DEFENSE INDUSTRIAL BASE ASSESSMENT: COUNTERFEIT ELECTRONICS

PREPARED BY

U.S. DEPARTMENT OF COMMERCE
BUREAU OF INDUSTRY AND SECURITY
OFFICE OF TECHNOLOGY EVALUATION

January 2010

FOR FURTHER INFORMATION ABOUT THIS REPORT, CONTACT:

Mark Crawford, Senior Trade & Industry Analyst, (202) 482-8239
Teresa Telesco, Trade & Industry Analyst, (202) 482-4959
Christopher Nelson, Trade & Industry Analyst, (202) 482-4727
Jason Bolton, Trade & Industry Analyst, (202) 482-5936
Kyle Bagin, Summer Research Intern
Brad Botwin, Director, Industrial Base Studies, (202) 482-4060
Email: bbotwin@bis.doc.gov
Fax: (202) 482-5361

For more information about the Bureau of Industry and Security, please visit:
http://bis.doc.gov/defenseindustrialbaseprograms/

EXECUTIVE SUMMARY

In June 2007, the U.S. Department of the Navy, Naval Air Systems Command (NAVAIR) asked the Bureau of Industry and Security's (BIS) Office of Technology Evaluation (OTE) to conduct a defense industrial base assessment of counterfeit electronics. NAVAIR suspected that an increasing number of counterfeit/defective electronics were infiltrating the DoD supply chain and affecting weapon system reliability. Counterfeits could complicate the Navy's ability to sustain platforms with extended life-cycles and maintain weapon systems in combat operations.

The purpose of this study is to provide statistics on the extent of the infiltration of counterfeits into U.S. defense and industrial supply chains, to provide an understanding of industry and government practices that contribute to the problem, and to identify best practices and recommendations for handling and preventing counterfeit electronics.

OTE surveyed five segments of the U.S. supply chain – original component manufacturers (OCMs), distributors and brokers, circuit board assemblers, prime contractors and subcontractors, and Department of Defense (DOD) agencies. The objectives of the survey were to assess: levels of suspected/confirmed counterfeit parts; types of devices being counterfeited; practices employed in the procurement and management of electronic parts; recordkeeping and reporting practices; techniques used to detect parts; and best practices employed to control the infiltration of counterfeits.

This assessment focused on discrete electronic components, microcircuits, and circuit board products – key elements of electronic systems that support national security, industrial, and commercial missions and operations. A total of 387 companies and organizations, representing all five segments of the supply chain, participated in the study covering the 2005 to 2008 reporting period.

OTE data revealed that 39 percent of companies and organizations participating in the survey encountered counterfeit electronics during the four-year period. Moreover, information collected highlighted an increasing number of counterfeit incidents being detected, rising from 3,868 incidents in 2005 to 9,356 incidents in 2008. These counterfeit incidents included multiple versions of DOD qualified parts and components.

The rise of counterfeit parts in the supply chain is exacerbated by demonstrated weaknesses in inventory management, procurement procedures, recordkeeping, reporting practices, inspection and testing protocols, and communication within and across all industry and government organizations.

Based on survey responses, independent research, and field interviews, OTE developed the following general findings:

- all elements of the supply chain have been directly impacted by counterfeit electronics;
- there is a lack of dialogue between all organizations in the U.S. supply chain;
- companies and organizations assume that others in the supply chain are testing parts;
- lack of traceability in the supply chain is commonplace;
- there is an insufficient chain of accountability within organizations;
- recordkeeping on counterfeit incidents by organizations is very limited;
- most organizations do not know who to contact in the U.S. Government regarding counterfeit parts;
- stricter testing protocols and quality control practices for inventories are required; and
- most DOD organizations do not have policies in place to prevent counterfeit parts from infiltrating their supply chain.

