect I do feel some corrections and amplifications are in order regarding Craigslist, and will mention three of those here.

First, describing Craigslist as "a global marketplace with international reach" is somewhat misleading. Craigslist is a collection of separate, strictly local marketplaces. The for sale section of each local Craigslist site is used nearly exclusively to facilitate in-person, face-to-face transactions. Sales involving shipping are rare and are strongly discouraged by Craigslist, and international sales are extremely rare.

I should hasten to add that, although Craigslist is not close to being a go-to site for international trade in military items, we do not accept any misuse of Craigslist, and are determined to do our very best to eliminate it.

Contrary to what the GAO report implies, Craigslist actually has more people actively engaged in its anti-fraud efforts than any Web site on Earth. In addition to our in-house anti-fraud team numbering a dozen or more staff members and the automated blocking and screening routines we have developed, Craigslist benefits from tens of millions of passionate users diligently reviewing every ad on the site, with each user having the power to delete inappropriate ads, which they do to the tune of several million ads each month.

On the plus side, the GAO investigators did notice that ads were being actively removed from Craigslist as they were searching the site, an observation that they did not make about any other site in their report.

I was surprised that the GAO did not highlight in the report the fact that, unlike every other party cited, Craigslist uniquely earns absolutely nothing from the sale of military items. Military personnel, shopkeepers, online storefronts, Web sites large and small, as cited in the report, all are earning money from each sale of sen-

sitive military equipment, with the largest players undoubtedly reaping many millions of dollars per year from such sales.

It should be noted that, with the exception of Craigslist, each of these parties has a strong financial incentive for failing, or at least delaying, putting an end to this trade. Craigslist has no such incentive, and we are eager to solve this problem.

My humble request to those assembled here is for clear and concise guidelines as to which items are allowed to be sold and which are not. With clear and concise guidelines available, very few of our users will violate them, and those few who do will quickly find themselves blocked, screened, and flagged off of our site.

Without clear and concise guidelines, though, I fear that even the most conscientious efforts to eliminate this trade will struggle. Armed with clear and concise guidelines which we will use to educate our users, our staff, and our blocking and screening software, I am extremely confident that we can quickly reduce the volume of such ads on Craigslist by more than 90 percent.

By the way, I do have an idea for removing all financial disincentives that may delay a solution to this problem. I would like to challenge each party cited in the GAO report to make a commitment to donate 100 percent of any revenue they may have earned in connection with the sale of sensitive and/or stolen military items to charity, preferably one that provides aid to our military veterans.

Although Craigslist has collected no revenue from such sales, as a show of good faith, if each of the other parties is willing to commit to donating all such revenue to charity, past, present, and future, Craigslist would be proud to make a very sizable donation, as well.

I think my 5 minutes are up. Thank you, Mr. Chairman and members of the subcommittee, for inviting me to speak. I look forward to your questions.

[The prepared statement of Mr. Buckmaster follows:]

STATEMENT OF CRAIGSLIST, INC.,

Testimony before

The Subcommittee on National Security and

Foreign Affairs

Committee on Oversight and Government Reform

United States House of Representatives

Jim Buckmaster

Chief Executive Officer

April 10, 2008

****

Craigslist, Inc., owns and operates the "craigslist" internet sites, which provide people in 450 cities worldwide with largely free classified advertisements, along with topical discussion forums and other services. Craigslist supports its entire operations by charging below-market fees for job listings in 10 large cities and for brokered apartment listings in New York City. More than 30 million people use craigslist each month, including more than 25 million people in the United States. Craigslist users submit more than 30 million new classified ads each month, and generate 10 billion page views per month. Craigslist's usage has grown by 100% or more in each of its 13 years of existence.

eBay, Inc. owns a minority stake in craigslist. However, eBay does not have a representative on the craigslist board of directors, and the two companies operate completely independently.

Craigslist believes that its success is a direct result of unusual focus on public service, with business metrics such as revenue, profits and market share largely left to take care of themselves.

****

My name is Jim Buckmaster. I am the Chief Executive Officer of craigslist, Inc., which owns and operates the "craigslist" website. Craigslist's sole place of business is in San Francisco, California, but from this one office and from servers located in San Francisco we host local community web sites featuring self-service and largely free classified advertisements, including jobs, housing, for sale, services, personals and community information for 450 local cities, worldwide.

Craigslist's Sources of Revenues.

Craigslist's revenues come from only two sources: paid job listings in 10 US metropolitan areas, and paid advertisements for brokered apartments in New York City. Craigslist does not accept paid "banner" advertisements, does not serve paid "text ads", "pop up" ads, or any other kind of display advertising, and does not engage in affiliate marketing, email marketing, or any of the dozens of other ways internet companies typically derive revenue. More than 99% of classified ads on craigslist are free of charge, including most job ads, nearly all housing ads, all services ads, all community and event ads, and all "for sale" ads. I can say unequivocally that craigslist did not collect so much as a penny on any of the transactions involving sale of military equipment to undercover agents that are the topic of today's hearing.

How Sale Transactions are Completed on Craigslist.

Craigslist's service is essentially an online version of the traditional local newspaper classified advertisement. A person wishing to post a "for sale" advertisement on craigslist first visits the craigslist web site for their city, where the sale is to take place, clicks on the "post to classifieds" link, which then leads through a series of prompts that results in the advertisement being placed "live" on craigslist. "For Sale" advertisements are categorized by the type of good being sold. Although there is a catch-all "General for Sale" category, it is worth noting that there are no specific categories that are applicable to military equipment or paraphernalia.

Someone can respond to a craigslist advertisement either by replying to the email or, as is often the case, calling a local telephone number included as part of the advertisement. Local people in the same community seeking to buy and sell goods thus use craigslist to meet one another, much like people in the same community also use newspaper advertisements to meet one another. Craigslist operates as a local venue where people can find others in their city or area with complementary needs, and arrange to meet, as job applicant and interviewer, apartment seeker and prospective landlord, potential boyfriend and girlfriend, or buyer and seller. In the case of a "for sale" ad, once the initial connection is made, craigslist has no further involvement in any transaction that may take place. We do not remain as a party to the dialogue between buyers and sellers, and in fact, our site is engineered so that if a person placing an advertisement wishes to respond to someone who has replied to the initial advertisement, the response *cannot* be through our servers. We also are not a financial intermediary, neither facilitating payment, receiving a commission or other compensation, or even being aware that a sale has taken place.

Craigslist Transactions are Intended to be Local.

Significantly, an advertisement can be posted in only one of craigslist's 450 cities. There is no function permitting an advertisement to be posted throughout craigslist. In fact, posting the same

advertisement to multiple cities or areas violates craigslist's terms of use, and we have implemented technical measures to prevent cross-posting to multiple areas. Similarly, the search feature within craigslist is restricted to searching one city site, and it is not possible to conduct a broad geographic search. If someone wishes to search on craigslist for military equipment, that person would need to perform 450 individual searches, one for each local craigslist site, in order to search all of craigslist.

We also discourage long-distance transactions that are completed by mail, shipping or other means. In fact, users of craigslist are also cautioned that the most effective way to avoid online "scams" is to deal only with local people they meet face-to-face. Limiting interactions between buyers and sellers on craigslist to local transactions is intentional and is one of the primary distinctions between craigslist (which is intended to facilitate local communication and face-to-face meetings) and the other large internet sites (which are intended to facilitate global communication, generally without face-to-face meetings). If we wanted to permit national or international postings or searches, we of course could do so. However, we believe that creation of a marketplace of national or international scale would detract from the community nature of craigslist. In short, the "for sale" section of craigslist is specifically intended to facilitate "face-to-face" meetings and local in-person transactions. As a result, craigslist is not a good forum to use if someone wants to offer something for sale to a national or worldwide marketplace.

Craigslist's Terms of Use.

Craigslist's terms of use constitute a contract between craigslist and the people using its service. Postings that violate craigslist's terms of use are often blocked before they reach the craigslist website using computerized filters, or removed by members of the craigslist community using a "flagging" tool. The flagging tool permits any person viewing a questionable advertisement to flag the advertisement as objectionable, with the advertisement being automatically removed from the site after receiving a specified number of flags. The number of flags required to remove an individual posting varies from category to category, from city to city, and from day to day, depending on conditions. We also manually remove advertisements and block accounts of people who come to our attention as violating the terms of use. Currently, our terms of use prohibits the sale of items that are prohibited by or heavily regulated by applicable laws. A link from the terms of use lists a partial list of specific items prohibited on craigslist, including "weapons and related items," and "stolen property." There are also links to various other websites that provide information regarding what property may be legally sold, including sites maintained by the Bureau of Alcohol, Tobacco, Firearms and Explosives. Our terms of use and related online educational materials are constantly being reviewed and are periodically modified, as our community, including members of law enforcement and regulatory agencies, call our attention to the need to modify the Terms of use to address specific issues, or to improve the related educational materials that craigslist provides.

Commitment to Enforcing Our Terms of Use

The vast majority of people who use craigslist are well intentioned, law abiding citizens who use craigslist to find items that they need in their everyday lives, including jobs, employees, housing, tenants, roommates, automobiles, furniture, computer equipment, household goods, local services, event listings, and community information. People also use craigslist to participate in

free forums on a wide array of topics. Many users of our free "personals" section have also found their spouses on craigslist. On rare occasions, however, craigslist is misused. Any criminals misusing craigslist will soon learn, if they have not learned already, that craigslist provides no safe haven for their activities. People using craigslist leave behind a variety of electronic records, sometimes including telephone records, that can be traced when craigslist is misused. Craigslist has a long and successful history of cooperation with law enforcement agencies to track down criminals. However, we do not rely solely on law enforcement to enforce our terms of use. Ensuring that users of craigslist abide by the law and use our website only for legal purposes is one of our very highest priorities. Although we are a small company, a majority of our employees are involved in projects designed to enforce our terms of use, and these activities constitute a large portion of their daily duties. I personally spend a large percentage of my working time engaged in these efforts, as does our founder, Craig Newmark. When matters come to our attention that require the assistance of law enforcement, we proactively call these matters to the attention of the appropriate authorities. Partly because we are a small company, we have developed a reputation for being exceptionally responsive to requests for assistance from law enforcement.

