Tech Talk provides a medium for industry professionals to share ideas about trends, new methods, and cost-saving techniques. Tech Talk articles are not peer-reviewed, but are selected for general interest and timeliness.

Mitigating the Risk of Counterfeit Parts

Reprinted from the *WSTIAC Quarterly*, Volume 10, Number 1, with permission of the Weapons Systems Technology Information Analysis Center (WSTIAC). This article was derived from excerpted portions of a US Government Accountability Office (GAO) report, *Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts*, submitted to Congress in March 2010.

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 the DoD draws from a large network of global suppliers. Based on a congressional request, the Government Accountability Office (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 were 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. GAO recommended that the DoD leverage existing initiatives to establish anti-counterfeiting guidance and disseminate this guidance to all DoD components and defense contractors. The DoD concurred with each of the recommendations.

Key findings

The 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 department-wide definition of the term *counterfeit* or 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 (i.e., those that do not conform to standards) are not designed to track counterfeit parts. A third government-wide 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, the DoD cited instances of counterfeit parts, as shown in Table 1. A recent Department of Commerce study also identified the existence of counterfeit electronic parts within DoD and industry supply chains. The DoD is in the early stages of developing a program to help mitigate the risks of counterfeit parts.

Table 1. Examples of counterfeit parts in the 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.

The 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 the DoD's supply chain. For example, several DoD weapon system program and logistics officials told the GAO 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 anti-counterfeiting 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 the DoD, agency officials have an opportunity to leverage knowledge and ongoing and planned initiatives to help mitigate the risk of counterfeit parts as the DoD develops its anti-counterfeiting strategy.

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. The DoD procures millions of parts through its logistics support providers — Defense Logistics Agency (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 the DoD can come from different types of suppliers, as shown in Table 2.

Table 2. Types of DoD suppliers of parts and components[1]

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.

Counterfeit parts in the DoD's supply chain

Defining counterfeit parts

The DoD lacks a department-wide definition of the term counterfeit. In the absence of a definition, 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, the DoD endorsed an aerospace standard created by SAE International that includes a definition of the term *counterfeit part*.* While this standard is available department-wide, 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 GAO they were using or considering use of the standard, while other DoD officials told GAO 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.

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),† have data fields that enable users primarily to track information on deficient parts, but neither is designed specifi-

* 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.

† 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.

cally to track counterfeit parts. The DoD considers products that do not conform to quality or design specifications to be deficient.[*] 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 GAO that when he searched the JDRS system, he found three out of more than 94,000 entries that discussed counterfeit parts. The GAO 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, the GAO 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.[†] The GAO found that less than 1 percent of the reports in the databases included one of these 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 agencies to use GIDEP to report deficient[‡] parts. However, the GIDEP Deputy Program Manager told the GAO 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 the DoD had previously issued a military standard requiring use of GIDEP, which was canceled during acquisition reform in 1996.[2] DoD logistical support providers and contractors that the GAO 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.[§]
- **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.

[*] 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.

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

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

[§] 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.

Counterfeit parts in the DoD's supply chain

In the absence of data collected on counterfeit parts, the GAO visited military services, Missile Defense Agency (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 the 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:

- 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
- Parts with fake packaging

The GAO met with DoD program officials and logistical support providers across 16 DoD programs and three DLA supply centers and discussed instances of suspected and confirmed counterfeit parts. 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 the 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 two-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.

[*] Kevlar is a registered trademark of the E.I. du Pont de Nemours and Company.

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 two-year period, a supplier and three co-conspirators were alleged to have 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 co-conspirators have been convicted.

The Department of Commerce also identified the existence of counterfeit parts in the DoD's supply chain in a study released in January 2010.[*] [3] 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. 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 counterfeit parts team

In April 2009 the DoD formed a department-wide team (partially in response to media reports that highlighted the existence of counterfeit parts in the DoD supply chain) to collect information and recommend actions to mitigate the risk of counterfeit parts in its supply chain.[4,5] Standing participants include representatives from the 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

[*] In conducting its assessment, the Department of Commerce defined a counterfeit electronic part 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.

agencies.[*] 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 the 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 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.

Limited protection of the supply chain against counterfeit parts

The 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 specifically to address counterfeit parts. Limitations in the areas of obtaining supplier visibility, investigating part deficiencies, and reporting and disposal may reduce the DoD's ability to mitigate risks posed by counterfeit parts.

Obtaining supplier visibility: The 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.[6]

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 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, the 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 the DoD's visibility into a part's pedigree, additional steps are required in assuring that the part is reliable or authentic.

Detecting part deficiencies: The DoD can have a part's quality and authenticity tested through destructive and nondestructive methods prior to awarding a contract. However, several DoD offi-

[*] 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 department-wide handbook.

cials told the GAO 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 the GAO 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, the 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, the 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 the GAO 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 the 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 the DoD's supply chain. However, the 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 the DoD's inventory.

Initial steps to address counterfeit parts

In the absence of a department-wide 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 the 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 the 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.

