United States Government Accountability Office

GAO

Report to Congressional Requesters

March 2010

DEFENSE SUPPLIER BASE

DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts

GAO-10-389

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAR 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Government Accountability Office,441 G Street NW,Washington,DC,20548**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**35**	

March 2010

DEFENSE SUPPLIER BASE

DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-389, a report to congressional requesters

Why GAO Did This Study

Counterfeit parts—generally those whose sources knowingly misrepresent the parts' identity or pedigree—have the potential to seriously disrupt the Department of Defense (DOD) supply chain, delay missions, and affect the integrity of weapon systems. Almost anything is at risk of being counterfeited, from fasteners used on aircraft to electronics used on missile guidance systems. Further, there can be many sources of counterfeit parts as DOD draws from a large network of global suppliers.

Based on a congressional request, GAO examined (1) DOD's knowledge of counterfeit parts in its supply chain, (2) DOD processes to detect and prevent counterfeit parts, and (3) commercial initiatives to mitigate the risk of counterfeit parts.

GAO's findings are based on an examination of DOD regulations, guidance, and databases used to track deficient parts, as well as a Department of Commerce study on counterfeit parts; interviews with Commerce, DOD, and commercial-sector officials at selected locations; and a review of planned and existing efforts for counterfeit-part mitigation.

What GAO Recommends

GAO recommends that DOD leverage existing initiatives to establish anticounterfeiting guidance and disseminate this guidance to all DOD components and defense contractors. DOD concurred with each of the recommendations.

View GAO-10-389 or key components.
For more information, contact Belva Martin at (202) 512-4906 or martinb@gao.gov.

What GAO Found

DOD is limited in its ability to determine the extent to which counterfeit parts exist in its supply chain because it does not have a departmentwide definition of the term "counterfeit" and a consistent means to identify instances of suspected counterfeit parts. While some DOD entities have developed their own definitions, these can vary in scope. Further, two DOD databases that track deficient parts—those that do not conform to standards—are not designed to track counterfeit parts. A third governmentwide database can track suspected counterfeit parts, but according to officials, reporting is low due to the perceived legal implications of reporting prior to a full investigation. Nonetheless, officials we met with across DOD cited instances of counterfeit parts, as shown in the table below. A recent Department of Commerce study also identified the existence of counterfeit electronic parts within DOD and industry supply chains. DOD is in the early stages of developing a program to help mitigate the risks of counterfeit parts.

Examples of Counterfeit Parts in DOD's Supply Chain

Part	Description
GPS oscillators	The Air Force and Navy use these oscillators for navigation on over 4,000 systems. Part failure could affect the mission of certain systems.
Self-locking nuts	Self-locking nuts, used in aviation braking, were cracking.
Titanium	The supplier sold substandard titanium, used in fighter jet engine mounts.
Brake shoes	Brake shoes were made with substandard materials, including seaweed.

Source: DOD.

DOD does not currently have a policy or specific processes for detecting and preventing counterfeit parts. Existing procurement and quality-control practices used to identify deficient parts are limited in their ability to prevent and detect counterfeit parts in DOD's supply chain. For example, several DOD weapon system program and logistics officials told us that staff responsible for assembling and repairing equipment are not trained to identify counterfeit parts. Some DOD components and prime defense contractors have taken initial steps to mitigate the risk of counterfeit parts, such as creating risk-assessment tools and implementing a new electronic parts standard.

Also facing risks from counterfeit parts, individual commercial sector companies have developed a number of anticounterfeiting measures, including increased supplier visibility, detection, reporting, and disposal. Recent collaborative industry initiatives have focused on identifying and sharing methods to reduce the likelihood of counterfeit parts entering the supply chain. Because many of the commercial sector companies produce items similar to those used by DOD, agency officials have an opportunity to leverage knowledge and ongoing and planned initiatives to help mitigate the risk of counterfeit parts as DOD develops its anticounterfeiting strategy.

Contents

Abbreviations

DCMA	Defense Contract Management Agency
DLA	Defense Logistics Agency
DOD	Department of Defense
GIDEP	Government Industry Data Exchange Program
HMMWV	High Mobility Multi-purpose Wheeled Vehicles
JDRS	Joint Deficiency Reporting System
Joint STARS	Joint Surveillance Target Attack Radar System
MDA	Missile Defense Agency
OCM	Original Component Manufacturer
PDREP	Product Data Reporting and Evaluation Program

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

March 29, 2010

The Honorable Sherrod Brown
Chairman
Subcommittee on Economic Policy
Committee on Banking, Housing, and Urban Affairs
United States Senate

The Honorable Evan Bayh
Chairman
Subcommittee on Security and International Trade and Finance
Committee on Banking, Housing, and Urban Affairs
United States Senate

DOD draws from a large network of global suppliers and manages over 4 million different parts at a cost of over $94 billion; therefore, counterfeit parts can enter its supply chain.[1] Almost anything is at risk of being counterfeited including fasteners used on aircraft, electronics used on missile guidance systems, and materials used in body armor and engine mounts. Counterfeit parts have the potential to cause a serious disruption to DOD supply chains, delay ongoing missions, and even affect the integrity of weapon systems. Counterfeits are not limited to the DOD supply chain and exist in other government entities, such as the National Aeronautics and Space Administration and the Department of Energy, as well as in many commercial settings as diverse as software, commercial aviation, automotive parts, and consumer electronics and can threaten the safety of consumers.

On the basis of your interest in DOD's ability to detect and prevent counterfeit parts, we examined (1) the extent of DOD's knowledge of counterfeit parts in its supply chain, (2) DOD processes to detect and prevent counterfeit parts, and (3) commercial initiatives to mitigate the risk of counterfeit parts in their supply chains.

To conduct our work, we reviewed regulations, guidelines, and databases to determine how DOD defines and tracks counterfeit parts. We

[1]For purposes of this report, we are using the term "counterfeit" to refer generally to instances in which individuals or companies knowingly misrepresent the identity or pedigree of a part.

interviewed senior DOD headquarters officials, as well as weapon system program and logistics officials from the Army, Navy, Air Force, Missile Defense Agency (MDA), and Defense Logistics Agency (DLA) about their knowledge of the counterfeit parts problem and instances of counterfeits. We also reviewed a Department of Commerce study of counterfeit electronic parts and met with officials to discuss their findings. To identify practices for preventing and detecting counterfeit parts, we selected and reviewed a nongeneralizable sample of 16 weapon systems representing a mix of aerospace, ground vehicle, and missile defense sectors with mature technologies. We identified initiatives planned and practices used by DOD and defense contractors to prevent and detect counterfeit parts. To identify commercial practices used to mitigate the risk of procuring counterfeit parts, we interviewed officials from selected companies and associations within the automotive, aviation, and electronics industries—sectors that have experienced counterfeit parts in their supply chains or produce items similar to those used by the DOD programs we reviewed. For more on our scope and methodology, see appendix I. We performed our review from January 2009 through March 2010, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Generally, the term counterfeit refers to instances in which the identity or pedigree of a product is knowingly misrepresented by individuals or companies. Counterfeiters often try to take advantage of the established worth of the imitated product, and the counterfeit product may not work as well as the genuine article. The threat of counterfeit parts continues to grow as counterfeiters have developed more sophisticated capabilities to replicate parts and gain access to scrap materials that were thought to have been destroyed. Counterfeiters exist across industries and are able to respond to changes in market conditions. Counterfeit parts can be quickly distributed in online markets. Almost every industry can be affected by counterfeit parts.