Comments on the GAO Report

On Monday April 7, the staff of this committee provided us with a draft of the GAO report to be released on April 10, and we thank the staff for this courtesy. We have not had much time to consider all of the aspects of this report as we would need to provide a full response, but, for the record, we would like to make the following correction:

- Although craigslist does not have a formal "Fraud Investigation Team," prevention of fraud and other misuse of craigslist is a top priority for a majority of our employees, across all departments, including Craig Newmark and me, and several of our employees have extensive experience in this area. The draft GAO report we received implied that only one person at craigslist was engaged in combating fraud, which is very misleading.

In addition, for the record we would like to add the following observations:

- Craigslist is intended to facilitate only local transactions, between buyers and sellers in who live in the same geographic area. Because we strongly discourage users from doing business with persons who do not reside in the same local area, we haven't historically felt that we needed to provide information regarding export laws.

- The business models of craigslist and eBay are fundamentally different, with eBay providing a single global marketplace, and craigslist providing hundreds of separate local marketplaces. Under the circumstances, we believe that craigslist does not deserve the equal billing it received with eBay throughout the report, implying that craigslist approaches eBay as a marketplace for the re-sale of sensitive defense related items sold using the internet. As a collection of 450 separate local classified ad venues, craigslist is not a very effective marketplace for people to use if they want to engage in global trafficking of specific items of military equipment.

Tangible Steps for the Future

For the reasons described previously, craigslist is not "user friendly" to those who would misuse the site for illegal purposes, and our company has zero tolerance of persons seeking to illegally sell military equipment. We thank the committee for calling this problem to our attention and are very interested in learning more, as we prepare to take whatever steps prove to be most effective in preventing such misuse on our website in the future. Possible steps that we could take that have occurred to us as we have begun to think more deeply about this issue include the following:

- We think that it would be helpful to update our terms of use and our prohibited items page to specifically list the resale of defense-related equipment that has not been disposed of in accordance with Department of Defense demilitarization policies. Craigslist users are generally willing to refrain from posting items for sale that they know are prohibited, and likewise are passionate about using the flagging tool to remove listings of items they know are prohibited.

- Our experience is that technical screens can be very effective in preventing advertisements that facilitate illegal activities. Once we have a better understanding of this class of prohibited items, we think that it will be fruitful to task our engineers with implementing technical screens targeting advertisements of specific kinds of equipment designated as not eligible for resale.

We will consider other measures as well, including adding staff, in order to effectively address the problems at hand. We would welcome additional suggestions from all interested parties.

Concluding Statement

Craigslist believes that nature of its 450 distinct local marketplaces discourages the use of craigslist by people who are interested in acquiring military equipment for export outside of the United States. While craigslist currently can be used to find such equipment locally as the GAO report has demonstrated, we feel that we have identified measures that will dramatically curtail this trade, and we are motivated to do what it takes to address these issues. We would like to thank the subcommittee on National Security and Foreign Affairs for inviting us to participate in this hearing, and look forward to working together to help solve this important problem.

Mr. TIERNEY. Thank you very much.

We are going to start with some questions and answers here. Some of the Members have left to go vote, so as it gets closer to that we will probably take a brief break and go back and then ask you folks to rejoin us at the end of that. I apologize for that, but it is something beyond the control of this subcommittee.

Let me start with the last suggestion that was made by Mr. Buckmaster. Is the financial gain by not just eBay but any company that might be being used as a conduit by bad actors, is that perceived to be the driving force here, Mr. Kutz?

Mr. KUTZ. I can't discuss intent of people, but certainly it is a fact. I mean, if eBay sells something that is stolen from the Government, the taxpayers paid for it and eBay would make a small profit on that, and whoever sold it and got it for zero dollars or whatever.

One of our eBay sellers was buying them from soldiers for $20 and selling them for $55, so they were making $35. There is profit for the seller.

Mr. TIERNEY. That was a seller, but not an Internet company.

Mr. KUTZ. As a seller, but eBay would get some sort of commission on that, I would assume, and so would other sites. I am not pointing to them only, but others are doing for-profit.

And I agree with Craigslist, they are not making any money on those sales. I believe that is factually accurate.

Mr. TIERNEY. Mr. Beardall.

Mr. BEARDALL. I think so as well, sir, that for the Internet sales, that is the main motivator. Now, the cases that we get involved in in our undercover operations, then it usually involved nationalistic interests as well as big dealers making big bucks, which are the arms dealers who we ferret out by a number of means, including undercover operations setting up storefronts for them to come in and try to buy items from us.

Mr. TIERNEY. Mr. Beardall, it seems to me from your testimony that you are, in a sense, trying to do what Mr. Kutz' group did as an enforcement mechanism. You are trying to do the same kind of things from time to time. Is that the best way for us to approach it? Is that the best we can do, is after the horse is out of the barn, sort of go around and collect it? I am sure we have a lot of questions for our next panel as to what are policies going on here and how do these things hit the place in the first instance.

Mr. BEARDALL. Sure, preventive measures would be much preferable to us devoting the amount of time that we do, and with the small force I have, that is why we have to prioritize, as well, and cannot spend a lot of time on the Internet, but are going after more serious things that Iranians and the Chinese want.

Mr. TIERNEY. From the standpoint of Mr. Kutz, Mr. Beardall, and your respective agencies, is there anything more that private or not-for-profit Web sites that these two witnesses represent, but are certainly not exclusive just those, is there anything they can do?

Mr. BEARDALL. Sir, I think one of the great examples of what we can do is what was referred to by Mr. Cohen, regarding our cooperation. As you noticed, he mentioned the DCIS continues to

work with eBay to try to find ways that we can stop this stuff and, if we discover it, then go after it.

Now, in a lot of cases, because of our small number of agents, we also get the assistance of Army CID, of OSI—Office of Special Investigations—for the Air Force, and Naval Criminal Investigative Service. Unfortunately, those folks are also tied up with major missions in Southwest Asia, which reduces the amount of agents they can provide to this effort.

Mr. TIERNEY. So assuming we have all these different people doing investigations, trying to get people that have sort of breached the gap here and gotten on some site at some point in time, and that is not drying up what is going on, because apparently the incentive is too high, either nationalism or some other driving forces like the money, itself, for these people, we are going to continue to find them trying to do this. You are going to continue to clean up, unless we take care of those policies that allow for these types of things to get out into the marketplace to begin with. Is that a fair assessment?

Mr. BEARDALL. Correct. And one of the other things is sometimes the sellers don't even know what they have. This stuff is picked up at garage sales and other things and it comes on the Internet and it raises our antenna up, but it is just an inadvertent sale. That is the trouble with prosecutions, as well. You understand that most of these cases—you have a couple of cases of MREs, night vision goggles here and there—are not going to get prosecuted because, again, the amount of work that the U.S. Attorney's Office has to prosecute this. That is why at times I think we have been lucky to have some UCMJ results.

I smiled today when Mr. Kutz talked about the soldier who got 30 months. He's lucky he wasn't a marine, because one marine staff sergeant was sentenced to 10 years and a dishonorable discharge by the marines for the theft and sale of body armor. I think that made a point in Camp Pendelton and other areas of the Marine Corps.

Mr. TIERNEY. How extensive is this situation? How many Web sites might we be talking about?

Mr. BEARDALL. Well, there are two that are the main Web sites, High Bidder and Inventory Locator Service, which actually is a compendium of a number of links where you can try to get stuff from legitimate dealers in military equipment and all the rest, but, again, if somebody is looking for that odd item—and, again, the trouble with Defense contractors, we have tons of them doing a small part here, a big part there, and, again, we are looking for bulk and stuff that will harm our soldiers, sailors, airmen, and marines, and have them lose the advantage on the battlefield.

Mr. TIERNEY. How real is the prospect that somebody would move some of these very sensitive materials internationally? Are there a lot of barriers for people to break to get that done successfully, or is it something that we know happens more frequently than we like, and on a large scale?

Mr. BEARDALL. I am really not the right person. Perhaps the FBI has a better handle on that. But I do at times feel like the Dutch boy in trying to stop the flow of the dam. And it is all kinds of stuff. I just got a report this week about one of our investigations

resulting in an 11-year sentence and a 9-year sentence from two Americans who were sending weapons to Canada, and it was a large shipment of sensitive items, and Canada is recognized as one of the trans-shipment areas for Iraq. Again, we were pleased to be able to get these two guys off the street.

It takes a lot of work. The problem with it is that undercover operations are very agent intensive. If I have an agent or two working an undercover operation, they are no use to me in any of the other stuff we do with fraud and all the rest, and so we have a small force. You have to really pick and choose and try to get your biggest bang for the buck.

Mr. TIERNEY. Mr. Cohen, something that Mr. Kutz said grabbed my attention, and I want to ask you to respond to it. We talk about enforcement maybe not being adequate, there are no resources that it ties up in the cost/benefit of that, but there was a comment made that eBay is able to keep used cosmetic sales or ban used cosmetics from being sold on eBay. If that is the case and you are successful in doing that, where is the breakdown in our apparent inability to keep sensitive military equipment off of eBay?

Mr. COHEN. There are a lot of categories like the used cosmetic category in which we have a prohibition on, and we rely on the community to help us to enforce those tools. Where we think we should be spending our time and effort, obviously, is on sensitive military equipment. That is where we devote our energy, so that a listing of different standards of what is allowed and what is not allowed does not reflect where we are going to place our efforts against that.

Mr. TIERNEY. So for all you know the ban on used cosmetics may not be any more successful than your attempts to keep off the sensitive military equipment?

Mr. COHEN. No. I would say just that it is more in the line of where is the greater risk to the public.

Mr. KUTZ. And that is based on an FDA regulation that they do that.

Mr. TIERNEY. I guess what I am trying to say is if you are successful at keeping the used cosmetics off, then what are we doing with respect to used cosmetics that we are not doing and should be doing with respect to sensitive equipment?

Mr. COHEN. I do think that it is fair to say that, because the regulation is in place—and I can't quote specifically as to what our effectiveness is on the used cosmetic categories, so I can't necessarily say that we have a large problem or a small problem in that area, so I don't want to suggest that we have absolutely eliminated the sale of all used cosmetics, but I wanted to suggest more so that it is where we are going to place our resources to where the greater risk is to the public, and obviously it is going to be in this other area.