The DoD's prime contractors are also independently taking steps to protect the supply chain from counterfeits. As the DoD relies on its suppliers to provide weapons, equipment, and raw materials to meet US national security objectives, these activities directly affect the DoD's own efforts. Several prime contractors told the GAO that they are using a recently adopted industry standard to develop counterfeit protection plans.[1] 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.

Industry anti-counterfeiting practices

As supply chains across industries are also vulnerable to the risk of counterfeit parts, the GAO met with selected companies representing commercial aerospace, electronics, and automotive sectors that have taken measures to address the counterfeiting challenges they face. Companies that were 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 that the GAO 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 that the GAO 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 website 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
- Witnessing the destruction of seized or returned counterfeit parts

Industry associations' anti-counterfeiting 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.[*] 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 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.

In 2009, a number of conferences were held to facilitate a collaborative dialogue between industry representatives, law enforcement, and government agencies. Specifically, in September, the 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 Decem-

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

ber, the Center for Advanced Life Cycle Engineering hosted its third annual symposium on avoiding, detecting, and preventing counterfeit electronic parts. 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.

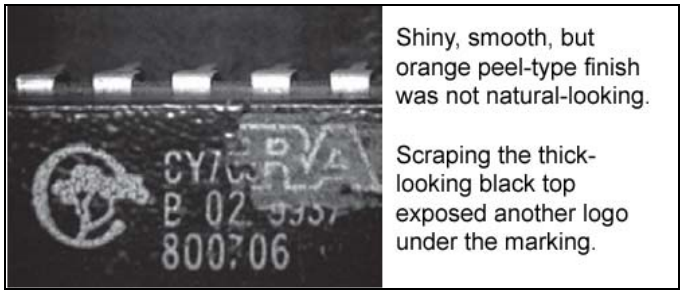

Figure 1. Visual detection of a counterfeit integrated circuit.[7]

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 US 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 US government in discussions concerning enforcement of policies to avoid the introduction of counterfeit products into the US. 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 US 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.[*] 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 sub-tier suppliers. The International Anti-Counterfeiting Coalition has helped the auto industry bring 10 global manufacturers together to discuss common global counterfeiting problems, and also provides opportunities to its members to participate in training programs.

The recent Department of Commerce report provided practices for managing electronic counterfeits industry-wide, as well as recommendations for the US 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) re-

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

move 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 the 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 the DoD's weapon systems and the success of its missions. DoD needs a department-wide 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 the DoD and have reported taking actions to mitigate the risks of counterfeit parts in their supply chains offers the DoD the opportunity to leverage ongoing and planned initiatives in this area. Some of these initiatives, such as MDA practices and industry detection and disposal processes, can be considered for the DoD's immediate use. However, as the 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

The GAO recommends that the Secretary of Defense take the following three actions as the DoD develops its anti-counterfeit program:

1. Leverage existing anti-counterfeiting 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 the DoD components and defense contractors
3. Analyze the knowledge and data collected to best target and refine counterfeit-part risk-mitigation strategies

Agency comments and GAO evaluation

In written comments on a draft of this report, the DoD concurred with the recommendations and identified a number of actions that it will take to address them. The DoD noted that it has established teams that will leverage anti-counterfeit initiatives and practices used by DoD components and industry to develop guidance by late 2010. The 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, the 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 the DoD's counterfeit parts efforts, the DoD will continue to refine risk-mitigation strategies on an ongoing basis as it gains

more knowledge on counterfeit parts. The DoD also provided technical comments, which were incorporated as appropriate.

The DoD's comments can be found with the GAO report *Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts*, http://www.gao.gov/new.items/d10389.pdf. The Department of Commerce concurred with the findings in this report. The Department of Commerce's comments can also be found with the original report.

References

1. SAE International. 2009. *SAE Aerospace Standard 5553: Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition*. Warrendale, Pennsylvania: SAE International.

2. US Department of Defense. *MIL-STD-1556B, Government/Industry Data Exchange Program, Contractor Participation Requirements.* 1986.

3. US Department of Commerce. *Defense Industrial Base Assessment: Counterfeit Electronics*. January 2010.

4. Reed, J. 2008. Fake parts are seeping into military aircraft maintenance depots. *Inside the Air Force*, March.

5. Grow, B., C. Tschang, C. Edwards, and B. Burnsed. 2008. Dangerous fakes: How counterfeit, defective computer components from China are getting into U.S. warplanes and ships. *Business Week*, October 2, 2008.

6. General Services Administration, US Department of Defense, National Aeronautics and Space Administration. *Code of Federal Regulations — Title 48: Federal Acquisition Regulations System*, Subpart 9.103: Responsible prospective contractors. 2005. http://cfr.vlex.com/vid/9-103-policy-19866380

7. SAE International and the Jet Propulsion Laboratory. 2009. *SAE Aerospace Standard 5553 Training Manual*. Warrendale, Pennsylvania: SAE International.

Key contributors to this report included: Belva Martin, Anne-Marie Fennell, John Neumann, Lisa Gardner, Kevin Heinz, Robert Bullock, MacKenzie Cooper, Jonathan Mulcare, Josie Sigl, Sylvia Schatz, and Jean McSween.