Counterfeiting can affect the safety, operational readiness, costs, and the critical nature of the military mission. DOD procures millions of parts through its logistics support providers—DLA supply centers, military service depots, and defense contractors—who are responsible for ensuring the reliability of the DOD parts they procure. As they draw from a

large network of suppliers in an increasingly global supply chain, there can be limited visibility into these sources and greater risk of procuring counterfeit parts. Also, as DOD weapon systems age, products required to support it may no longer be available from the original manufacturers or through franchised or authorized suppliers but could be available from independent distributors, brokers, or aftermarket manufacturers. Parts and components bought by DOD can come from different types of suppliers, as shown in table 1.

Table 1: Types of DOD Suppliers of Parts and Components

Type of source	Description
Original component manufacturer (OCM)	Organization that designs, or engineers, or both, a part and is pursuing or has obtained the intellectual property rights to that part.
Franchised distributor	Distributor with which OCM has a contractual agreement to buy, stock, repackage, sell and distribute its product lines.
Independent distributor	Distributor that purchases new parts with the intention to sell and redistribute them back into the market, and which does not have contractual agreements with OCM.
Broker / broker distributor	In the independent distribution market, brokers are professionally referred to as independent distributors. A broker distributor is a type of independent distributor that works in a just-in-time environment by searching the industry and locating parts for customers.
Aftermarket manufacturer	Manufacturer that either produces and sells replacement parts authorized by the OCM, or produces parts through emulation, reverse-engineering, or redesign that match OCM specifications and satisfy customer needs without violating OCM intellectual property rights, patents, or copyrights.

Source: GAO summary of SAE International data.

Note: The definitions are based on SAE Aerospace Standard 5553, Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition, issued in April 2009.

The Extent of Counterfeit Parts in DOD's Supply Chain Is Unknown

DOD Does Not Have a Common Definition for Counterfeit Parts

DOD lacks a departmentwide definition of the term counterfeit. In our discussions with DOD logistics and program officials, several told us they are uncertain how to define counterfeit parts, and many officials also stated that a common definition would be useful. In the absence of a departmentwide definition of counterfeit parts, some DOD entities have developed their own. Although there are similarities among these definitions, the scope varies. For example, one DLA supply center defined a part as counterfeit only when it misrepresented the part's trademark. In contrast, a different DLA supply center defined counterfeit parts more broadly to include misrepresentations of a part's quality and performance. In August 2009, DOD endorsed an aerospace standard created by SAE International that includes a definition of the term counterfeit part.[2] While this standard is available departmentwide, it is left to the discretion of each DOD program as to whether it wants to use the standard. Some DOD officials who support aviation programs, such as the F-15, told us they were using or considering use of the standard, while other DOD officials told us they were unaware of it. Others were uncertain how it would apply beyond avionics to components like fasteners, uniforms, tires, and brake pads. In some cases, officials stated the definition is too broad for their use.

[2]SAE International is a member organization that shares information and exchanges ideas for advancing the engineering of mobility systems. SAE Aerospace Standard 5553 defines a counterfeit part as a suspect part that is a copy or substitute without legal right or authority to do so or one whose material, performance, or characteristics are knowingly misrepresented by a supplier in the supply chain.

DOD Databases Do Not Capture Data on Counterfeit Parts

The two primary databases DOD uses to report deficient parts—the Product Data Reporting and Evaluation Program (PDREP) and the Joint Deficiency Reporting System (JDRS)[3]—have data fields that enable users primarily to track information on deficient parts, but neither is designed specifically to track counterfeit parts. DOD considers products that do not conform to quality or design specifications to be deficient.[4] Both of these systems allow users to enter a cause code for why a part is deficient, but neither database has a code to capture the deficiency as counterfeit. As a result, users are limited to reporting a suspected counterfeit part in narrative descriptions. However, identifying instances of counterfeit parts through searches of narrative descriptions is difficult due to a lack of common terminology. For example, an Air Force official told us that when he searched the JDRS system, he found 3 out of more than 94,000 entries that discussed counterfeit parts. We performed similar searches and found that the terms associated with counterfeit are rarely included in narrative fields. In consultation with database managers from both PDREP and JDRS, we developed a list of 11 terms associated with counterfeit parts and searched the systems' narrative fields for these terms over a 5-year period ranging from October 1, 2004, to September 30, 2009.[5] We found that less than 1 percent of the reports in the databases included one of our search terms, and a manual review of these cases determined that only a few were relevant to counterfeit parts.

DOD entities also have access to the Government Industry Data Exchange Program (GIDEP)—a Web-based database—that allows government and industry participants to share information on deficient parts, including counterfeit. Specifically, a GIDEP user can submit information on a suspected counterfeit part and GIDEP policy allows for up to 15 days for the supplier to respond before posting this information to the database. A 1991 Office of Management and Budget policy letter instructs government

[3]PDREP is an automated information system managed by the Navy to track quality, including part deficiencies, and is used by the Navy, DLA, the Defense Contract Management Agency (DCMA), Army ground forces, and the Marine Corps. JDRS is an automated information system that Naval Air Systems Command developed for reporting of part deficiencies for aeronautics. JDRS users include Naval Air Systems Command, Army Space and Missile Defense Command, the Air Force, the Coast Guard, and DCMA.

[4]A part that is found to be deficient is not necessarily counterfeit as counterfeit parts involve the intent to misrepresent the identity or pedigree of a part.

[5]The terms included in the list were "bogus," "counterfeit," "deliberate," "falsify," "fraud/fraudulent," "illegal," "intentional," "knowingly," "misrepresent," "piracy," and "unauthorized product substitution."

agencies to use GIDEP to report deficient[6] parts. However, the GIDEP Deputy Program Manager told us that GIDEP is not widely used to report suspect counterfeits. He stated that the policy letter was intended as a short-term requirement for government use of GIDEP until a Federal Acquisition Regulation change was made, which never occurred. He further stated that DOD had previously issued a military standard[7] requiring use of GIDEP, which was canceled during acquisition reform in 1996. DOD logistical support providers and contractors that we spoke with cited concerns with using the GIDEP system such as delayed reporting, liability issues, and effect on criminal investigations.

- Delayed Reporting: A 15-day delay in posting reports to the system allows suppliers to investigate and respond to reports concerning their products. However, during this time, a counterfeit part could continue to be used or purchased.[8]
- Liability Issues: Some officials expressed concerns about the legal implications of reporting a part as suspect counterfeit before it had been proven. Fear of lawsuits was repeatedly cited as a reason cases are not reported to GIDEP.
- Effect on Investigations: Another concern officials raised about reporting cases to GIDEP is the possibility of alerting suppliers to active investigations, as investigators may want to monitor a supplier's activities to gather further evidence of possible illegal activity.