We also prohibit other items that are prohibited that may be found in lots of different locations, and yet we don't invest energy to try to eliminate that category.

Mr. TIERNEY. Right. So are we fair in saying that there is at least as strong a regulation prohibiting the sale of sensitive military equipment as some of these other products?

Mr. COHEN. Yes.

Mr. TIERNEY. All right. We are all comfortable with that.

I will stop for a second and yield to Mr. Shays.

Mr. SHAYS. Thank you, Mr. Chairman, again for holding this hearing.

In 2002 the subcommittee basically was made aware of top-grade chemical suits that were being sold to the public when we had the military waiting in line, and then in 2003 we saw biological warfare laboratory that was basically sold for pennies on the dollar. In 2005 we learned DOD was transferring, donating, and selling excess property in near or good condition, while at the same time purchasing similar items for a soldier. In 2006 we learned from the GAO that sensitive military equipment was being sold or given to the public.

I want to first know, are those problems still occurring, or do we not know because we haven't looked at that again? Has there been improvement in those areas?

Mr. KUTZ. There is definitely improvement, and only a couple of these cases could potentially have come from Government liquidation, which is the one that sells the excess property for DOD. Both of the individuals we bought the F–14 parts from also were buyers from Government liquidation, as was one of the individuals that said they bought their kevlar helmets from Government liquidation. So there is potentially two or three of the buys we made that may have come from Government liquidation; otherwise, these are other sources feeding the secondary market for military property.

Mr. SHAYS. But, bottom line, this committee has continued to look at this. The GAO has determined that you all have determined that things have gotten noticeably better. So now what we are looking at is something different. We are looking at theft.

My first question is: should we have been aware of the theft without seeing it being sold on eBay, but just seeing that our inventory didn't match, that there was tampering with the record or there was an imbalance, there were things not there that should have been? Should that have been what told us that there was some stolen items taken, whether they were sold or just kept for that person's use?

Mr. KUTZ. Yes, most of the items that we identified were, in fact, stolen, we believe. Other ones we are not sure of.

Mr. SHAYS. You are not hearing my question. The issue is: how did we learn they were stolen? If you have a system that works properly, if Sam's Club can tell us in 15 minutes where everything is stored and what sold in the last half hour or earlier, why do we still not have the ability? Do we have leakage, stolen items that we would never know about because we don't have systems in place? Or do we now start to have systems in place to know when we have this problem?

In other words, we found out this was stolen, I think, Mr. Beardall, because you noticed it on eBay, correct?

Mr. BEARDALL. EBay and other things, as well. Our undercover operations are the most successful in finding people who are stealing and selling or people who are wanting to buy. But eBay items is another place that we keep looking.

Again, a lot of the sellers on eBay are, frankly, one or two items.

Mr. SHAYS. I understand that.

Mr. BEARDALL. We are concerned more with the bulk items, and I have not seen a lot of that, and perhaps——

Mr. SHAYS. Do we have a serious theft problem, or do we not even have the ability to know we have a serious theft problem?

Mr. BEARDALL. I might say the latter might be more accurate.

Mr. SHAYS. OK.

Mr. BEARDALL. And I would defer to the witnesses on the next panel who manage the distribution centers and know more.

Mr. SHAYS. Really, what I am asking you, Mr. Kutz, is, if we did the same operations that you did in 2002, 2003, and so on, would we encounter the same abuses that I just read off, or would it be likely that DOD is in a better position to prevent that?

Mr. KUTZ. I believe there are fundamental DOD property management issues that resulted in the stolen property, yes. But I don't think they are excess property; I think they are the rest of the supply chain. You are talking about items distributed to the Army from DLA that the Army loses control of, either through soldiers or a warehouse or something like that. So it is a little different problem. I think you said at the beginning, it is stolen property, but the source of it is not the stuff that is going through the excess property system. Now you are talking about supply warehouses, like the Korea case, where soldiers are stealing body armor. This didn't come from a soldier, this came from a contractor, and the contractor sold it to us.

Mr. SHAYS. When I see that, what I wrote down, you know, night vision goggles, F–14 parts, body armor, infrared tape are being stolen, you know, and then it is either a private citizen's illegal possession, maybe something that was stolen or not stolen, but equipment that has been stolen by individuals or unauthorized vendors, to me that is what we are looking at today. To me that is basically treason.

I mean, the fact that someone can get a uniform and basically get in our base using that uniform—now, admittedly, that may have been items that were stolen in Iraq, but, in particular, the night vision goggles, we go out at night in Iraq every night with Special Forces. We go out at night instead of the daytime because we have that advantage. If we lose that advantage, we are going to have many of our soldiers killed and marines killed. That is the thing that I find most outrageous.

I am going to end my question by saying progress has been made. It appears that stolen items is an issue. It appears that it is small items so far. You have prosecuted some when you should. We are always going to have a stolen item issue, it seems to me. We want to catch them quick and go after them.

Thank you.

Mr. TIERNEY. Thank you.

Mr. Welch.

Mr. WELCH. Thank you, Mr. Chairman.

Mr. Kutz and Mr. Beardall, are there any things that you would recommend that could be done in what I understand is a positive relationship with eBay and Craigslist that would improve it so that we could diminish the illicit sale?

Mr. BEARDALL. Yes, sir. I think one of the things that is obvious is that the DCIS—Defense Criminal Investigative Service—and

eBay have a long-term relationship after our original operation was completed, and we continue to try to refine ways to identify those items on eBay. They have been very cooperative and helpful, and we are trying to work through them because they, of course, are the biggest online seller where these things are showing up.

Mr. WELCH. But then there are other locations like, I guess, Craigslist and all kinds of entities out there that can sell on the Internet. Are there any things that you would recommend to us legislatively or rulemaking that might provide better protection?

Mr. BEARDALL. I think the emphasis is obviously on keeping the stuff from getting stolen. Again, in comment to Mr. Shays' questions, if there are going to be large, bulk thefts of items from the Department of Defense, we are not going to see those on eBay. Those are going to be sold another way, which is what DCIS is trying to really home in on. I think that is the area where you try to stop it later on. We are just cleaning up the mess.

Mr. WELCH. Sure.

Mr. Cohen, I understand eBay gets millions of for-sale opportunities a day from participants, so obviously it is a huge management issue. I understand you have testified about your fraud investigation teams. Do you have any recommendations on what the Government and Department of Defense could do that would facilitate your efforts to keep improper military and other things offline?

Mr. COHEN. I think the most important thing was what Jim alluded to with regard to clear rules. One of the dilemmas we face is, because we are visible and the Internet is more visible, there sometimes is the tendency to try to impose restrictions on the Internet that would not apply to an off-line world. Our goal is to say that if we want to prohibit the sale of night vision goggles, then it should be a technology neutral decision to make it illegal across the board, and especially in the area of export control.

For us, the most difficult issue of all is that you can buy an item that is limited for export control at a store and then walk out the store and ship it overseas for individuals to do that, and yet the complaint has been raised that we aren't able to do that because individuals are able to look at our items from around the world.

So if there is a decision made by the Congress to say that these are export controls, then we probably should try to have that consistent across all the different platforms, rather than just picking one platform. That would be our request from the Congress.

Mr. WELCH. OK. How about just in the day-to-day interaction that you have with the Government about trying to monitor and sty on top of what should not be sold?

Mr. COHEN. We receive remarkable cooperation from law enforcement and a desire for people to help solve the problems, and that is why we spend so much time and effort on it. I mean, it is important. I think it is important for there to be always an open level of cooperation, and from our perspective one of the things that we and others in all industry should do is, wherever possible, not make our law enforcement officials jump through hoops, like subpoenas, on areas of important national security. That is why we have always had a much more open and active policy to cooperate, work with DCIS and others, before making them have to jump through the hoops.

I will mention one other thing. We many times get requests from DCIS and others to leave items up for sale that may be sensitive military equipment, and that may then end up in the press, and that is at a direct request from the investigators to say leave that up so we can help track down both who are the buyers or potential buyers, and who the seller is. That is why you may see stories in which items would be inappropriate but have been left up.

Mr. WELCH. OK. Thank you.

I yield back.

Mr. TIERNEY. Thank you. While Mr. Hodes is getting situated, I just want to ask one question. Mr. Kutz and Mr. Buckmaster, I noticed that some items were body armor vests, and were purchased from eBay and Craigslist sellers. Am I right in assuming that Craigslist is like a newspaper, but online, and it could have also been that somebody went to a newspaper and saw a listing for this and made the same kind of transaction? Is that right?

Mr. KUTZ. That is correct, yes.

Mr. TIERNEY. And Mr. Buckmaster, that fits?

Mr. BUCKMASTER. Yes, I think that is correct, and I would just quickly say that I think the problem from our perspective is that our otherwise well-intentioned users are somewhat ignorant about what they are allowed to sell and what they are not. From our perspective, it would simplify things greatly if a law were passed banning the sale of any U.S. military issued item, say, that is less than 50 years old, and our users would understand that.

If we, absent such a law, try to make such a blanket rule on our site, our users would rightfully chaff. Why are we not allowed to do this when it is legal?

If we are going to end up with a 50-page long description of items that can and cannot be sold, our users, if we are lucky, will read half a page of items.

Mr. TIERNEY. Lucky if they read half a page is right. Well, what about that, Mr. Kutz and Mr. Beardall? Would you recommend legislation that just banned the sale of military equipment beyond a certain vintage date?

Mr. BEARDALL. That could potentially work. Yes, sir.

Mr. KUTZ. Certain items, possibly, yes.

Mr. TIERNEY. Why just certain items?

Mr. KUTZ. Well, it depends. Meals ready to eat, all of these are potentially stolen. Stolen ones should not be sold, certainly, but there is a whole bunch of other types of meals ready to eat out there. But certainly things like the night vision goggles, these are the ones that are used by hundreds of thousands of troops today. That doesn't seem like something that——

Mr. TIERNEY. It is sort of amazing to me that we haven't had a law to ban the sale of that, or the units and all that. It certainly would make things easier on this end, and it would make the prosecution easier on your end.

Mr. KUTZ. Yes, for certain.

Mr. BEARDALL. But, again, you have to react to the most sensitive and the most controlled and, for example, night vision goggles in versions one and two are now sold commercially. Three, four, and five are still controlled.

