United States Government Accountability Office

GAO

Testimony

Before the Committee on Armed Services, U.S. Senate

For Release on Delivery
Expected at 9:30 a.m. EST
Tuesday, November 8, 2011

DOD SUPPLY CHAIN

Preliminary Observations Indicate That Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms

Statement of Richard J. Hillman, Managing Director
Forensic Audits and Investigative Service

Chairman Levin, Ranking Member McCain, and Members of the Committee:

Thank you for the opportunity to discuss the preliminary observations of our ongoing investigation into the availability of counterfeit military-grade electronic parts on Internet purchasing platforms. 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, affect the integrity of weapon systems, and ultimately endanger the lives of our troops. Almost anything is at risk of being counterfeited, from fasteners used on aircraft to electronics used on missile guidance systems. There can be many sources of counterfeit parts as DOD draws from a large network of global suppliers.[1]

We recently reported that the increase in counterfeit electronic parts is one of several potential barriers DOD faces in addressing parts quality problems.[2] In your request letter, you cited specific questions about the availability of counterfeit parts on Internet platforms commonly used to buy hard-to-find military-grade electronic parts, including those used in weapon systems. My statement today summarizes preliminary observations from our ongoing investigation into the purchase and authenticity testing of selected, military-grade electronic parts that may enter the DOD supply chain. We will issue our final report when our investigation is complete.

In conducting this investigation, we created a fictitious company to gain access to Internet platforms that sell military-grade electronic parts. Our company included a fictitious owner and employees, mailing and e-mail addresses, a website, and a listing on the Central Contractor Registration.[3] We attempted to purchase memberships to three Internet

[1]GAO, *Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts*, GAO-10-389 (Washington, D.C.: Mar. 29, 2010).

[2]GAO, *Space and Missile Defense Acquisitions: Periodic Assessment Needed to Correct Parts Quality Problems in Major Programs,* GAO-11-404 (Washington, D.C.: June 24, 2011).

[3]The Central Contractor Registration is the primary contractor registrant database for the U.S. federal government. The Central Contractor Registration collects, validates, stores, and disseminates data in support of agency acquisition missions.

platforms that were of interest to this committee. We were granted memberships to two platforms but denied by the third. We then requested quotes from vendors on both platforms to purchase a total of 13 parts from a list of parts this committee provided that fell into one of three categories: (1) authentic part numbers for obsolete and rare parts, (2) authentic part numbers with postproduction date codes (date codes after the last date the part was manufactured), and (3) bogus part numbers. We independently verified with the Defense Logistics Agency (DLA) that the authentic part numbers were used for military applications using DLA's Federal Logistics Information System and by interviewing DLA officials.[4] We also confirmed with DLA and selected part manufacturers that the bogus part numbers were not associated with actual parts. We altered all part numbers in this testimony due to the ongoing nature of our investigation. We requested parts from vendors that were new in original packaging, not refurbished, and had no mixed date codes. We selected the first vendor among those offering the lowest prices that provided enough information, such as name, addresses, and payment method, to make a purchase. We attempted to avoid using the same vendor more than once unless no other vendor responded to our request; however, vendors may operate under more than one name. We did not attempt to verify the independence of any vendor before we made our purchases. Finally, we contracted with the SMT Corp. for full component authentication analysis. For details on this analysis, see appendix I. The results of this investigation are based on the use of a nongeneralizable sample, and these results cannot be used to make inferences about the extent that parts are being counterfeited. We began this investigation in August 2011 and are conducting it in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

In summary, as of November 8, 2011, we have purchased 13 parts. None of the 7 parts we have complete results for are authentic. Specifically, according to SMT Corp., all three parts tested after we requested legitimate but rare or obsolete parts failed at least three of seven

[4]DLA's Federal Logistics Information Service via the World Wide Web provides general information about more than 8 million supply items used by the U.S. government and North Atlantic Treaty Organization (NATO) allies.