Counterfeit Parts Have Been Found in DOD's Supply Chain

In the absence of data collected on counterfeit parts, we visited military services, MDA, DLA, selected defense contractors, and suppliers; many of these officials provided specific examples of counterfeit or suspect counterfeit parts. As definitions of "counterfeit" vary within DOD, they generally refer to instances in which individuals or companies knowingly misrepresent the identity or pedigree of a part. Specific examples of the types of counterfeits encountered by DOD include

[6]The policy letter uses the term "nonconforming," which has the same meaning in DOD as the term "deficient."

[7]Department of Defense, Military Standard (MIL-STD)-1556B, *Government/Industry Data Exchange Program, Contractor Participation Requirements* (Feb. 24, 1986).

[8]According to the GIDEP Deputy Program Manager, this 15-day delay is in addition to the time—which can range from 30–180 days—that the DOD logistical support providers and contractors spend gathering evidence before reporting the suspect supplier to GIDEP.

- parts falsely claimed by the supplier to be from a particular manufacturer,
- parts that deliberately do not contain the proper internal components or construction consistent with the ordered part,
- authentic parts whose age or treatment have been knowingly misrepresented, and
- parts with fake packaging.

We met with DOD program officials and logistical support providers across 16 DOD programs and three DLA supply centers and discussed instances of suspect and confirmed counterfeit parts; examples are shown in appendix II. About two-thirds of these instances involved fasteners or electronic parts while the remainder included materials ranging from titanium used in aircraft engine mounts to Kevlar used in body armor plates. The following illustrates the examples of counterfeit parts and actions taken provided by officials across DOD.

Army

- **Seatbelt clasps:** Seatbelt parts were made from a grade of aluminum that was inferior to that specified in DOD's requirements. The parts were found to be deficient when the seatbelts were accidentally dropped and they broke.

Navy

- **Routers:** The Navy, as well as other DOD and government agencies, purchased counterfeit network components—including routers—that had high failure rates and the potential to shut down entire networks. A 2-year FBI criminal investigation led to 10 convictions and $1.7 million in restitution.

Air Force

- **Microprocessor:** The Air Force needed microprocessors that were no longer produced by the original manufacturer for its F-15 flight-control computer. These microprocessors were procured from a broker and F-15 technicians noticed additional markings on the microprocessor and character spacing inconsistent with the original part. A total of four counterfeit microprocessors were found and as a result were not installed on the F-15's operational flight control computers.
- **Global Positioning System:** Oscillators used for navigation on over 4,000 Air Force and Navy systems experienced a high failure rate and failed a retest. These oscillators were provided by a supplier that Global Positioning System engineers had previously disapproved as a supply source. Air Force officials stated that while the failure would not cause a safety-of-flight issue, it could prevent some unmanned systems from returning from their missions.

MDA

- **Operational Amplifiers:** A counterfeit operational amplifier, which can be used on multiple MDA systems, was identified on MDA hardware during testing. The failed part was found on a circuit board

supplied by a subcontractor. It was later determined that the subcontractor purchased these parts from a parts broker who was not authorized to distribute parts by the original component manufacturer. To date, all parts have been accounted for and secured from further use on any other products.

- **Microcircuits:** A counterfeit microcircuit, which can be used on multiple MDA systems, was identified on MDA hardware. MDA's visual inspection showed that the part was resurfaced and remarked, which prompted authenticity testing. Tests revealed surface scratches, inconsistencies in the part marking, and evidence of tampering. These parts were purchased from a parts broker who was not authorized to distribute parts by the original component manufacturer.

DLA

- **Packaging and small parts:** During a 2-year period, a supplier and three coconspirators packaged hundreds of commercial items from hardware and consumer electronics stores and labeled them as military-grade items. For example, the supplier placed a rubber washer from a local hardware store in a package labeled as a brass washer for use on a submarine. The supplier also labeled the package containing a circuit from a personal computer as a $7,000 circuit for a missile guidance system. The suppliers avoided detection by labeling packages to appear authentic, even though they contained the wrong part. The supplier received $3 million from contracts totaling $8 million before fleeing the country. He has been extradited to the United States and awaits trial; his coconspirators have been convicted.

The Department of Commerce also identified the existence of counterfeit parts in DOD's supply chain in a study released in January 2010.[9] This study, sponsored by Naval Air Systems Command, was designed to provide statistics on the extent of infiltration of counterfeit electronic components into the United States industrial and supply chains, to understand how different segments of the supply chain currently address the issue, and to gather best practices from the supply chain on how to handle counterfeits. The department received completed surveys from 387 respondents representing five segments in the U.S. supply chain—OCMs, distributors and brokers, circuit-board assemblers, prime contractors and

[9]U.S. Department of Commerce, *Defense Industrial Base Assessment: Counterfeit Electronics* (Washington, D.C., January 2010). In conducting its assessment, the Department of Commerce defined a counterfeit electronic parts as one that is not genuine because it: is an unauthorized copy; does not conform to original OCM design, model, or performance standards; is not produced by the OCM or is produced by unauthorized contractors; is an off-specification, defective, or used OCM product sold as "new" or working; or has incorrect or false markings or documentation, or both.

subcontractors, and DOD entities. The surveys included questions addressing past experiences with counterfeit parts and practices used in identifying them. While the study did not provide a number for the total counterfeit incidents at DOD, it noted that 14 DOD organizations had reported incidents of counterfeit parts. The study's survey respondents identified a growth in incidents of counterfeit parts across the electronics industry from about 3,300 in 2005 to over 8,000 incidents in 2008. Survey respondents attributed this growth to a number of factors, such as a growth in the number of counterfeit parts, better detection methods, and improved tracking of counterfeit incidents.

DOD Is in the Early Stages of Gathering Information on the Counterfeit Parts Problem

In April 2009 DOD formed a departmentwide team—partially in response to media reports that highlighted the existence of counterfeit parts in the DOD supply chain[10]—to collect information and recommend actions to mitigate the risk of counterfeit parts in its supply chain. Standing participants include representatives from DOD's Office of the Under Secretary of Defense for Acquisition, Technology & Logistics, DLA, the Defense Contract Management Agency, the Defense Standardization Program Office, MDA, and military law enforcement and investigative agencies.[11] The team also incorporates liaisons from groups such as the defense industry, Defense Intelligence Agency, Federal Aviation Administration, National Aeronautics and Space Administration, Department of Energy, Department of Commerce, and state and federal law enforcement organizations.

To gather preliminary information on the counterfeit problem in DOD, the team has visited three DOD facilities to observe operations and discuss occurrences of and problems with counterfeit in the supply chain. The team plans to complete a review of current DOD processes and procedures for the handling and storage, detection, disposal, and reporting of counterfeit parts by July 2010. The team then plans to assess the

[10]"Fake Parts are Seeping Into Military Aircraft Maintenance Depots," *Inside the Air Force* (Mar. 28, 2008) and "Dangerous Fakes: How Counterfeit, Defective Computer Components from China Are Getting into U.S. Warplanes and Ships," *Business Week* (Oct. 2, 2008).