Mr. TIERNEY. I mean, it would let you prioritize what you need to do, but, on the other hand, it would help these gentlemen out in terms of just saying to all of their users it is just not allowed.

Mr. BEARDALL. Roger.

Mr. TIERNEY. Now you know that if they put it on there they are at risk, or whatever, and you go after it, it simplifies it a little bit on that basis.

Mr. BEARDALL. And there are some other little things that we can talk to your staff about that we would like to discuss. One of the things if I don't mention my agents will really get mad, and that is demilitarized items. If somebody is in possession of an item that has not been demilitarized, agents do not have the authority to seize that item if we can't tie another offense to it, as in it was stolen.

Mr. TIERNEY. So possession of a demilitarized item is not yet an offense?

Mr. BEARDALL. If it was improperly demilitarized and somebody has it, we usually have to say, couldn't we have it back? We can't seize it because we don't have that authority.

Mr. TIERNEY. I do think we need to hear those kinds of recommendations. I think that was well put, Mr. Buckmaster, and that is something for us seriously to consider yours, as well, and if you have others I am not averse to hearing them publicly so that people know that you have some ideas here and things we do.

Mr. BEARDALL. Yes, sir.

Mr. TIERNEY. So you think of those while we go to Mr. Hodes, and then before we close out I would like to hear what other things you think we might do legislatively.

Mr. BEARDALL. That is a big one, because when we try to take it they also say, well, are you going to reimburse me for it, and we can't do that, either.

Mr. TIERNEY. Exactly. Thank you.

Mr. Hodes, you are recognized for 5 minutes.

Mr. HODES. Thank you, Mr. Tierney.

I just want to followup on the discussion you have just been having so I am clear. Mr. Beardall, you amplified your written testimony, in which you said, "One limitation to our efforts is that DCIS agents have no statutory authority to seize items that were legally sold but were not appropriately demilitarized."

Mr. BEARDALL. Yes, sir.

Mr. HODES. How do you think, exactly, we need to expand legislation to address that concern?

Mr. BEARDALL. Right. Particularly authorize us to seize items that were not properly demilitarized and that are in the possession of the public when they should not be.

And we had that issue a lot in our Operation High Bidder, where we were going after the vests, and unfortunately a lot of times it was moms and pops who were distressed because they heard from their soldier in Iraq that they weren't getting the best vests or didn't have enough vests to distribute, and there was that initial surge and concern that raised the public concern, and we went out and, of course, at times there were people who had items that were military items and we couldn't seize them from them, we had to give them back. That was a little tough.

Mr. HODES. I note that eBay lists numbers of items that it says are prohibited or restricted from being sold online because of Federal or State regs. The list includes prescription medications, pesticides, firearms, ammunition, lock-picking devices. And eBay also says that many restrictions may involve the sale of dangerous or sensitive items not necessarily prohibited by law. So both seem to list prohibited or restricted items and provide links to State and Federal agencies Web sites.

To Mr. Cohen and Mr. Buckmaster, what are some examples of dangerous or sensitive items prohibited on eBay and Craigslist that are not specifically restricted by Federal or State regulation?

Mr. COHEN. I can give you one example, the meals ready to eat. We prohibit the sale of any of the MREs that have the internal heating device in it, which, because of safety reasons, we decided to prohibit those from being transferred and sold on our site, even though it is not illegal to do that. So it is a safety issue in which we made a decision that we would prohibit those from being sold.

Mr. HODES. But there is no current legislation prohibiting it; that was your own decision?

Mr. COHEN. That was our own decision. That is correct.

Mr. HODES. And what factors do eBay and Craigslist use to decide to prohibit the sale of items that are not restricted by law, other than safety? Are there other factors that you have taken it upon yourself to say we won't sell because we just don't think it is a good idea?

Mr. COHEN. Certainly. There are lots of different areas in which, for taste reasons, for community acceptance, I can think of many different areas in which it would make sense for us to work, as any other industry does with any other community of interest. There are certain areas where you are going to say this is something that we would like to be available, and this is something we wouldn't like to be available.

Mr. KUTZ. Congressman, could I use an example of that is particularly relevant here?

Mr. HODES. Sure.

Mr. KUTZ. They did prohibit the sales of police officer uniforms, I guess working with local law enforcement, etc. But these Army combat uniforms are not specifically prohibited, so hopefully something like today's hearing can bring DOD together with eBay to consider do we want to have Army combat uniforms that are used by our soldiers today, especially with infrared tabs on them, available for sale on eBay? That would be an example of something that isn't illegal at this point, I don't believe, but that would hopefully be something eBay and DOD could work on together to improve after today.

Mr. HODES. I guess for the folks from eBay and Craigslist, what I am getting at is not generally community taste factors, but more specifically dealing with the military issues that we are dealing with today. What factors are you currently using to decide whether or not to allow the sales of arguably military equipment. It may not be illegal, but what factors are you using there? And is this a protocol or policy that your companies have written out? Is it a written policy?

Mr. BUCKMASTER. We do have written policies. Postings that our staff remove are mostly illegal postings or sale of illegal items, although we do have a blanket ban on the sale of all weapons, whether they are legal or not, and a ban on the sale of pet animals.

Our users, on the other hand, are empowered to remove any ad for any reason.

Mr. HODES. I know my time is up, but let me just ask both eBay and Craigslist if you would be willing to provide this committee with a copy of your written policies as they may relate to the subjects of today's hearing, which will help us understand how you are currently self-limiting, if you will, the legal but items of concern that are at issue here today.

Mr. COHEN. Yes, we will be absolutely responding in writing, Mr. Chairman.

Mr. HODES. That would be very helpful.

Mr. BUCKMASTER. We will do so, as well.

Mr. HODES. Thank you, Mr. Chairman.

Mr. TIERNEY. Thank you.

I guess part of the issue is you probably feel constrained about not selling anything that hasn't been made illegal to sell. Other than self-constraint, otherwise kind of what maybe controls is it is not illegal, where you jump in is not pulling people back. My question I guess is what is the driving, overwhelming need for people to be able to purchase this type of thing unless they are up to no good. That is part of the problem. So I think the idea of us defining what should and should not be made available for public sale and consumption is probably a large part of this, and I am just sort of stunned that nobody stumbled across that before. We will talk to the next panel about that.

I want to thank all of you that have shown up here this morning. Mr. Buckmaster, I know you came all the way from California, and I greatly appreciate that. I know that both eBay and Craigslist stood the list of looking like they were somehow complicit or involved in this, or whatever, as opposed to what really is the fact here, that they have tried to be cooperative and they have tried very hard on their own, as well as in cooperation with the Government agencies, to work with us on this, and I thank both of you for that.

There are many, many other companies out there on the Internet that are part of this discussion.

Mr. Beardall, thank you for the good work that you and your agency do every day. It is hard to chase it down on the other end after it is out of the box, and we realize that.

Mr. Kutz, thank you and your organization and staff for providing us the information that we needed to be able to have this hearing and try to root out some solutions. We always appreciate the good investigations that you do.

I am going to let this panel go, rather than retain you during the vote. We are going to suspend until after the next votes, and then ask the second panel to come back at that time. I apologize for any inconvenience that causes.

Thank you once again.

[Recess.]

Mr. TIERNEY. The hearing will reconvene.

I want to thank our witnesses for waiting. It was a little bit longer than we anticipated. There was a new Member being sworn in, as you may know, to fill Mr. Lantos' seat, who used to be a member of this subcommittee, in fact.

The subcommittee will now receive testimony from our second panel of witnesses. Before us we have Mr. Alan Estevez, who is the Principal Assistant Deputy Under Secretary of Defense for Logistics and Materiel Readiness. From 2002 to 2006 Mr. Estevez served as Assistant Deputy Under Secretary of Defense for Supply Chain Integrations.

And we have Ms. Sarah Finnecum, Director of the Supply and Maintenance Directorate within the U.S. Army. Ms. Finnecum was an Army civilian for over 25 years of Federal service.

I also want to just note for the record that we had asked Mr. Estevez and Ms. Finnecum to testify and appear on the first panel with the other witnesses, and we thought that if everybody who had a stake in the process was on the same panel, that this would be the best way to comprehensively explore all the links of the chain from these materials being in the Defense Department's control and ending up for sale on the Internet. In the spirit of constructive oversight, we thought having everybody on the same panel would facilitate a free exchange of ideas and communications between all the actors and the stakeholders on how best to work together to clamp down on theft and sale of sensitive military items.

However, the Defense Department insisted on appearing separately from our private sector witnesses, and therefore you had to wait during that period of time and we had to break up the discussion that we were on.

The reasoning apparently given doesn't appear clear to me, but it was not clear to anybody, I don't think, especially as the focus of the hearing is how we can all do our part to fix this situation going forward.

You can rest assured, I don't think we will have that problem again, because if we have to use a subpoena next time to make sure that we bring them in, we will do it, if we can't get the cooperation of the Department of Defense to come in and work with Congress on these issues without looking for some special dispensation. I don't know what the concern was, whether people thought that they were going to be held accountable and didn't want to be held accountable or what the problem was, but I have now talked to the chairman and the ranking member and we won't have that issue again. Next time we ask somebody to come in and cooperate with us, I expect that they will come in and cooperate with us.

But we got notice too late that kind of pettiness was going to be going on, and so we didn't have a chance to issue a subpoena or whatever. And so we have a second panel and you are on it and I hope we now can go forward and try to at least look at this part of the picture.

Given the nature of the ubiquitous marketplace here, we want to find out what is the best line of defense for keeping track of this materiel in the first place. Once body armor or night vision goggles or F–14 parts leave our control, as you heard from the first panel, we seem to have already lost a good part of the battle.

So we are not going to waste any more time on ceremony or playing games. We have a panel going in. It is the policy of this subcommittee to swear you in before you testify. I ask you to please stand and raise your right hands.

If there are any other persons who are going to testify or assist in your testimony, I would ask that they stand to be sworn, as well.

[Witnesses sworn.]

Mr. TIERNEY. The record will please reflect that both witnesses answered in the affirmative.