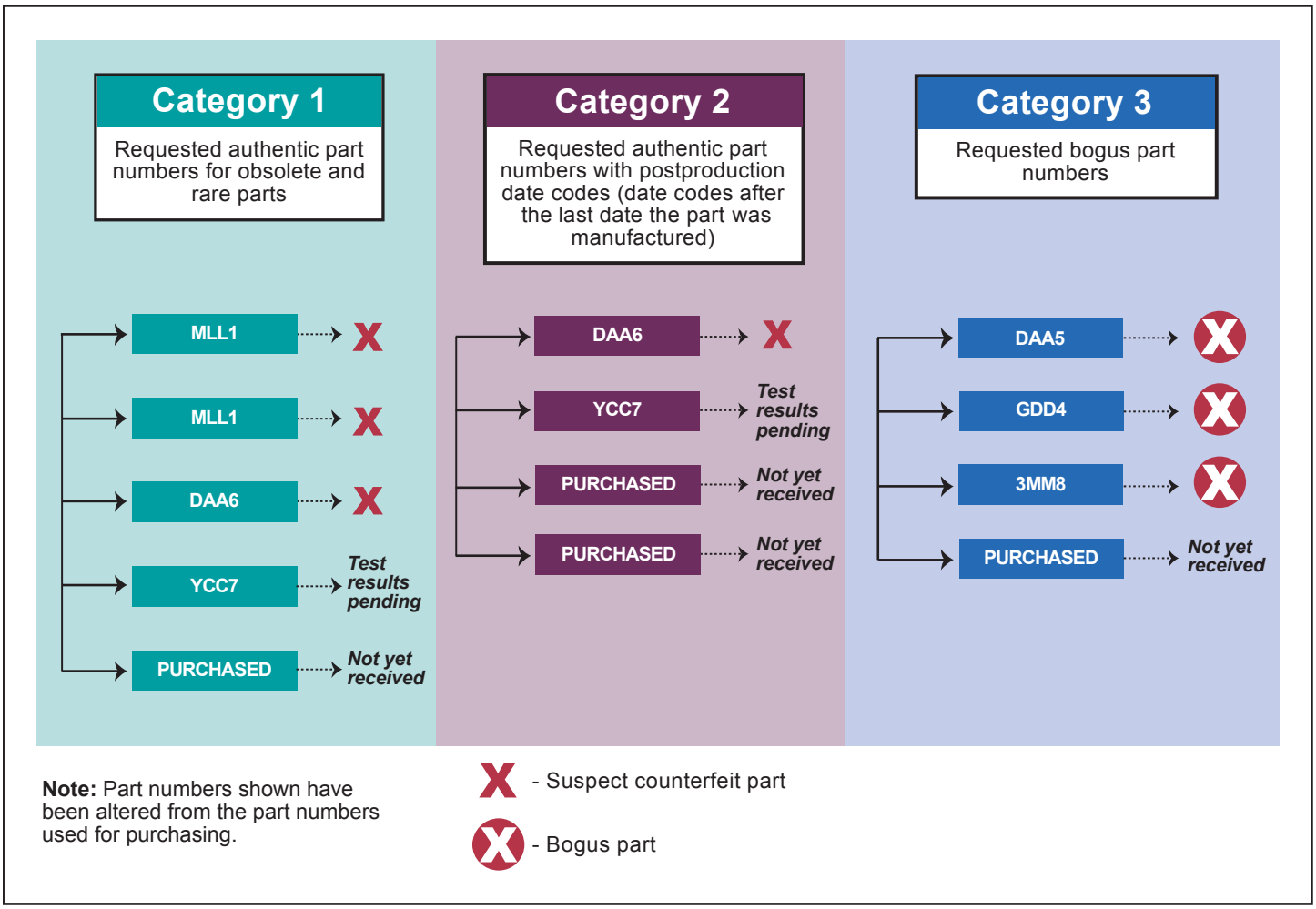
authentication analyses and were "suspect counterfeit."[5] These parts included two voltage regulators and one operational amplifier, the failure of which could pose risks to the functioning of the electronic system where the parts reside. SMT Corp. also made the same determination for the other operational amplifier we received after requesting a legitimate part number with a postproduction date code. In this instance, the part failed four of seven authentication analyses, and the vendor also misrepresented the part as 9 years newer than the date it was last produced. In addition, we received three bogus parts after submitting orders using invalid part numbers. Because no legitimate parts in this final category exist—the part numbers are not in DLA's Federal Logistics Information System and selected manufacturers confirmed they have never been produced—we did not send them for authenticity testing. We are awaiting authentication analysis results for two additional parts, and have not yet received another four purchases. We will report the results for these and additional parts we plan to purchase in a future product. While we sent requests to both domestic and international companies, all of the parts we purchased and received to date were provided by vendors in China. We will issue our final report when our investigation is complete.