[11]The Air Force Material Command is also developing a handbook that aims to educate its workforce on what a counterfeit part is, steps to be taken to prevent counterfeit parts from entering the supply chain, detection methods and ways to identify counterfeit parts that have already entered the supply chain, and what reporting is to be accomplished when counterfeit parts are identified. However, the command is delaying the distribution of this handbook to potentially be incorporated into a departmentwide handbook.

policies, procedures, and metrics needed to address the issue of counterfeit parts . Additionally, the team is developing training materials that it plans to make available through the Defense Acquisition University, to increase the general awareness of counterfeit parts and plans to develop additional training on detection techniques.

DOD's Existing Practices Are Limited in Protecting Its Supply Chain against Counterfeit Parts

DOD Relies on Existing Procurement and Quality Control Practices That Are Not Specifically Designed to Address Counterfeit Parts

DOD relies on existing procurement and quality control practices to ensure the quality of the parts in its supply chain. However, these practices are not designed to specifically address counterfeit parts. Limitations in the areas of obtaining supplier visibility, investigating part deficiencies, and reporting and disposal may reduce DOD's ability to mitigate risks posed by counterfeit parts.

Obtaining supplier visibility: DOD and its prime contractors rely on suppliers across a global supply chain for parts and materials. Federal acquisition regulations require that agency contracting officers consider whether a supplier is responsible before awarding a contract and note that the award of a contract to a supplier based on the lowest price alone can result in additional costs if there is subsequent default, late deliveries, or other unsatisfactory performance.[12] While cost or price is always a consideration when purchasing goods, an abnormally low price, especially from an unfamiliar source, can be an indication that there is a need to assess the supplier's ability to meet the requirements of the contract. For example, a DLA contracting official described an instance in which a supplier new to DLA was awarded a contract based on a low price and a performance score of 100 percent. However, the score was misleading as the supplier had no past performance to measure. Ultimately, the supplier was unable to meet the requirements of the contract. Further, DOD parts can be purchased through the use of automated systems that have limited

[12]Federal Acquisition Regulations, Part 9.103.

visibility on suppliers and can increase the risk of purchasing counterfeit parts. To address the risks of using automated source selection, DLA has a pilot project to create a list of qualified distributors for the supply of two electronic items—semiconductors and microcircuits. Of the 53 distributors that applied, 13 were selected based on their qualifications. DLA plans to review other parts to determine if the pilot can be expanded. In addition, DOD has a number of weapons systems that have remained in service longer than expected—such as the B-52 bomber—and require parts that are no longer available from the original manufacturer or its authorized distributors. When parts are needed for these systems, they are often provided by brokers or independent distributors. As buying from these sources reduces DOD's visibility into a part's pedigree, additional steps are required in assuring that the part is reliable or authentic.

Detecting Part Deficiencies: DOD can have a part's quality and authenticity tested through destructive and nondestructive methods prior to awarding a contract. However, several DOD officials told us that staff responsible for assembling and repairing systems and equipment may not have the expertise to identify suspect counterfeit parts outside of those that demonstrate performance failures because they are not trained to identify counterfeit parts and have limited awareness of the issue. In addition, DOD contracting officials told us that the cost and time associated with testing may be prohibitive, especially for lower-cost parts such as a 50-cent fastener. Other factors were cited by DOD officials at several testing centers as limitations such as the barriers to testing parts that are only available in limited quantities or are expensive. For instance, the F-15 program was in need of two spare parts, but only two of these parts were available in the supply chain, so the preferred destructive testing could not be performed.

Reporting and disposal: Generally, DOD has processes in place for reporting and disposal of deficient parts. Reporting of a deficient part that is suspected to be counterfeit enables further investigation to confirm that a part is counterfeit. As described above, DOD uses JDRS and PDREP to report deficient parts, but does not have a specific field in these databases to report counterfeit parts. Some DOD officials stated that they report suspect counterfeits to internal fraud teams, others indicated that they would contact local law enforcement or the Federal Bureau of Investigation in similar cases. DOD officials told us that when they found counterfeit parts they have shared this information through informal methods such as e-mails or phone calls. Others, such as MDA, use formal methods to convey this information such as bulletins that alert MDA staff of counterfeiting techniques and how to detect them as well as advisories

on confirmed counterfeit parts found in MDA programs. MDA officials stated that these methods are an effective way to immediately alert their staff of counterfeit parts.

Further, depending on the condition of a noncounterfeit, deficient part and its related demilitarization code, it can be refurbished, resold, or destroyed. The disposal of counterfeit and scrapped parts is an area of vulnerability as they could reenter the supply chain. According to officials from the Defense Reutilization and Marketing Service—the agency responsible for destroying and disposing of DOD's excess and surplus parts—it is critical that a part and its related demilitarization code be identified as counterfeit when it is sent for disposal to prevent it from reentering DOD's supply chain. However, DOD does not have a consistent method to identify parts as counterfeit when they are sent for disposal. Some parts designated for disposal have made their way back into the supply chain. For example, DOD program officials described a helicopter part that had the same serial number as a defective one that had been destroyed. An X-ray test revealed the destroyed part had been welded back together and put back in DOD's inventory.

Some DOD Components and Contractors Have Taken Initial Steps to Address Counterfeit Parts

In the absence of a departmentwide policy, some DOD components and their contractors have supplemented existing procurement and quality-control practices to help mitigate the risk of counterfeit parts in the DOD supply chain. For example, MDA has established a 12-person organization that leverages subject-matter expertise at two DOD laboratories to identify, evaluate, and track the effects of counterfeit parts on all MDA hardware. MDA policies to address counterfeits are part of its Parts, Materials, and Processes Mission Assurance Plan which includes instructions on part selection, procurement, receipt, testing, and use of parts. This plan specifically identifies three steps to offset the presence of counterfeit parts and materials in the market: (1) preventing counterfeit parts and materials by using only authorized distributors, with associated certifying paperwork; (2) detecting and containing counterfeit parts and materials through appropriate inspection and test methods; and (3) notifying the user community of potential counterfeit concerns and assisting in prosecution. The plan also instructs programs to impound suspect counterfeit parts and all items from the same lot and to not return suspected counterfeit parts to suppliers, preventing them from being sold to others. According to MDA officials, all new contracts include adherence to the plan's section on counterfeit parts and materials, and MDA has developed policies that can be applied to existing contracts. MDA further has applied DOD's item-unique identification technology that provides for

the marking of individual items—whose unit acquisition cost is $5,000 or more—with a set of globally unique data elements. This technology is designed to help DOD value and track items throughout their life cycle by requiring equipment manufacturers to assign unique identification numbers to parts acquired under DOD contracts, thus enabling better traceability of a part to a specific manufacturer. MDA also has an ongoing effort to develop tools to identify, quantify, and manage the risk of counterfeit parts in the supply chain as counterfeits or suspect counterfeits are detected. DLA's Supply Center in Columbus, Ohio, has an established team that investigates suspect counterfeit parts under the broader scope of fraud. The team is composed of members from DLA's product verification, contracting, and legal offices as well as the Defense Criminal Investigative Service and handles cases ranging from part deficiencies to contractor misconduct. When encountering a counterfeit part, the team's analysis of engineering investigations, product testing, and criminal investigations can be used as evidence in criminal and civil cases.