I understand, Ms. Finnecum, that you did provide testimony. I would like to thank you for that. Mr. Estevez, you did not, so we would ask you to give a brief oral statement to fill the subcommittee in on policies and procedures in place across the Department of Defense to keep a tight hold on sensitive and expensive military technology and equipment. Please keep your oral statements as close to 5 minutes as you can, and then we will allow for some questions and answers.

Mr. Estevez, you are recognized.

STATEMENTS OF ALAN F. ESTEVEZ, PRINCIPAL ASSISTANT DEPUTY UNDER SECRETARY OF DEFENSE, LOGISTICS AND MATERIEL READINESS, U.S. DEPARTMENT OF DEFENSE; AND SARAH H. FINNECUM, DIRECTOR, SUPPLY AND MAINTENANCE DIRECTORATE, U.S. ARMY, G–4, LOGISTICS

STATEMENT OF ALAN F. ESTEVEZ

Mr. ESTEVEZ. Thank you, Chairman Tierney, and thank you for the opportunity to appear before you to discuss the issue of Internet sales of sensitive Defense-related items.

As you note, I am Alan Estevez, Principal Assistant Deputy Under Secretary of Defense for Logistics and Materiel Readiness. In my position I am responsible for developing over-arching logistics policy for the Department of Defense, which includes policies related to how our Department ensures our soldiers, sailors, airmen, and marines are supplied with materiel needed to fulfill their missions.

Our focus is to ensure that policies and procedures are in place to effectively provide that materiel, including food, fuel, munitions, protective equipment, and repair parts to our globally deployed forces when and where they need it, as cost effectively as possible to meet mission requirements.

Before focusing on the specific issues of this hearing, I believe it would be useful to put those issues within the context of the broader DOD logistics enterprise, a $178 billion operation in fiscal year 2007, including supplemental funding.

We feed and clothe over 2 million fighting men and women and support weapons systems engaged in air, land, sea, space, and cyberspace programs around the world daily.

Today more than 2.4 million American men and women are in uniform, including active, reserve, and National Guard components.

Over the last 5 years, approximately 1.7 million American military forces have deployed to the U.S. Central Command area of operations.

In support of our global operations, the DOD manages more than 4.4 million types of items, we process over 82,000 requisitions for that materiel daily. DOD issued 31.6 million cases of meals ready to eat [MREs], over the last 5 years, both in support of our forces and for humanitarian assistance, to include providing MREs to other Federal agencies and to international partners in support of Hurricanes Katrina and Rita, for the Indian Ocean tsunami, and Pakistani earthquake relief.

Over that same period, over 1.6 million small arms protective inserts and 846,000 enhanced small arms protective inserts were issued in support of current military operations.

With the assistance from this Congress, DOD maintains a world class military logistics system.

That said, the Department is always concerned about ensuring the security of our forces. In past hearings before this committee, the focus has been on our reutilization and disposal process. The Department has made significant strides over the past few years based on our own internal transformation, with some guidance and support from the U.S. Government Accountability Office and this committee to significantly tighten procedures associated with those operations.

As Congressman Shays noted, in a July 6, 2007, letter to the committee GAO noted DOD's significant progress in this area.

Even with that progress, we continue to reassess our policies and tighten our procedures related to realization and disposal.

The focus of the GAO investigation that prompted this hearing is not to be the Department's internal materiel disposition processes, but rather on the criminal activity of a few members or former members of our armed forces, as well as the sale of Defense-related materiel from commercial sources.

The Department obviously deplores criminal activity, especially when committed by members or former members of the armed forces, and supports law enforcement efforts to prosecute such malfeasance.

With regards to sales of materiel over Internet sites, I want to emphasize that the DOD does not set nor enforce export control policy. In addition, the Department does not manage commercial entities nor determine what they are allowed to legally sell domestically or internationally when the associated technology is not owned by the Government, nor can we prevent legal sales of that materiel.

Responsibility for export control of military unique items is assigned to the Department of State, for dual use items to the Department of Congress [sic]. Enforcement resides with the Departments of Homeland Security and Justice. DOD complies with the controls for that materiel within our passenger after the controls are set by those agencies.

With regard to DOD's internal inventory management practices, my office is responsible for establishing the policies for an integrated DOD supply chain process that fully supports military operational requirements. In this capacity, DOD prescribes policies for the management and control of the materiel from its initial entry into the Department of Defense to disposal, when the materiel becomes excess to the needs of our war fighters and military services.

My office establishes Department-level policies, while the military components are charged with establishing their own processes and procedures to execute those policies within the guidelines provided.

In closing, Mr. Chairman, thank you for the opportunity to testify before the committee. As the DOD continues to provide support to our military forces at the scale referenced above, the Department also continues to monitor and adjust our policies, as required, to continue to better support our American men and women in harm's way and to do justice to the American taxpayer.

I would be happy to answer any questions you or the committee may have.

Mr. TIERNEY. Thank you, Mr. Estevez.

Ms. Finnecum, you are recognized.

STATEMENT OF SARAH H. FINNECUM

Ms. FINNECUM. Chairman Tierney, on behalf of the Army we thank you for the opportunity to appear before you today to discuss the sale of sensitive, in-demand Army equipment and supplies on the Internet, specifically the two Web sites eBay and Craigslist.

Mr. Chairman, I have submitted a written statement that I ask be made part of the official record.

Mr. TIERNEY. It is done, without objection.

Ms. FINNECUM. I want to assure you that the Army has both law and policy that prohibits the sale of Government property by private individuals. We also have processes and systems to account for our materiel and prevent such abuses. Having said that, there is a fine balance between providing our fighting forces the equipment they need as expeditiously as possible, while also maintaining accountability of that equipment.

In the early stage of OIF and OEF, we recognized the obstacles that field commanders faced in conducting combat operations while carrying out the property accountability responsibilities. Therefore, in May 2003 the Army developed a limited wartime accountability policy to relieve commanders of the administrative burden that impeded the rapid re-supply and refit of our forces; however, we found our aggressive efforts to ensure deploying and deployed units had the best equipment possible also created challenges to account and track equipment.

In November 2005 we rescinded the limited wartime accountability policy. We followed with additional guidance on accountability requirements to include safekeeping and disposition of Government property entrusted to units and individuals.

The Army's bottom line is that soldiers and civilians are responsible for maintaining and properly accounting for materiel in their possession. The Uniform Code of Military Justice authorizes punitive action to be taken against soldiers for the following: Article 92, failure to obey an order or regulation; Article 108, military property of the United States lost, damaged, destruction, or wrongful disposition of property; and Article 134, stolen property, knowingly receiving, buying, or concealing.

Additionally, the Army has two specific regulations that address accounting for Army property. The principal regulation is AR735–5, policies and procedures for property accountability. This regula-

tion establishes the basic policies and procedures to account for Army property. It also prescribes the accounting procedures to be used when Army property is discovered lost, damaged, or destroyed through causes other than fair wear and tear.

AR735–5 clearly states that no Government property will be sold, given as a gift, loaned, exchanged, or otherwise disposed of unless specifically authorized by law.

The second regulation is AR710–2, supply policy below the national level. It provides policy for the accountability and responsibility of property issued to a unit or an individual. The key provision of this regulation requires employees of the Army, be that a civilian or a soldier, to turn in to the supply system all Government property that has been found, and to place that property under the control of an accountable property officer.

I would also like to quickly provide you a summary of some of the other initiatives we have put in place to prevent improper use of our Government materiel.

We implemented Operation Total Recall in September 2006 to improve accountability of Army assets. All Army units were directed to conduct focused inventories, training, and emphasize the command supply discipline program. To date, the Army has returned to property book accountable records over 20,000 items worth more than $135 million.

Two, revitalization of the command supply discipline program. This is a commander's program that standardizes supply discipline requirements across the Army. Each commander is required to provide the personal interest and direction necessary to establish and ensure the success of his or her unit is stewardship of resources and property.

We have also fielded a new Web-based system called the property book unit supply enhanced system. We did that in 2001 and completed fielding of it in 2007. This system significantly improves accountability at the local level—and by that I mean unit—and allows asset visibility of unit property across the Army.

We have also implemented the central issue facility integrative system management in 2006. That system captures organizational clothing and individual equipment issued to soldiers and civilians.

We are constantly putting articles in soldier magazines, on the Internet so that soldiers are aware of the proper procedures for accounting for equipment.

We have ongoing and constant review and analysis of property accountability.

Mr. Chairman, I will save any further comments on Army property accountability for the question and answer session. Thank you for your time today.

[The prepared statement of Ms. Finnecum follows:]

STATEMENT BY

MRS. SARAH H. FINNICUM
DIRECTOR OF SUPPLY
OFFICE OF DEPUTY CHIEF OF STAFF, G-4
UNITED STATES ARMY

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY AND FOREIGN AFFAIRS
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

SECOND SESSION, 110TH CONGRESS

ON

INVESTIGATION INTO THE SALE OF SENSITIVE, IN-DEMAND MILITARY EQUIPMENT AND SUPPLIES ON THE INTERNET

APRIL 10, 2008

NOT FOR PUBLICATION
UNTIL RELEASED BY THE
HOUSE COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM

Chairman Tierney, Ranking Member Shays and distinguished Members of the Committee: on behalf of the Army, thank you for the opportunity to appear before you today to discuss the sale of sensitive, in-demand Army equipment and supplies on the Internet. I welcome this opportunity to provide you forthright and honest assessments of Army property accountability and to further assure you that the Army is taking the measures necessary to maintain control of our equipment and supplies.

Today's testimony focuses on the sale of sensitive, in-demand Army equipment and supplies on the Internet, specifically two websites – eBay and Craigslist. The Army takes seriously its responsibility as stewards of the US taxpayers' dollars. We have both law and policy in place that prohibits the sale of Government property by private individuals. We also have processes and systems to track our material and prevent such abuses.

First, let me say that the Army recognizes that all the Services have had property accountability and visibility challenges. Before beginning a discussion on the Army's current property accountability issues, it is essential to highlight a fundamental contributing factor. There is a significant challenge in attempting to balance the rapid fielding of critical equipment and supplies to Theater with the necessary business processes to manage this flood of new assets. With Congress' assistance the Department of Defense was able to push essential materiel to troops in Operation Enduring Freedom and Operation Iraqi Freedom (OEF/OIF). In some cases, particularly early on in OIF and OEF, our ability to maintain adequate accountability of those assets lagged behind this new, rapid fielding methodology. This has been a learning process for all the Services and we continue to refine our processes.