To curtail the flow of counterfeit parts into U.S. defense and industrial supply chains, OTE developed key best practices for organizations dealing with electronic components based on survey respondent recommendations, independent research, and field interviews, including:

- provide clear, written guidance to personnel on part procurement, testing, and inventory management;
- implement procedures for detecting and reporting suspect electronic components;

- purchase parts directly from OCMs and/or their authorized suppliers when possible, or require part traceability when purchasing from independent distributors and brokers;
- establish a list of trusted suppliers – which can include OCMs, authorized suppliers, independent distributors, and brokers – to enable informed procurement and develop an untrusted supplier list to document questionable sources;
- utilize third-party escrow services to hold payment during part testing;
- adopt realistic schedules for procuring electronic components;
- modify contract requirements with suppliers to require improved notices of termination of the manufacture of electronic components and of final life-time part purchase opportunities;
- ensure physical destruction of all defective, damaged, and substandard parts;
- expand use of authentication technologies by part manufacturers and/or their distributors;
- screen and test parts to assure authenticity prior to placing components in inventory, including returns and buy backs;
- strengthen part testing protocols to conform to the latest industry standards;
- verify the integrity of test results provided by contract testing houses;
- perform site audits of supplier parts inventory and quality processes where practical;
- maintain an internal database of suspected and confirmed counterfeit parts; and
- report all suspect and confirmed counterfeit components to federal authorities and industry associations.

In addition, OTE proposes the following recommendations, based on survey responses, interviews, and field visits, which the U.S. Government should institute to inhibit the circulation of counterfeit electronics:

- consider establishing a centralized federal reporting mechanism for collecting information on suspected/confirmed counterfeit parts for use by industry and all federal agencies;

- modify Federal Acquisition Regulations (FAR), including Defense Federal Acquisition Regulations (DFAR), to allow for "best value" procurement, as well as require U.S. Government suppliers and federal agencies to systematically report counterfeit electronic parts to the national federal reporting mechanism;

- issue clear, unambiguous legal guidance to industry and U.S. federal agencies with respect to civil and criminal liabilities, reporting and handling requirements, and points of contact in the Federal Bureau of Investigation regarding suspected/confirmed counterfeit parts;

- establish federal guidance for the destruction, recycling, and/or disposal of electronic systems and parts sold and consumed in the United States;

- establish a dialogue with law enforcement agencies on the potential need to increase prosecution of counterfeiters and those entities knowingly distributing counterfeit electronic parts;

- consider establishing a government data repository of electronic parts information and for disseminating best practices to limit the infiltration of counterfeits into supply chains;

- develop international agreements covering information sharing, supply chain integrity, border inspection of electronic parts shipped to and from their countries, related law enforcement cooperation, and standards for inspecting suspected/confirmed counterfeits; and

- address funding and parts acquisition planning issues within DOD and industries associated with the procurement of obsolete parts.

I. INTRODUCTION

This defense industrial base assessment was initiated by the Bureau of Industry and Security (BIS) to provide statistics on the extent of infiltration of counterfeit electronic components into United States industrial and defense 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. This comprehensive assessment was designed to replace existing anecdotal information within the U.S. Navy and other industry and government organizations with concrete data on the impact and pervasiveness of counterfeit electronics within the U.S. supply chain.

In June 2007, the Naval Air Warfare Systems Command (NAVAIR) requested BIS' Office of Technology Evaluation (OTE) to conduct a defense industrial base assessment of counterfeit electronics. NAVAIR suspected that an increasing number of counterfeit/defective electronics were infiltrating the DoD supply chain and affecting weapon system reliability. Upon further investigation, it was discovered that counterfeit electronics were also affecting industry at large.

Two major challenges facing the Navy and other U.S. military services are the extension of weapon systems and platform lifecycles and the sustainment of those aging systems. Systems such as the F-15, which was put into service in 1975 and is scheduled to be in service well beyond 2010, are used far after their original end-of-life projections. This is as opposed to the projected lifecycles of electronic parts and components produced by industry, which can be as brief as two years. Thus, DOD procurement agents quickly find their multiple sources of needed electronic parts turning into sole sources or disappearing altogether. This problem has been further compounded by extended usage of weapon systems and platforms in Iraq and Afghanistan, which have diminished existing and well intentioned life of type or life time buys and spare parts inventories.