[5]According to SMT Corporation, industry standards dictate that the term "counterfeit" cannot be used by an independent test lab; only the product manufacturer can deem a product counterfeit. Therefore, the term "suspect counterfeit" is defined as items that are produced or distributed in violation of intellectual property rights, copyrights, or trademark laws, as well as any items that are deliberately altered in such a way as to misrepresent the actual quality of the item with intent to defraud or deceive the purchaser.

Preliminary Observations Point to Availability of Counterfeit and Nonexistent Parts

Figure 1 shows the preliminary status of the 13 parts we have purchased as of November 8, 2011. The text below details our preliminary findings for each of the three categories of parts.

Figure 1: Preliminary Status of Parts Purchased and Tested

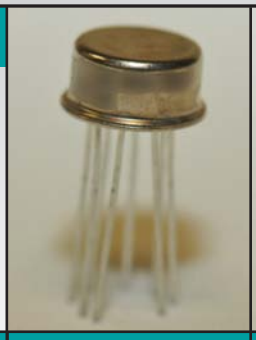
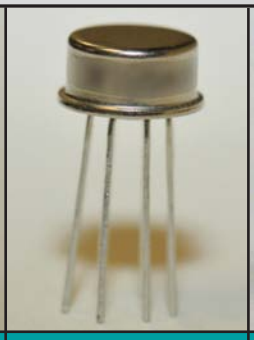
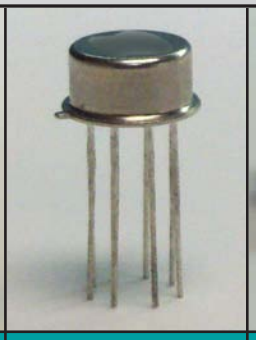
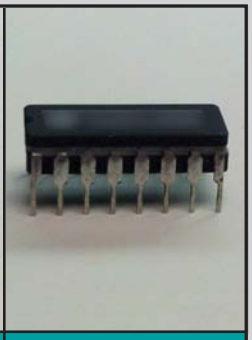


Source: GAO analysis of SMT test results.

Authentic Part Numbers for Obsolete or Rare Parts

All three of the obsolete or rare parts that SMT Corp. tested were suspected counterfeits. The parts were subject to a component authentication analysis, which included visual, chemical, x-ray, and microscopic testing. Figure 2 provides photos and detailed test results for each part. We purchased two additional parts; one is currently being tested by SMT Corp., while we have not yet received the other. All five parts were purchased through the same Internet platform.

Figure 2: Preliminary Authentication Analysis Results of Obsolete or Rare Parts

Category 1 Requested authentic part numbers for obsolete and rare parts				
Analysis performed	**MLL1**	**MLL1**	**DAA6**	**YCC7**
Visual inspection	Fail ✗	Fail ✗	Fail ✗	*Test results pending*
Package configuration and dimensions	Pass ✓	Pass ✓	Pass ✓	*Test results pending*
XRF elemental analysis	Fail ✗	Fail ✗	Fail ✗	*Test results pending*
Real-time x-ray analysis	Pass ✓	Pass ✓	Pass ✓	*Test results pending*
Scanning electron microscopy (SEM) analysis	Pass ✓	Pass ✓	Fail ✗	*Test results pending*
Solderability test	Pass ✓	Pass ✓	Pass ✓	*Test results pending*
Delidding and die microscopy	Fail ✗	Fail ✗	Fail ✗	*Test results pending*
Suspect counterfeit	**Yes**	**Yes**	**Yes**	*Test results pending*

Note: Part numbers shown have been altered from the part numbers used for purchasing.

Source: GAO analysis of SMT test results.