In the early stages of OIF and OEF, we recognized the obstacles field commanders faced in conducting combat operations while carrying out their property accountability responsibilities. In May 2003, we developed a limited wartime accountability policy to relieve commanders of the administrative burden that impeded the rapid resupply and refit of our forces. However, we found that in our aggressive efforts to ensure deploying and deployed units had the best equipment possible, we created challenges for commanders

and the supply system in accounting for and tracking equipment. In November 2005, we rescinded the limited wartime accountability policy in order to meet the demands of the Global War on Terrorism, transformation, reset, training and modernization. We then published additional guidance on accountability responsibilities to include proper use, care, custody, safekeeping and disposition of Government property entrusted to units and individuals. This message also addressed the Command Supply Discipline Program, which I will talk about later, Financial Liability Investigations of Property Loss and accountability of locally purchased items.

Before explaining the more specific actions the Army has taken to maintain property accountability and visibility, the following highlights the statutory and regulatory guidance that govern military equipment in the hands of units or individuals. The Uniform Code of Military Justice (UCMJ) and Army Regulations (AR) provide for numerous punitive actions for misappropriation, theft and/or sale of military property. There are three articles in the UCMJ that specifically pertain to these criminal activities:

1. **Article 92. Failure to obey order or regulation**. This offense carries a maximum penalty of Dishonorable Discharge, forfeiture of pay and allowances, and up to 2 years confinement.

2. **Article 108. Military Property of the United States-loss, damage, destruction, or wrongful disposition**. This offense carries a maximum penalty of a Bad Conduct Discharge, forfeiture of pay and allowances, and up to 1 year confinement for property valued less than $100 or Dishonorable Discharge, forfeiture of pay and allowances, and up to 10 years confinement for property valued more than $100.

3. **Article 134. (Stolen property: knowingly receiving, buying or concealing)**. This offense carries a maximum penalty of a Bad Conduct Discharge, forfeiture of pay and allowances, and up to 6 months confinement for property valued less than $100 or Dishonorable Discharge, forfeiture of pay and allowances, and up to 3 years confinement for property valued more than $100.

In addition to the UCMJ, the Army has two specific regulations that address accounting for Army property. The overarching regulation for accountability of Army property is **AR 735-5, Policies and Procedures for Property Accountability**. This regulation lays down the basic policies and procedures in accounting for Army property. Specifically, it sets the requirement for formal property accounting within the Army, implements specific property accounting procedures, defines accountability and responsibility, identifies the categories of property and the accounting procedures to be used with each, identifies the basic procedures for operating a property account and provides the policy for offering rewards for the recovery of lost property.

AR 735-5 also prescribes the accounting procedures to be used when Army property is discovered lost, damaged, or destroyed through causes other than fair wear and tear. The policies and procedures contained in this regulation derive their authority from several US Codes. AR 735-5 clearly states that "No Government property will be sold, given as a gift, loaned, exchanged, or otherwise disposed of unless specifically authorized by law. Items replaced-in-kind and payments made... for lost, damaged, or destroyed Army property do not constitute a sale of Army property. Title to such property remains with the U.S. Government". In other words, even if an individual is found liable for lost, damaged or destroyed Government property, the Government retains ownership of the lost, damaged or destroyed property even if the individual has made full restitution for the equipment.

The regulation also specifies five levels of responsibility to prevent unauthorized sale of military equipment and supplies. The levels of responsibility are: Command responsibility, Supervisory responsibility, Direct responsibility, Custodial responsibility and Personal responsibility.

The second regulation is **AR 710-2, Supply Policy Below the National Level**, which applies in peace and war and provides specific policy for the accountability and assignment of responsibility for property issued to a unit. It also provides for the accountability, management of stocks and inventory controls of items stored at supply support activities (SSAs) for issue to a Soldier. Chapter 1-12 of AR 710-2 specifically states that all property acquired by the Army, regardless of source, whether paid for or not,

is accounted for as prescribed by these and other applicable Army regulations. The regulation also distinguishes between, and provides policy regarding, the different types of property. The key provisions of AR 710-2 pertaining to property accountability are:

1. Employees of the Army, both military and civilian, are required to turn in to the supply system all Government property that has been found.
2. Property that has been found but not otherwise accounted for is immediately placed under the control of an accountable property officer.
3. If there is no mission need for the item(s) they must be turned in immediately per instructions detailed in the regulation.

The Army has aggressively tackled the issue of property accountability across the Service and continues to make improvements to increase visibility and control of equipment and supply.

On 28 August 2006, the Army implemented an initiative called "Operation Total Recall" to establish 100% accountability of Army assets through policy revision and enforcement, focused inventories, training, and emphasis on the Command Supply Discipline Program (CSDP). The intent of Operation Total Recall is to assist commanders in their efforts to re-establish property accountability and ensure that they account for equipment using automated systems called Standard Army Management Information Systems (STAMIS). Our end-state is corporate-wide Army asset visibility. Operation Total Recall required units to conduct quality and focused inventories; initiate property record adjustments; update property books; and report the completion of all inventories and their results through command channels. To date, the Army has returned to accountable records over 20,000 items worth more than $135M.

The Army's Command Supply Discipline Program (CSDP) is a commander's program that standardizes supply discipline requirements across the Army, provides responsible personnel with a single listing of all existing supply discipline requirements and makes the Army more efficient regarding time spent monitoring subordinates' actions. Under the

CSDP, each commander is required to provide the personal interest and direction necessary to establish and ensure the success of his or her CSDP and appoint a CSDP coordinator to assist him/her in monitoring the program. The CSDP requires commanders and supervisory personnel to instill supply discipline in their operations; provide feedback through command and technical channels for improving supply policy and procedures; and follow-up to ensure that supply discipline is maintained. Local CSDP monitors and CSDP coordinators can provide supply discipline training, accept and forward supply policy and procedure deviation and change requests, and perform follow-ups. External evaluations to determine compliance with the CSDP are required for active duty units on a quarterly, semi-annual or annual basis, depending on the type of unit. Commanders may also direct an external evaluation at any time. Evaluations are recorded and results are provided to the organization evaluated and the next higher organization in the chain of command. Discrepancies are assigned a suspense date and repeat discrepancies are noted in the report. Units are required to maintain their last two evaluations on file.

Operation Total Recall also granted specific joint inventory supply policy deviation for United States Army Central Command (USARCENT). The deviation allows sub-hand receipts to be used in lieu of joint inventories for most equipment. This offers relief to commanders and their workload by allowing them to let junior leaders take control of property accountability, especially at remote Forward Operating Bases, and minimizes travel within the Theater of Operation during Relief in Place/Transfer of Authorities (RIP/TOAs).

Operation Total Recall contains six segments for actions: Organizational Clothing and Individual Equipment (OCIE) inventory; asset visibility issues resolutions; management of Controlled Cryptographic Items (CCI), Communication Security (COMSEC) and classified equipment; Installation property movement exceptions; Financial Liability Investigation of Property Loss (FLIPL) policy and procedure updates; and specific Command Supply Discipline Program (CSDP) procedures.

The Army directed wide dissemination of information on the establishment of Amnesty

Boxes at OCIE Central Issue Facilities (CIFs) in November 2007. Soldiers could turn in unrecorded or excess organizational clothing and individual equipment without fear of attribution or reprisal. The OCIE that was turned in was documented using Found On Installation procedures. Serviceable items excess to a specific CIF were identified to the Central Management Office (CMO) for redistribution to fill requirements. This program proved to be very successful.

Prior to 2001, the Army relied on an automated property accountability system that was of limited use in providing total asset visibility across the entire Army. In 2001, the Army began replacing the outdated property accountability system with a new, web-based system, the Property Book Unit Supply – Enhanced (PBUSE), that has provided greatly expanded capability for both property accountability and asset visibility. PBUSE is the first web-based property accountability system with features that significantly improve not just accountability at the local level, but allows asset visibility of unit property across the Army. Among the many benefits to the Army that have resulted from the development and fielding of PBUSE is the management of excess property and shortages. Unit commanders now have the capability to see excess property across multiple units and to redistribute the property when needed. We are also leveraging PBUSE to assist in the visibility and accountability of PM-owned equipment prior to fielding, battle loss turn-ins, physical losses, and RESET turn-ins. In early 2007, PEO-Soldier, working with the OCIE Central Management Office and HQDA, developed an automated PEO interface with PBUSE. Data is uploaded to PBUSE and the Central Issue Facility Integrated Support Module (CIF-ISM) which automatically captures all issues to a Soldier's Clothing Record that is maintained throughout the Soldier's career. This interface allows the Army to capture in automated records all the OCIE that has been fielded. Fielding of PBUSE began in November 2002 and ended in September 2007 for Army field units.

As you can tell, Mr. Chairman and Members of the Committee, the Army has been proactive in the development of property accountability policies and processes. We take our fiscal responsibilities very seriously and continue to look for ways to improve our property accountability enterprise. We have conducted studies on property accountability;

we have a website (LOGNET) where we encourage lively exchanges on supply policy issues; we have published articles on property accountability in Soldier magazines; and we welcome input from Soldiers, civilians and contractors on process improvements.

To close, Mr. Chairman, and Members of the Committee, on behalf of our Soldiers, we greatly appreciate the tremendous support of the Congress in the Global War on Terrorism and Army Transformation. The Army remains committed to transforming, sustaining, resetting and preparing our Soldiers and equipment for current operations and future contingencies, while continuing to uphold the values on which our Army was built. Thank you for this opportunity to appear before you today.

Mr. TIERNEY. Thank you for your testimony.

Mr. Shays gives his apologies. He has been called away. He had wanted to ask questions, and unfortunately the delay has prohibited that.

Let me ask each of you, do you think that our systems in place are working?

Mr. ESTEVEZ. Let me answer that first, Chairman Tierney. I think yes, on the macro scale. Obviously, there are some cases up in front of us of theft on the part of some individuals.

Let me start off by saying of those 2 million American men and women under uniform, most of those, the vast, vast majority of those are heroes who deserve our gratitude. Within that small group that have committed some crimes, as I stated in my statement, we support prosecuting them to the fullest extent of the law.