DOD's prime contractors are also independently taking steps to protect the supply chain from counterfeits. As DOD relies on its suppliers to provide weapons, equipment, and raw materials to meet U.S. national security objectives, these activities directly affect DOD's own efforts. Several prime contractors told us that they are using a recently adopted industry standard to develop counterfeit protection plans.[13] The standard provides strategies to mitigate the risks of procuring counterfeit products and standardizes practices to maximize availability of authentic parts and procure parts from reliable sources. Additionally, it standardizes practices to assure the authenticity of parts, control parts that are identified as counterfeit, and report counterfeit parts to other potential users and government investigative authorities. Prime contractors using this standard are also focusing on ensuring traceability within their supply chains through flow-down requirements to subcontractors. For example, one contractor includes a clause in its contracts that states that its suppliers shall ensure that they do not deliver counterfeits but if this occurs, the supplier would immediately notify the defense contractor and assume responsibility for the cost of replacing the counterfeit parts. Several of the companies also provide training on detecting counterfeits within their product lines.

[13]In April 2009, SAE International issued Aerospace Standard 5553, "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition."

A Number of Commercial Initiatives Exist to Mitigate the Risk of Counterfeit Parts in Supply Chains

Companies Have Developed Anticounterfeiting Practices to Address Vulnerabilities to Counterfeit Parts

As supply chains across industries are also vulnerable to the risk of counterfeit parts, we met with selected companies representing commercial aerospace, electronics, and automotive sectors that have taken measures to address the counterfeiting challenges they face. Companies we met with cited procedures and practices that they have incorporated to help mitigate the risk of counterfeit parts in the areas of supplier visibility, detection, and reporting and disposal.

Supplier Visibility: To ensure that parts and materials are reliable, commercial companies we met with described several practices to identify potential sources of counterfeiting activity. These practices include regular assessments of a supplier's internal controls ranging from their access to product designs to manufacturing facility security. Some practices also included instituting extra measures when purchasing from independent distributors such as internal and external validation and testing requirements, and part-authenticity documentation—such as certificates of conformance.

Detection of Counterfeits: Companies we spoke with are using a number of practices to make their products and packaging more difficult to replicate and to increase the opportunities to identify counterfeits in their supply chains. Some companies incorporate rare, proprietary, or expensive materials on parts and packaging, which can deter counterfeiters. Some companies also include markings on products and packaging that, when absent or altered, could alert investigators or consumers to potential counterfeits. One company allows customers to report suspected counterfeits on its Web site and posts pictures of markings and security features for customers and investigators to use in distinguishing genuine from counterfeit products. Companies have also coordinated with the Department of Homeland Security's Customs and Border Protection inspectors to identify counterfeits. One company visited inspectors at two ports that receive a high volume of imports for this

company, to inform inspectors of product packaging characteristics and how to easily identify counterfeit packaging. This effort resulted in an increased number of seizures of suspected counterfeit products at these two ports.

Reporting and Disposal of Counterfeits: Several company officials identified the lack of oversight of the scrapping, recycling, and disposal of parts as an avoidable source of counterfeiting. Specific practices that companies use to confirm that scrapped, excess, and suspected counterfeit materials are not used to make more counterfeit parts include

- requiring suspect counterfeits to be quarantined upon detection,
- auditing suppliers to ensure proper tracking of the amount of scrapped material destroyed,
- requiring suppliers to use contract clauses that prevent the resale of scrap parts to third parties, and
- witnessing the destruction of seized or returned counterfeit parts.

Industry Associations Identify and Share Anticounterfeiting Practices

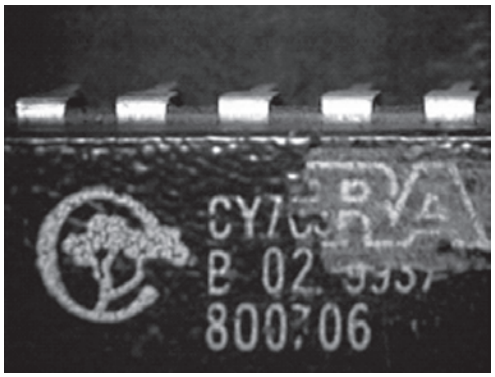
Several industry associations identify and share counterfeit-mitigation practices. Activities include training, knowledge exchange, and developing standards. These associations can provide a forum for a diverse set of participants to arrive at agreement on collaborative mitigation steps for the counterfeit issue. The recently issued Department of Commerce report on the existence of counterfeit electronics across the industry has also recommended mitigation strategies for counterfeit parts.

In April 2009, SAE International issued Aerospace Standard 5553, "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition." The standard was created to provide uniform requirements, practices, and methods to mitigate the risks of receiving and installing counterfeit electronic parts.[14] It also provides guidance for establishing a counterfeit-control plan to include parts availability, purchasing process, product verification, investigation, reporting, and disposal. SAE International is providing training on applying this standard, including a segment on detection and visual inspection of actual counterfeit parts. For example, in its visual inspection segment, the SAE training notes that characteristics of a part that may indicate it is counterfeit include inconsistencies in the part's texture, colors, material, or condition; quality

[14]SAE International officials told us that they plan to expand the aerospace standard to include other sectors such as the automotive industry.

of ink or laser markings; condition of part labels; and markings that include information such as production dates and manufacturing locations. As shown in figure 1, visual inspection of a part's texture can uncover counterfeits that have been resurfaced.

Figure 1: Visual Detection of a Counterfeit Integrated Circuit



- Shiny, smooth, but orange peel—type finish was not natural looking
- Scraping the thick-looking black top exposed another logo under the marking

Source: SAE International and the Jet Propulsion Laboratory.

Note: Information is from SAE 5553 Training Manual dated November 2009.

In 2009, a number of conferences were held to facilitate a collaborative dialogue between industry representatives, law enforcement, and government agencies. Specifically, in September, DOD's Defense Standardization Program Office sponsored its annual Diminishing Manufacturing Sources and Material Shortages and Standardization Conference where participants discussed the counterfeit part issue and how to increase awareness across industries. Additionally, in December, the Center for Advanced Life Cycle Engineering hosted its third annual symposium on avoiding, detecting, and preventing counterfeit electronic parts.[15] Sessions at the symposium were aimed at generating awareness of the counterfeit parts issue and sharing the perspectives of law enforcement, supply chain managers, and government. The symposium also provided information on technical tools and methods to detect and prevent counterfeit parts.

[15]The Center for Advanced Life Cycle Engineering is an electronic products and systems research center focused on electronics reliability and is dedicated to providing a knowledge and resource base to support the development of competitive electronic components, products, and systems.

In late 2008, the Aerospace Industries Association established an integrated project team across aerospace, space, and defense products to address challenges in the supply chain for mitigating the risk of counterfeit parts. The team worked with government agencies, original manufacturers, industry associations, and independent distributors across three main objectives to: (1) discuss U.S. government acquisition and procurement policies to avoid introducing counterfeit parts and materials into products; (2) create a set of recommendations for government and industry to ensure that the risk of introducing counterfeit parts and materials is minimized, is consistent with risks accepted by the customer, and implementable without sacrificing the benefits of buying commercially available products; and (3) engage the U.S. government in discussions concerning enforcement of policies to avoid the introduction of counterfeit products into the United States. The project team has provided its recommendations to its association members and expects final recommendations to be available in the fall of 2010.