For two of the tested parts, purchased with part number MLL1, evidence lots contained a number of samples that failed three of seven analyses, leading SMT Corp. to conclude that they are suspect counterfeit. Both parts were purchased from different vendors using the same part number,

as pictured in figure 2. An authentic part with this number is a voltage regulator that may be commonly found in military systems such as the Air Force's KC-130 Hercules aircraft, the Navy's F/A-18E Super Hornet fighter plane, the Marine Corps' V-22 Osprey aircraft, and the Navy's SSN-688 Los Angeles Class nuclear-powered attack submarine. If authentic, these parts provide accurate power voltage to segments of the system they serve. Failure can lead to unreliable operation of several components (e.g., integrated circuits) in the system and poses risks to the function of the system where the parts reside.

Visual inspection was performed on all evidence samples for both parts. Different color epoxy seals were noted within both lots according to SMT Corp., which is common in suspect counterfeit devices because many date and lot codes are remarked to create a uniform appearance. Moreover, according to SMT Corp., x-ray fluorescence (XRF) testing of the samples revealed that the leads contain no lead (Pb), which, according to military performance standards defined in section A.3.5.6.3 of the MIL-PRF-38535J DOD Performance Specification for Integrated Circuits (Microcircuits) Manufacturing, should be alloyed with at least 3 percent of lead (Pb).[6],[7] Further, XRF data between the top and bottom of the lead revealed inconsistencies in chemical composition, leading SMT Corp. to conclude that the leads were extended with the intention to deceive. Microscopic inspection revealed that different revision numbers of the die and differences in various die markings were found even though the samples were advertised to be from the same lot and date code.[8] Commonly, components manufactured within the same date and lot code will have the same die revisions. According to SMT Corp.'s report, the manufacturer also stated that "it is very unusual to have two die runs in a common assembly lot. This is suspicious." Finally, the devices found in the first lot tested went into "last time buy" status—an end-of-life designation—on September 4, 2001, meaning that the parts

[6]XRF analyzers quickly and nondestructively determine the elemental composition of materials commonly found in microelectronic devices. Each of the elements present in a sample produces a unique set of characteristic x-rays that reveals the chemistry of the sample in an analogous manner to a fingerprint. A lead is an electrical connection consisting of a length of wire or soldering pad that comes from a device. Leads are used for physical support, to transfer power, to probe circuits, and to transmit information.

[7]Department of Defense, MIL-PRF-38535J (Dec. 28, 2010).

[8]A die is a small wafer of semiconducting material on which a functional circuit is fabricated.

were misrepresented as newer than they actually were. The manufacturer confirmed this status and added that the part marking did not match their marking scheme, meaning that the date code marked on the samples would not be possible.

For the third tested part, purchased as part number DAA6, evidence lots contained many samples that failed four authentication analyses, leading SMT Corp. to conclude that they are suspect counterfeit. An authentic part with this part number is an operational amplifier that may be commonly found in the Army and Air Force's Joint Surveillance and Target Attack Radar System (JSTARS); the Air Force's F-15 Eagle fighter plane; and the Air Force, Navy, and Marine Corps' Maverick AGM-65A missile. If authentic, this part converts input voltages into output voltages that can be hundreds to thousands of times larger. Failure can lead to unreliable operation of several components (e.g., integrated circuits) in the system and poses risks to the function of the system where the parts reside.

Visual inspection for DAA6 found inconsistencies, including different or missing markings and scratches, which suggested that samples were remarked. Scanning electron microscopy analysis revealed further evidence of remarking. Similarly to parts MLL1, XRF testing of the DAA6 samples revealed that the leads contain no lead (Pb) instead of the 3 percent lead (Pb) required by military specifications.[9] Five samples were chosen for delidding because of their side marking inconsistencies. While all five samples had the same die, the die markings were inconsistent. According to SMT Corp., die markings in components manufactured within the same date and lot code should be consistent. Finally, the devices found in the first lot tested went into "last time buy" status in 2001, meaning that the parts were misrepresented as newer than they actually were. The manufacturer confirmed this status and added that the part marking did not match its marking scheme, meaning that the date code marked on the samples would not be possible.