To the greater extent, I would put our processes for maintaining accountability and control of materiel up against the retail sector, for example.

Mr. TIERNEY. Well, at what point do you think you reach the capacity of the retail center, because it doesn't appear that is the case for some time. I notice that Ms. Finnecum indicated she put some things into effect in 2006 on that basis. It seems to me a little bit late. Did we learn nothing from prior engagements or missions?

Mr. ESTEVEZ. I think, Congressman, we have to separate stolen from our warehouses and from our controls versus stolen by individual soldiers or sailors, airmen, and marines that may have been issued that equipment and, in the combat operation where things are not quite as stable as they are inside a Wal-Mart store, for example. But the retail sector gets about 1½ to 2 percent material that they own percent of sales is lost, shrinkage.

Mr. TIERNEY. You are not making the assertion that all of the stolen materials are stolen on the battlefield?

Mr. ESTEVEZ. No, I am not, but I am saying that it is not stolen from our wholesale national inventory for the most part. Obviously, there are always cases, and we put processes and procedures to mitigate those possibilities as best we can. If we find a hole in that, we go back and we close that hole, as well.

Mr. TIERNEY. Where do you suppose things like complete uniforms are stolen from?

Mr. ESTEVEZ. Well, I can't say that was stolen, that one in particular. We issue uniforms and soldiers buy their own uniforms. They are allowed to sell them. American companies are allowed to sell those uniforms. They are legal for sale worldwide, frankly.

Mr. TIERNEY. Toward what end? I mean, other than issuing uniforms to people that are in the service going to use them in their military duty, why are people selling military uniforms?

Mr. ESTEVEZ. Our soldiers, sailors, and marines buy their uniforms at the officer level. They buy them direct from some of these companies, first.

Second, there is an industrial base issue at large. If we are going to discuss shutting down uniform sales, I think that raises a broader issue. I am probably not the person from a force protection perspective to have that discussion. My focus is on providing materiel to our folks inside the Department of Defense. But there are cer-

tainly industrial base issues on precluding some of those companies from selling materiel that is legal.

Mr. TIERNEY. Well, at least directly. You would think that if you wanted to keep some control on your inventory you wouldn't have the people sell directly, you would have them sell them through the military to their members and you could keep track of it.

Mr. ESTEVEZ. A uniform is not in DOD inventory. That is owned by the individual soldier.

Mr. TIERNEY. I understand that. My question is whether or not that is a good idea; whether, if we are worried about uniforms ending up on eBay and Craigslist and other places, whether it is a great idea to allow them to be sold outside of the chain that you can keep some monitoring on.

Mr. ESTEVEZ. Again, Congressman, that is a force protection issue regarding whether we want people that are not members of the military to be wearing our uniform, and I understand that. I am not the person to be having that discussion with.

As far as controlling our own inventory inside the Department, the uniform is not an item that we manage. We do issue uniforms and we manage those due to folks going off into battle, but once they are issued they are owned by those folks.

Mr. TIERNEY. So lets just drill down a little bit, the problem is the uniform with the infrared identifier that was purchased and sold, either as a composite or individual parts and then put together. I think that would be a problem. We don't disagree about that, or do we?

Mr. ESTEVEZ. I certainly agree that having someone dress themselves up as a U.S. military member is an issue that we need to control, from a force protection perspective. Again, I am not the force protection person. You would have to have someone in here to discuss that.

Mr. TIERNEY. That is the beauty of bureaucracy.

Mr. ESTEVEZ. But a uniform, in and of itself, does not gain access to anywhere. It is a uniform, it is procedures, it is a TAC card, your entry card. So a uniform in and of itself does not gain entrance to an facility.

Mr. TIERNEY. It certainly helps, doesn't it?

Mr. ESTEVEZ. It lowers the threshold.

Mr. TIERNEY. As in that incident in January where somebody put one on and ended up killing five of our people. They certainly lowered the threshold enough to cause some damage there.

Mr. ESTEVEZ. I am not the person to discuss that particular incident, but there is more to that incident than just a uniform. And there is tactics, techniques, and procedures that mitigate those risks out in the field.

Mr. TIERNEY. So you have identified two possible ways of this equipment or supplies getting into control. One is that they are stolen directly from the warehouse or in your control. Each of you contested you have that perfectly under control, as best we can possibly do; there is nothing else we can do to improve those system?

Mr. ESTEVEZ. We are always looking at other ways to control our inventory. Like our counterparts in the commercial sector, we have a viable program to introduce things like radio frequency identification technology to help us manage our inventory. We are one of the

leaders of pushing that technology across the globe right now, quite frankly. We are moving toward more serial numbered tracking of our materiel so you can get down to each part versus the gross level of parts. Again, we are leading the world in that push.

But those are things that are out there in the commercial sector, so we are constantly assessing how things are done to better control our inventory and better account for that inventory.

Mr. TIERNEY. What would you do or what do you recommend be done to stop this type of thing? The vests, for instance, where do you suspect they came from? Was it the warehouse? Was it some place else in your custody? Or was it a member of the forces selling it later on, or was it somebody that stole it from somewhere else?

Mr. ESTEVEZ. The outer tactical vest, I am not sure. I would have to go back to the GAO report. I can't say whether that was stolen or whether that was an individual soldier. That is an accountable item that the soldier should have turned in, whether that was from an individual soldier.

Mr. TIERNEY. Does seeing any of this displayed and listening to the testimony earlier and reading the Government Accountability Office's report strike the notion in you that we ought to change our policies in any way?

Ms. FINNECUM. Sir, I don't believe we need to change our policies. I think we need, in some instances, to do a better job of enforcing our policies and procedures.

Mr. TIERNEY. Speak to me specifically, if you would, please, about what better enforcement would look like, in your estimation.

Ms. FINNECUM. I would tell you, sir, if you take the outer tactical vest that you are looking at, when we were pushing so desperately to get those fielded, we did not put them on the individual clothing records. We issued it to a soldier, and so when he came out of the war zone, redeployed back to home station, we did not have on his record whether he had been issued that outer tactical vest or not.

Mr. TIERNEY. It strikes me, this is not the first time we have deployed soldiers in this country.

Ms. FINNECUM. No, sir.

Mr. TIERNEY. And given them equipment that we have had to track. I mean, we have had a number of other missions. My earlier question, did we learn nothing from those occasions so that when we have to deploy people we were ready to ramp up and do it with these precautions in place.

Ms. FINNECUM. Well, what I would tell you, Mr. Chairman, is that if you take Operation Desert Storm, that only lasted for such a short amount of time, we were not rapidly fielding new technology like we have done here.

Mr. TIERNEY. And nobody anticipated it?

Ms. FINNECUM. No, sir. If you look at our budget, we certainly didn't anticipate fielding all of this new gear in such a short span of time.

Mr. TIERNEY. This is stunning that nobody in that whole outfit thought that there might be an occasion where this has to be done and we would better put it in place. You don't need the money to actually conceptualize a plan. You don't need that much imagination, I don't think, to think that you would be in a situation like

this some day. I just think it is sort of stunning that nobody was ready for it.

Ms. FINNECUM. Well, again, sir, we have gone from a flack vest, which you have up there, to an outer tactical vest, to a new IOTV. We have gone through three iterations in 5 years. I will tell you, as we fielded the IOTV we can account for the issue of every IOTV. We know which soldier has it and when it got issued to him, and when he comes out of the war zone we will collect it.

Mr. TIERNEY. And why is that not the case in the other items?

Ms. FINNECUM. Sir, because as we were fielding them so rapidly and trying to get them out there because of the pressure—they had nothing that would give them the protection that they needed. Now we continue to improve.

Mr. TIERNEY. So you developed the system after the fact, and now you are applying the system?

Ms. FINNECUM. No, sir, we had the system; we didn't enforce the system. We have always required soldiers to carry this gear on their clothing records. In our effort to push it out there, we took the gear to Iraq and issued it to soldiers, in many cases on the FOBs. We did not capture it because of doing it in the environment. We have changed that. We know that we made mistakes in that. That is why we rescinded our policy.

Mr. TIERNEY. That is a little bit more direct. It could have been done; it just wasn't done.

Ms. FINNECUM. It was not done.

Mr. TIERNEY. That is at least an acknowledgement of making sure that looking forward we will know what we didn't do.

Ms. FINNECUM. Yes.

Mr. TIERNEY. We realize what could have been done, and we just messed up and didn't do it.

Ms. FINNECUM. Yes.

Mr. TIERNEY. Somebody hopefully was held accountable for that, and now we will move forward and hopefully keep improving on the system that we have. That is at least a start.

Ms. FINNECUM. Yes, sir. I have to tell you, if I am still in charge of supply policy and we get back into this, wartime accountability procedures will not be put in place. We thought we were doing something that would be of benefit, and instead it has caused us some problems, and we have taken corrective action.

Mr. TIERNEY. OK. The other military items, like the night vision goggles, Mr. Estevez, you said that they were probably stolen from a manufacturer or something like that. How do you think they got into play?

Mr. ESTEVEZ. Those were legally sold by manufacturer.

Mr. TIERNEY. With the insert for infrared reading?

Mr. ESTEVEZ. Yes, sir.

Mr. TIERNEY. The sensitive information?

Mr. ESTEVEZ. Yes, sir. There is an export control on that item, but it is legal to sell that item in the United States.

Mr. TIERNEY. Do you think that is wise? Some of the earlier witnesses today made a recommendation that some of that equipment just be banned and not allowed to be sold. Would that be a way of solving some of our issues here?

Mr. ESTEVEZ. Yes, but there are issues on the industrial base that we need to concern ourselves with. We have to deal with the fact that this is technology that is not owned by the Department of Defense; it is owned by companies who are subject to the export control laws of the United States in moving that technology.

Mr. TIERNEY. Are there other uses for that particular technology that the public may not be aware of?

Mr. ESTEVEZ. Hunting.

Mr. TIERNEY. Are there other uses that would be more compelling in protecting our troops other than sports?

Mr. ESTEVEZ. Night vision goggles are all over the world.

Mr. TIERNEY. Not with the special insert, though.

Mr. ESTEVEZ. I am not even sure what the special insert does.