The Semiconductor Industry Association established an Anti-Counterfeiting Task Force in June 2006, which aims to stop counterfeit semiconductors from entering the marketplace. According to the task force Chairman, its work with U.S. Customs and Border Protection led to the seizure of 1.6 million counterfeit semiconductors over the past 2 years.

Other industry associations are also focusing their efforts on mitigating the risk of counterfeit parts. Business Action to Stop Counterfeiting and Piracy has developed a clearinghouse for information about counterfeiting and piracy to facilitate information exchange.[16] The Electronic Industry Citizenship Coalition developed a risk-assessment tool for technology-industry companies to help determine the appropriate level of intensity of supplier audits and also asks suppliers about how they manage their subtier suppliers.[17] The International Anti-Counterfeiting Coalition has helped the auto industry bring 10 global manufacturers together to discuss

[16]The International Chamber of Commerce established the Business Action to Stop Counterfeiting and Piracy to take a leading role in the fight against counterfeiting.

[17]The Electronic Industry Citizenship Coalition mission is to promote an industry code of conduct for global electronics supply chains.

common global counterfeiting problems, and also provides opportunities to its members to participate in training programs.[18]

The recent Department of Commerce report provided practices for managing electronic counterfeits industrywide, as well as recommendations for the U.S. government to mitigate the risk of electronic counterfeit parts. The practices for managing counterfeits included (1) provide clear, written guidance to employees on what steps to take if they suspect a part is counterfeit, (2) remove and quarantine suspected and confirmed parts from regular inventory, (3) maintain an internal database to track all suspected and confirmed counterfeit components, and (4) report suspected and confirmed counterfeit parts to industry associations and databases and to law enforcement. The department's report also stated that there is little information collected on malfunctioning and nonoperational electronic parts, which gives a false impression of supply-chain security. According to the report's findings, personnel that use parts need to file Product Quality Deficiency Reports in a timely manner to report nonworking electronic components, and if this proves to be impractical for the field units, then another system of reporting needs to be developed to facilitate information sharing. Based on its survey responses, interviews, and field visits, the Department of Commerce made seven recommendations in the areas of reporting, contract award, legal guidance, enforcement activities, data collection, information sharing, and DOD acquisition planning.

Conclusions

As DOD draws from a large network of suppliers in an increasingly global supply chain, there can be limited visibility into these sources and greater risk of procuring counterfeit parts, which have the potential to threaten the reliability of DOD's weapon systems and the success of its missions. DOD needs a departmentwide definition and consistently used means for detecting, reporting, and disposing of counterfeit parts. Collaboration with government agencies, industry associations, and commercial-sector companies that produce items similar to those used by DOD and have reported taking actions to mitigate the risks of counterfeit parts in their supply chains offers DOD the opportunity to leverage ongoing and planned initiatives in this area. Some of these initiatives, such as MDA practices

[18]The International Anti-Counterfeiting Coalition aims to promote enforcement standards of the intellectual property owned by its members whether copyrights, trademarks, or patents.

and industry detection and disposal processes, can be considered for DOD's immediate use. However, as DOD collects data and acquires knowledge about the nature and extent of counterfeit parts in its supply chain, additional actions may be needed to help better focus its risk-mitigation strategies.

Recommendations for Executive Action

We recommend that the Secretary of Defense take the following three actions as DOD develops its anticounterfeit program:

1. leverage existing anticounterfeiting initiatives and practices currently used by DOD components and industry to establish guidance that includes a consistent and clear definition of counterfeit parts and consistent practices for preventing, detecting, reporting, and disposing of counterfeit parts;
2. disseminate this guidance to all DOD components and defense contractors; and
3. analyze the knowledge and data collected to best target and refine counterfeit-part risk-mitigation strategies.

Agency Comments and Our Evaluation

In written comments on a draft of this report, DOD concurred with the recommendations and identified a number of actions that it will take to address them. DOD noted that it has established teams that will leverage anticounterfeit initiatives and practices used by DOD components and industry to develop guidance by late 2010. DOD plans to include a consistent and clear definition of counterfeit parts and consistent practices for preventing, detecting, reporting, and disposing of counterfeit parts in its guidance, and plans to disseminate it to all of its components and defense contractors by early 2011. As it collects more knowledge and data on counterfeit parts, DOD plans to analyze this to best target and refine risk-mitigation strategies—which it expects to do by October 2010. According to the official leading DOD's counterfeit parts efforts, DOD will continue to refine risk-mitigation strategies on an ongoing basis as it gains more knowledge on counterfeit parts. DOD also provided technical comments, which were incorporated as appropriate. DOD's comments are reprinted in appendix III. The Department of Commerce concurred with the findings in this report. The Department of Commerce's comments are reprinted in appendix IV.

As arranged with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. At that time, we will send copies of this report to appropriate congressional committees; the Secretary of Defense; the Secretaries of the Army, Navy, and Air Force; the Secretary of Commerce; the Administrator of the Office of Federal Procurement Policy; as well as other interested parties. In addition, the report will be made available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions concerning this report, please contact me at (202) 512-4906. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix V.

Belva Martin
Acting Director
Acquisition and Sourcing Management

Appendix I: Scope and Methodology

To examine the extent of the Department of Defense's (DOD) knowledge of counterfeit parts that have entered its supply chain,[1] we reviewed regulations, guidelines, and databases to determine whether they addressed how DOD should define and collect data on counterfeit parts. We met with officials from the DOD Acquisition and Technology, Logistics and Material Readiness, Supply Chain Integration office; the DOD Defense Logistics Agency and its Supply Centers located in Columbus, Ohio; Philadelphia, Pennsylvania; and Richmond, Virginia; the Army, Navy, Air Force, and Missile Defense Agency; and five defense prime contractors—BAE, Boeing, Lockheed Martin, Northrop Grumman, and Raytheon—to discuss (1) their definition of the term counterfeit,(2) their procedures and practices for obtaining knowledge of counterfeit parts, (3) databases available for documenting instances of counterfeit or suspect counterfeit parts, (4) their knowledge of the existence of counterfeit parts, and (5) instances of counterfeit parts within the DOD supply chain.

We also met with database managers from the Joint Deficiency Reporting System (JDRS), the Product Data Reporting and Evaluation Program (PDREP), and the Government Industry Data Exchange Program (GIDEP) to discuss whether these databases are able to and have been used to document instances of counterfeit or suspected counterfeit parts. Additionally, we met with officials from the Department of Commerce, Bureau of Industry and Security's Office of Technology Evaluation, to discuss their study of counterfeit electronics, which the office performed for the Navy, through the office's authority to conduct surveys and analyses and prepare reports on specific sectors of the U.S. defense supplier base.

To further examine the processes that DOD has in place to detect and prevent counterfeit parts from entering its supply chain, we conducted a case study of DOD weapon programs and interviewed program officials as well as several logistics support providers. We selected a nongeneralizable sample of 16 DOD weapon programs based on criteria including representation of the aerospace, ground vehicle, or missile defense sectors; representation of the production and deployment or operations and support phase of the acquisition life cycle, and cross-representation of DOD components—Army, Navy, Air Force, and the Missile Defense

[1]Our review focused on DOD's knowledge of the aerospace, ground vehicle, and missile defense sectors of the defense supplier base in part given congressional interest in these sectors.