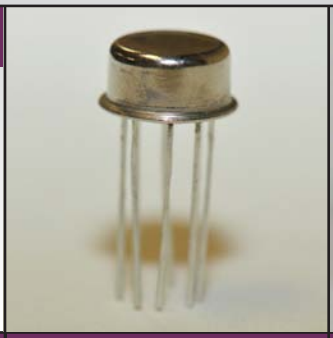
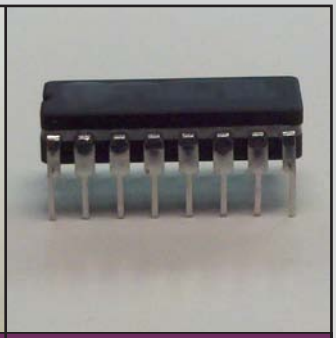
Authentic Part Numbers with Postproduction Date Codes

As of November 8, 2011, the part we received and tested after requesting a legitimate part number but specifying a postproduction date code was also suspected counterfeit, according to SMT Corp. Figure 3 provides a

[9]Department of Defense, MIL-PRF-38535J.

photo and detailed test results. We have purchased three additional parts with postproduction date codes; one is with SMT Corp. for testing, while we have not yet received the other two. By fulfilling our requests, the vendors agreed to provide parts that they represented as several years newer than when they were last manufactured. We verified the last date the parts were produced with the part manufacturers. Nonetheless, the parts will be subject to a full component authentication analysis.

Figure 3: Preliminary Authentication Analysis Results of Part with Invalid Date Codes

Category 2 Requested authentic part numbers with postproduction date codes (date codes after the last date the part was manufactured)		
Analysis performed	**DAA6**	**YCC7**
Visual inspection	**Fail** ✗	*Test results pending*
Package configuration and dimensions	**Pass** ✓	*Test results pending*
XRF elemental analysis	**Fail** ✗	*Test results pending*
Real-time x-ray analysis	**Pass** ✓	*Test results pending*
Scanning electron microscopy (SEM) analysis	**Fail** ✗	*Test results pending*
Solderability test	**Pass** ✓	*Test results pending*
Delidding and die microscopy	**Fail** ✗	*Test results pending*
Suspect counterfeit	**Yes**	*Test results pending*

Note: Part numbers shown have been altered from the part numbers used for purchasing.

Source: GAO analysis of SMT test results.

For the part purchased with part number DAA6, evidence lots contained many samples that failed four of seven analyses, leading SMT Corp. to

conclude that they are suspect counterfeit. This is the same part number used to purchase the DAA6 part tested under category one, which was also suspected counterfeit. However, for this part our order included a postproduction date code in place of a valid one, and the part we received was supplied by a different vendor.

Surfaces on the parts in the evidence lots were found to have scratches similar to suspect counterfeit devices that have been remarked, as confirmed by both visual inspection and scanning electron microscopy analysis. In addition, the quality of exterior markings, including a lack of consistency between the manufacturer's logo, was lower than would be expected for authentic devices. Tooling marks were also found on the bottom of all components within the evidence lot; these marks suggest the components were pulled from a working environment. Further inspection led SMT Corp. to conclude that many samples with refurbished leads were extended with the intention to deceive. Moreover, XRF analysis revealed the leads contain no lead (Pb), which according to military performance standards defined in section A.3.5.6.3 of the MIL-PRF-38535J DOD Performance Specification for Integrated Circuits (Microcircuits) Manufacturing, should be alloyed with at least 3 percent of lead (Pb).[10] Delidding, which exposes parts' die, revealed that the die, while correct for this device, were inconsistent. As previously stated, multiple die runs are considered suspicious. Finally, some of the samples went into "last time buy" status in 2001, despite the fact that we requested 2005 or later and the vendor agreed to provide 2010 or later.