Mr. TIERNEY. The infrared item on our particular troops——

Mr. ESTEVEZ. Well, actually, any night vision goggle will read that tab. That is also a legal technology that is sold worldwide, though we restrict it from export with an export control.

Mr. TIERNEY. So it is sold worldwide.

Mr. ESTEVEZ. Well, we are not the only——

Mr. TIERNEY. They can get it someplace else?

Mr. ESTEVEZ. Congressman Tierney, we are not the only country that makes that IR technology.

Mr. TIERNEY. That particular one?

Mr. ESTEVEZ. That particular one.

Mr. TIERNEY. So that we have more than just a problem with controlling its export from this country; we have a problem with it getting used because they bought it somewhere else.

Mr. ESTEVEZ. That technology is worldwide, global technology. That is not the only method that we would identify friend or foe in the battlefield.

Mr. TIERNEY. OK. Having heard the testimony earlier, and one of the individuals indicating that eBay already bans the sale of police uniforms on its system, do either of you think that it makes sense to talk or think about banning the sale of military items and prohibiting their sale on the Internet, period, or at least some of them?

Mr. ESTEVEZ. I certainly think we need to have that dialog with eBay. But, again, because most of these items that are up here are legal, unless they were stolen, it becomes hard to control that because you can sell night vision goggles legally in the United States. Maybe not the night vision goggles, the latest advancement of those, but if I was going to sell something on eBay I wouldn't say night vision goggle with special U.S. military insert; I would just say night vision goggles. You can sell body armor legally in the United States. So in order to control that with eBay, we would have to go through some other rigor on how to control items that are legally sold by domestic——

Mr. TIERNEY. Does anybody at DOD ever have that discussion or ever sit down and start thinking about whether there ought to be some recommendations made in that regard?

Mr. ESTEVEZ. DOD is a large place, Congressman.

Mr. TIERNEY. In your outfit?

Mr. ESTEVEZ. From a logistics standpoint, sir, that is not a logistics management issue. Again, we are focused on maintaining our

inventory and ensuring we have that inventory for the support of our forces.

Mr. TIERNEY. Within the constraints of what it is each of you do, what assurance can you give the public that items like this will not come from any lapse in what it is you are doing in tracking this equipment?

Ms. FINNECUM. I would say to you that most of that gear would be a result of a criminal activity occurring, somebody stealing the property. I can't give you that assurance with regards to the Army combat uniform or boots or berets. If you don't mind, I would take just a moment. The Army combat uniform and the boots, the berets, those are considered personal items of clothing. The rest of the gear up there, the plates, the mask, the vest, those are considered organizational items. The Army pays for those and the Army tracks the accountability of those. When a soldier either PCSes, leaves the Army, retires, his clothing record is reviewed and he is responsible to turn that gear in. He has to pay for it if he does not have it in his possession when it is time to clear. If he has wilfully disposed of it inappropriately, the military can take corrective action against it plus collect the dollars.

For the Army combat uniform, many of our soldiers pay for that out of their own pocket. Officers have to buy that uniform. It would be very hard, I think, to tell them you can't resell that item, when they have purchased it with their own resources.

That is my personal opinion, sir.

Mr. TIERNEY. I guess the question would be whether or not they should be purchasing it or the Army ought to be purchasing it and issuing it, one or the other. That would be a policy approach to that.

Ms. FINNECUM. Yes, sir, that is a policy and a resource issue.

Mr. TIERNEY. You also indicated that the Army's total recall operation yielded 20,000 items returned with $135 million value in less than 2 years.

Ms. FINNECUM. Yes, sir.

Mr. TIERNEY. That is pretty big leakage.

Ms. FINNECUM. I think it goes directly back in many cases to when we had that wartime accountability and we fielded items that we did not pick up to the appropriate accountable record.

Mr. TIERNEY. Well, the recall only went into effect, when, in 2006?

Ms. FINNECUM. Yes, sir.

Mr. TIERNEY. So you are saying all of that 20,000 items and $135 million in value is all from pre-2006 disposition?

Ms. FINNECUM. I think there is a strong possibility that is where it came from.

Mr. TIERNEY. OK. Do you have any numbers from more recently to show that there has been a decline, then, that this thing is winding up?

Ms. FINNECUM. What I can talk to you about is just overall inventory accuracy rates. We require literally everything in the Army inventory to be inventoried—sorry for the duplication of words.

Mr. TIERNEY. That is all right.

Ms. FINNECUM. For weapons, they are inventoried quarterly. For going out and just checking on a warehouse of materiel that be-

longs to a specific unit, that is done on an annual recurring basis. Clothing items are either you do a lay-down where we say we want to make sure you have your gear and the first sergeant says bring it in, and you look at it, and you make sure he has what is on his clothing record.

Our inventory rates are in the 98 percentile in terms of accuracy. And, as Mr. Estevez——

Mr. TIERNEY. That is since 2006?

Ms. FINNECUM. No, sir. That is in terms of what is on the accountable record. Found on installation or things that we pick up, we track that.

Mr. TIERNEY. I guess one question, if you don't mind me interrupting, would be this: you started this total recall operation in 2006?

Ms. FINNECUM. Yes, sir.

Mr. TIERNEY. All right. And that deals with equipment that you issued as of that date?

Ms. FINNECUM. Yes, sir.

Mr. TIERNEY. OK. So are we able to track what kind of leakage we have with respect to that equipment over these last couple of years and see if it is better than the 20,000 items and $135 million of value from what you say was previous issuance?

Ms. FINNECUM. I would have to take that for the record and get back to you, sir.

Mr. TIERNEY. All right. I would at least like to know if you have a system to track that so we can determine whether or not your new system is working better than your old system.

Ms. FINNECUM. No. We do have records of our inventory accuracy. When we go and do it, we know whether we have found 100 percent of what we have on our accountable record or if there is a shortfall.

Mr. TIERNEY. OK. That would be good to know for us, and know how it measures up against past records, whether or not you have a handle on this thing now going forward.

Ms. FINNECUM. Yes, sir.

Mr. TIERNEY. I don't want to beat this thing to death. I appreciate your both being here. But let me ask each of you to give me your thoughts generally on this. You have heard the testimony this morning. You have read the GAO report. You know what we are concerned about here. What recommendations do you have to make in terms of moving forward and trying to stop those kinds of purchases with those kinds of serious implications from being made.

Mr. ESTEVEZ. Thank you, Mr. Chairman. Let me start off.

Again, any assistance we have in looking at our inventory systems and processes, frankly, is beneficial to the Department, because it is always good to help tighten up your procedures and processes. We have worked with GAO before and we have worked with this committee before to do that very thing, and we will continue to do so.

Individual theft is a hard thing to stop, and we are working to do that and identifying that, as Mr. Beardall and Mr. Kutz alluded to earlier.

Mr. TIERNEY. Won't that new system Ms. Finnecum talks about address that pretty starkly, if somebody is responsible for their

items and you know whether or not they turn it in when they are discharged?

Mr. ESTEVEZ. That is the process the Army has put in place, to do exactly that.

Mr. TIERNEY. And does that go across all the services now, or is the Army the only service?

Mr. ESTEVEZ. No. Each service manages how the individual issue, certain gear that they expect back to the Government.

Mr. TIERNEY. And are they all on the same page on this, or are there different levels of success with their programs, running various programs and having different results?

Mr. ESTEVEZ. I would have to take that for the record. But let me just say that there are different degrees of vulnerability in a ground combat situation that the Army and the Marine Corps find themselves in in Iraq versus a more or less fixed even though expeditionary installation that the Air Force may be working out of or on a vessel that the Navy may be working out of.

Mr. TIERNEY. I understand.

Mr. ESTEVEZ. So there are different degrees across the services.

Mr. TIERNEY. Sure.

Mr. ESTEVEZ. But we obviously need to tighten down what happens with an individual.

As I said, on the wholesale level I think we are pretty good, but we are always looking at that, too.

I think the larger question is: what do we allow for sale to the general public and to the American people, quite frankly, and what are our expectations there and what are the implications for the industrial base? Frankly, that is something that you, as a Congressman, and we as the Department and Commerce and other folks at Justice, Homeland Security, should be having that dialog at large, because some of these items are, as I pointed out, quite legal, and some of the technology is not just a motion technology, it is global technology, and we need to deal with the implications of that.

Mr. TIERNEY. It seems to make sense that an interagency group might be put together to have just that discussion and make recommendations, I would think, on that, and that might be one of the things that results from this hearing.

Ms. Finnecum.

Ms. FINNECUM. Sir, what I would offer to you is it is very distressing to see SAPI plates available for sale. I mean, the Army finally has turned the corner on our protective gear where every soldier going into Afghanistan and Iraq gets what he needs before he enters the theater. But 5 years ago that wasn't the case. It is very disturbing for anybody to see something available commercially that you can't get to give to your own soldiers.

I like the idea of trying to identify things that shouldn't be sold and that there is an immediate flag that says don't even think about trying to put this on eBay.

I know that there is a challenge with that, because many of these things are commercial products, but I would think body armor, tactical vests, we could figure out a way to crack the code on that.

Mr. TIERNEY. Would it be too much to ask for you to go back and talk to your folks, your superiors, whoever you have to talk to,

about starting to put a list of those things together that they think would be appropriate for that?

Ms. FINNECUM. Sure.

Mr. TIERNEY. To the extent that involves you, Mr. Estevez, I would appreciate you doing that, as well.

Mr. ESTEVEZ. Certainly, sir.

Mr. TIERNEY. Thank you.

I was just going to note here it indicates the Department of Defense recently discovered a lost nuclear missile component that was shipped to Taiwan. It is that kind of thing that sort of gets everybody unnerved, so that there are obviously issues out there that we have to have some level of confidence that this kind of stuff is under control and moving forward on that.

I think we have taken some lessons out of this hearing. I appreciate your willingness to cooperate on some of those lists. On that, I think we still have some things to do with the manufacturing companies and, as you call them, the industrial base that will have to be included on that discussion, and the determination of just what makes sense to have the public use and then what doesn't make sense in terms of trying to balance safety of our troops against some other commercial or private use that people may have.

Do either of you have any final comment that you would like to make?

[No response.]

Mr. TIERNEY. Thank you for your testimony. This meeting is adjourned. Thank you.

[Whereupon, at 12:45 p.m., the subcommittee was adjourned.]