Agency. GAO also has ongoing work through its annual "Assessments of Selected Weapon Programs"[2] for many of these programs, which allowed the team to build upon our prior work efforts and existing DOD contacts. Programs selected were: F-15 Eagle, F-16 Fighting Falcon, F/A-18E/F Super Hornet, F/A-22 Raptor, C-5 Galaxy, C-130 Hercules, AH-64D Apache, UH-60 Black Hawk, E-2 Hawkeye, AV-8B Harrier, SH-60 Sea Hawk, V-22 Osprey, Aegis Cruiser, Ground-Based Midcourse Defense, High Mobility Multi-purpose Wheeled Vehicles (HMMWV), and M1 Abrams.

We identified initiatives and practices used by industry associations and commercial companies in selected commercial supply chains (electronics, automotive, aviation) to mitigate the risk of procuring counterfeit parts. We selected commercial supply chains and companies in those supply chains based on one or more of several criteria: industries in which instances of counterfeiting have taken place; companies that make products similar to DOD weapons systems in terms of complexity; and companies that make or buy products similar to those bought by DOD. We met with company officials from functions including Quality, Legal, Security, Brand Protection, and Sourcing and Supplier Management, to discuss their experiences with counterfeits (both incoming parts and counterfeit versions of their products) and processes in place to protect against counterfeits. Much of the information we obtained from these companies is anecdotal, due to the proprietary nature of the data that could affect the companies' competitive standing or level of protection against counterfeits. We visited or spoke with company officials at companies and locations including Advanced Micro Devices, Sunnyvale, California; Boeing Commercial Airplanes, Everett, Washington; Cisco Systems, Inc., San Jose, California; Federal-Mogul Corporation, Southfield, Michigan; Ford Motor Company, Dearborn, Michigan; Hewlett-Packard Company, Houston, Texas; Intel Corporation, Santa Clara, California; Meggitt Aircraft Braking Systems, Akron, Ohio; Microsoft Corporation, Redmond, Washington; and Rolls-Royce Corporation, Indianapolis, Indiana. We also met with or obtained documents from several industry associations, including the Aerospace Industries Association, Semiconductor Industry Association, Business Action to Stop Counterfeiting and Piracy, Electronic Industry Citizenship Coalition, and International Anti-Counterfeiting Coalition. We attended two counterfeit-mitigation conferences—one sponsored by DOD's Defense

[2]GAO, *Defense Acquisitions: Assessments of Selected Weapon Programs*, GAO-09-326SP (Washington, D.C.: Mar. 30, 2009).

Standardization Program Office and the other sponsored by the Center for Advanced Life Cycle Engineering—and attended an SAE International training workshop on Aerospace Standard AS5553.

We conducted this performance audit from January 2009 to March 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Examples of Counterfeit Parts in DOD's Supply Chain

As shown in table 2, Department of Defense (DOD) officials that we met with provided examples of counterfeit parts. As definitions of "counterfeit" vary within DOD, the examples are based on the individual's understanding of the term; however, the examples generally refer to instances in which individuals or companies knowingly misrepresent the identity or pedigree of a part. While many of the examples are confirmed cases of counterfeit, some include cases that were not yet confirmed as the case was under investigation or the DOD official did not know the outcome.

Table 2: Examples of Confirmed or Suspected Counterfeits in DOD's Supply Chain

Part	Description
	Confirmed Counterfeit
Electronics (confirmed)	
GPS receiver frequency standard oscillators	The Air Force and Navy use these oscillators on over 4,000 systems, including the Joint Surveillance Target Attack Radar System (Joint STARS). On the Joint STARS, deficient receivers could cause mission failure. An approved DOD supplier purchased the oscillators from a distributor who had used an unapproved source of supply and the problem was detected when the part had a high failure rate during depot repair. After detection, the contractor removed parts from the depot parts bin, but could not account for five parts. Officials reported that the unaccounted-for five parts may never be found.
Dual transistor	Multiple services commonly use this part to provide power in a system used to defeat shoulder-launched missiles. A supplier purchased the transistors from a nonfranchised distributor and detected the problem—counterfeit chips in the transistors—during routine acceptance testing and failure analysis. After detection, the supplier realized that 16 components had been shipped against the contract. The supplier paid for these 16 components to be replaced and retested.
Microprocessor and nonvolatile random access memory	The Air Force uses these components in the F-15 Flight Control Computer, but F-15 officials stated that the parts are in diminishing supply and difficult to procure. The microprocessors were procured from a broker, and F-15 technicians detected the problem—a falsely identified manufacturer in both cases—during repairs when they noticed additional markings on the microprocessor and character spacing inconsistent with the original part. Air Force officials stated that the parts were isolated and never released to the fleet or into supply.
Radar components	One of the Navy's suppliers discovered counterfeit radar components in its supply chain and worked with the Navy Criminal Investigative Service on the matter.
Electronic components	These components are used across services in the V-22 Osprey. Suppliers procured the parts—including fuel management units and dual digital map systems—and the problems were detected in a supply test house.
Microcircuit component	This microcircuit, no longer produced by the original manufacturer, is used by the Navy across a variety of platforms, including ships, airplanes, and submarines. After the Navy and its contractor purchased 75 of the microcircuits from a supplier, the Navy found that they were wired with the wrong material. Upon discovery, the parts were segregated and did not enter the supply stream.
Counterfeit network hardware	This hardware was purchased by multiple services and contractors and had fake labeling. Federal investigators identified nearly 3,500 counterfeit network components.

Part	Description
Operational amplifiers	The Missile Defense Agency (MDA) acquired the parts from a subcontractor who used an unauthorized distributor. MDA discovered the problem with the amplifiers while testing a circuit board.
Frequency synthesizer	MDA acquired a part that the supplier had acquired from an unauthorized distributor. MDA detected the problem—the surface was resurfaced and remarked—through visual inspections and authenticity testing. Investigations confirmed that a third party had tampered with the part.
Electronic piece parts	MDA acquired counterfeit parts used in booster and flight termination systems and detected the problem during related investigations and, in some cases, testing.
Fasteners (confirmed)	
Self-locking nuts	Self-locking nuts, used in aviation braking, were cracking. They were purchased from an unauthorized source.
Metals (confirmed)	
Titanium aerospace parts	Multiple services and government agencies purchased titanium for use on platforms that included F-15 engine mounts and F-22 and C-17 parts. The titanium was substandard and, if it had failed, could have caused casualties and property loss. The supplier has been charged with selling substandard titanium and repeatedly issuing fraudulent certifications stating that the titanium passed testing standards.
Aluminum parts	A supplier provided parts that it misrepresented as containing the aluminum bronze alloy required by DOD, but the parts were made from a lesser-grade of aluminum. Investigators raided the company's facility, which was located in a barn.
Aluminum parts	Eighteen DOD and National Aeronautics and Space Administration programs and 14 commercial programs procured aluminum for use in items including helicopters, guns, and automobile wheels. Although the parts passed initial inspections, it was determined that the aluminum supplier had falsely reported that it had provided the correct treatments. The failure to properly heat treat the aluminum made it susceptible to corrosion.
Packaging and labeling (confirmed)	
Assorted small parts	The Defense Logistics Agency (DLA) purchased assorted parts, such as washers and circuits, for use on a variety of platforms. The supplier was substituting the requested military-grade items with commercial items by providing correctly-labeled packages but putting the wrong parts inside.
Other hardware (confirmed)	
Brake shoes	This brake shoe is used on medium tactical trailers—the largest tactical trailers used by the military. The shoe was no longer produced by the original manufacturer, so a contract was awarded to a new company. These brake shoes were made with various materials, including seaweed. U.S. customs agents had already seized the brake shoes and DOD never took ownership of them.
Body armor	DLA procured non-Kevlar material that was misrepresented as Kevlar and discovered the discrepancy during testing.
Additional Cases Reported	
Electronics	
High-voltage diodes	An Air Force official was familiar with a case in which a U.S. company purchased diodes from China, rubbed off the part number, and sold the diodes to DOD. The official reported that the Department of Justice had successfully prosecuted the company involved.
Fasteners	