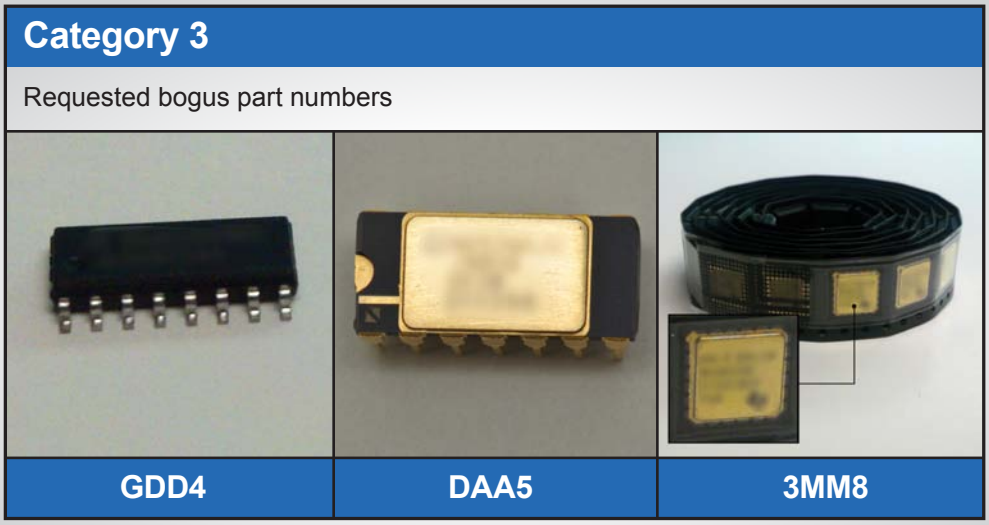
Bogus Part Numbers

As of November 8, 2011, we have received three bogus parts after submitting requests using invalid part numbers. The fact that vendors fulfilled our requests indicates that they were willing to sell parts stamped with nonexistent part numbers—essentially taking money in exchange for bogus parts. According to selected manufacturers, the part numbers we requested and received parts for, GDD4, DAA5, and 3MM8, are not associated with parts that have ever been manufactured. In addition, the parts were not listed in DLA's Federal Logistics Information Service. As such, we did not send the parts to SMT Corp. for authentication analysis. Figure 4 provides photos of the fictitious parts we received. We

[10]Department of Defense, MIL-PRF-38535J.

purchased a fourth part with an invalid part number but have not yet received it.

Figure 4: Photos of Parts Received Despite Requesting Invalid Part Numbers



Note: Part numbers shown have been altered from the part numbers used for purchasing.

Source: GAO.

Chairman Levin, Ranking Member McCain, and Members of the Committee, this concludes my prepared statement. I would be happy to respond to any questions you may have.

Contacts

For additional information about this testimony, please contact Richard J. Hillman at (202) 512-6722 or hillmanr@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

Appendix I: Details of Authentication Analysis Tests

This appendix provides details on each of the tests that constitute the authentication analysis SMT Corp. conducted for the parts we purchased.

Visual Inspection: Visual inspection is performed on a predetermined number of samples (usually 100 percent) to look for legitimate nonconformance issues as well as any red flags commonly found within suspect counterfeit devices.

X-Ray Florescence (XRF) Elemental Analysis: The XRF gathers and measures the elements within a target area. This is used specifically for testing components for RoHS or Hi-Rel conformance, which refer to dangerous substances such as Lead (Pb), Cadmium (Cd), Mercury (Hg) that are commonly used in electronics manufacturing. For suspect counterfeit devices, it helps determine if a component has the correct plating for the specification it supposed to adhere to.

Package Configuration and Dimensions: This test measures key areas of the device to see if they fall within industry specifications.

Real-Time X-Ray Analysis: X-ray analysis is performed on a predetermined number of samples (usually 100 percent). The internal construction of components is inspected (depending on the component package type) for legitimate issues such as broken/taut bond wires, electrostatic discharge damage, broken die, and so forth. For suspect counterfeit devices, the differences in die size/shape, lead frames, bond wire layout, etc. are inspected.

Scanning Electron Microscopy: A scanning electron microscope is used to perform an exterior visual inspection—more in-depth than the previous visual inspection. This is usually performed on a two-piece sample from the evidence lot. Depending on the package type, indications of suspect counterfeit devices are sought, including surface lapping, sandblasting, and sanding with regards to part marking removal.

Solderability: This test is usually for legitimate components to determine if they will solder properly when going to be used in production.

Decapsulation/Delidding and Die Verification: The die of a component is exposed with either corrosive materials or a cutting apparatus. This is done to inspect the die or “brain” of a component to determine its legitimacy. This process is performed on numerous samples to look for differences between samples such as die metallization layout, revisions,

part numbers, and so forth—all of which are red flags for suspect counterfeits.

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 website (www.gao.gov). Each weekday afternoon, GAO posts on its website 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 website, 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.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: 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