Part	Description
Rotor retaining nut (used to hold the rotor to the mast of some helicopters)	The rotor retaining nut is used to hold the rotor to the mast of some helicopters; its failure would cause the helicopter to crash. The Air Force reported that a supplier willfully supplied a substandard rotor retaining nut, but the supplier maintained its innocence and claimed that it was unaware that the part it procured was a counterfeit part.
Bolt	The Army reported that a bolt, intended for use in helicopters, was counterfeit. The problem was detected when Army officials recognized the serial number on the part and identified it as a defective part that had been cut in half for destruction. An X-ray test confirmed the bolt had been welded back together.
Hook point bolts	DLA procured this part, which is used to help stop aircraft when they land on aircraft carriers. Failure of the part could result in loss of life or aircraft. A supplier rubbed serial numbers off hooks that were too thin to use, welded additional material onto the hooks, and reused them. This problem was detected when premature part failure triggered an investigation and the welded material showed up in X-rays.
Packaging and labeling	
Hermetically-sealed microwave boxes	The Air Force reported that a contractor, who bid to repair parts, was sending them to Russia for repairs and that the resulting repairs were not done accurately. Part failure could have posed a risk to the program.
Other hardware	
Air conditioning component	Army personnel using the Bradley during operations detected a component that they suspected was counterfeit. In some climates, such as Iraq, air conditioning failure would make this vehicle inoperable and, therefore, compromise missions. Army officials were uncertain whether there was an investigation in this case.
Seatbelts	Army officials reported that seatbelts, provided by a supplier, were made from a cheap aluminum and were falsely certified to be the correct aluminum. The deficiency was discovered when a seatbelt part was accidentally dropped and broke. After investigation, Army investigators banned the company from selling to the Army.

Source: GAO summary of examples provided by DOD officials.

Appendix III: Comments from the Department of Defense

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
3500 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

LOGISTICS AND
MATERIEL READINESS

MAR 25 2010

Ms. Belva Martin
Acting Director, Acquisition and Sourcing Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. Martin:

This is the Department of Defense (DoD) response to the GAO draft report, GAO-10-389, "DEFENSE SUPPLIER BASE: DoD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts" dated February 24, 2010 (GAO Code 120802). Detailed comments on the report recommendations are enclosed.

The Department concurs with the draft report's recommendation to leverage existing anti-counterfeiting initiatives and practices used by DoD Components and industry to establish guidance that includes a clear and consistent definition of counterfeit parts and consistent practices for preventing, detecting, reporting, and disposal of counterfeit parts. The Department also concurs with the recommendations to disseminate the guidance to its Components and defense contractors as well as analyze the knowledge and data collected to best target and refine counterfeit part risk mitigation strategies.

The Department appreciates the opportunity to comment on the draft report. Technical comments are provided separately. For further questions concerning this report, please contact Mr. Lee Plowden, 703-604-0098 x137, email lee.plowden@osd.mil.

Sincerely,

Alan F. Estevez
Principal Deputy

Enclosure:
As stated

GAO Draft Report Dated February 24, 2010
GAO-10-389 (GAO CODE 120802)

"DEFENSE SUPPLIER BASE: DOD SHOULD LEVERAGE ONGOING INITIATIVES IN DEVELOPING ITS PROGRAM TO MITIGATE RISK OF COUNTERFEIT PARTS"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense leverage existing anti-counterfeit initiatives and practices currently used by DOD components and industry to establish guidance that includes a consistent and clear definition of counterfeit parts and consistent practices for preventing, detecting, reporting, and disposing of counterfeit parts.

DOD RESPONSE: Concur. DOD has organized specific teams to address counterfeit issues in electronic systems and components, as well as, the logistics supply chain. These teams will leverage existing anti-counterfeit initiatives and practices used by its Components and industry to establish guidance that includes a consistent and clear definition of counterfeit parts and consistent practices for preventing, detecting, reporting, and disposing of counterfeit parts. The estimated completion date for establishing sound guidance with a clear and consistent counterfeit parts definition and consistent practices is Dec 2010.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense disseminate this guidance to all DOD components and defense contractors.

DOD RESPONSE: Concur. DOD will disseminate anti-counterfeit guidance to all of its Components and defense contractors that includes a consistent and clear definition of counterfeit parts and consistent practices for preventing, detecting, reporting, and disposing of counterfeit parts. The estimated completion date is Feb 2011.

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense analyze the knowledge and data collected to best target and refine counterfeit-part risk mitigation strategies.

DOD RESPONSE: Concur. DOD will analyze all knowledge and data it collects on counterfeit parts to best target and refine risk mitigation strategies. The estimated completion date is October 2010.

Appendix IV: Comments from the Department of Commerce

UNITED STATES DEPARTMENT OF COMMERCE
Deputy Under Secretary for Industry and Security
Washington, D.C. 20230

March 12, 2010

Mr. John Neumann
Assistant Director, Acquisition and Sourcing Management
Government Accountability Office
441 G St., NW
Washington, DC 20548

Dear Mr. Neumann,

This letter is in response to a request from Belva Martin for comments on the draft report entitled "Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts" (GAO-10-389).

After reviewing the material, Commerce has no concerns with the report and concurs with GAO's findings for executive action. In fact, the recommendations are in line with a more comprehensive report issued by the Department of Commerce's Bureau of Industry and Security in January 2010, "Defense Industrial Base Assessment: Counterfeit Electronics." A copy of the report is enclosed.

If you need further assistance, please contact Mark Crace at (202) 482-8093 or via e-mail at mcrace@bis.doc.gov.

Sincerely,

D. O. Hill

Daniel O. Hill

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Belva Martin, (202) 512-4906 or martinb@gao.gov

Staff Acknowledgments

In addition to the individual named above, key contributors to this report were Anne-Marie Fennell, Director; John Neumann, Assistant Director; Lisa Gardner; Kevin Heinz; Robert Bullock; MacKenzie Cooper; Jonathan Mulcare; Josie Sigl; Sylvia Schatz; and Jean McSween.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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