DOD logistics offices in charge of solving obsolescence problems are challenged by limited budgets, procurement issues, and time issues. It is typically less expensive to find part substitutions and aftermarket manufacturing for needed electronic parts than reengineering and redesigning parts and components. Obsolescence mitigation strategies also take a long time to implement. These factors can force procurement agents to purchase parts from unknown sources, which can introduce counterfeit parts into weapon systems.

Obsolete components are not the only parts being counterfeited. This report highlights that there are also counterfeit versions of the newest parts and components currently being manufactured by OCMs. This increases the difficulty that procurement agents in industry and the government face when trying to locate authentic, dependable parts.

METHODOLOGY

BIS/OTE performed this assessment and data collection under authority delegated to the U.S. Department of Commerce under Section 705 of the Defense Production Act of 1950, as amended (50 U.S.C. App. Sec. 2155), and Executive Order 12656. These authorities enable BIS/OTE to conduct mandatory surveys, study defense-related industries and technologies, and monitor economic and trade issues affecting the U.S. defense industrial base. OTE recently completed assessments of the U.S. integrated circuit industry, the U.S. space industry, the U.S. machine tool industry, and the U.S. sensors and imaging industry.

Upon initiation of the assessment, OTE undertook a number of steps over several months to better understand the counterfeiting problem. OTE first held discussions with various industry and government groups taking a leadership role in the counterfeit parts issue, including the Semiconductor Industry Association (SIA), Aerospace Industries Association (AIA), Alliance for Gray Market and Counterfeit Abatement (AGMA), and the Department of Defense (DOD) managed community of government and industry representatives responsible for Diminishing Manufacturing Supplies and Material Shortages (DMSMS) issues. These discussions framed many of the aspects of counterfeit parts and the complexity of the problem.

OTE followed up these discussions with site visits to DOD depots, defense prime contractors, the Government-Industry Data Exchange Program (GIDEP), a circuit board assembler, and an original component manufacturer (OCM), as well as component distributors. The site visits and subsequent discussions informed OTE on procurement and supply chain processes.

Based on this information, OTE decided to focus this assessment on basic electronic parts: discrete electronic components, microcircuits, bare circuit boards, and assembled circuit boards.[1] These parts are key elements of electronic systems that support national security missions and control essential commercial and industrial operations.

OTE also developed a broad definition of the term “counterfeit” to encompass the views of different segments of the supply chain.[2] For this assessment, a counterfeit is an electronic part that is not genuine because it:

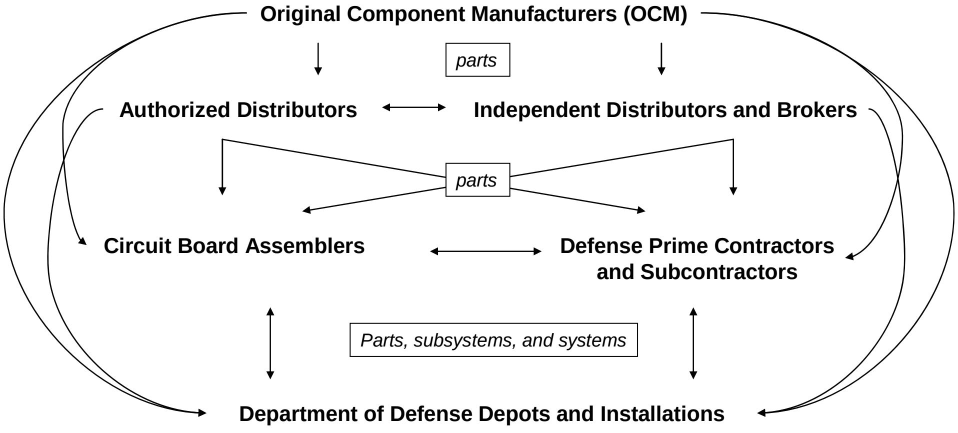
- is an unauthorized copy;
- does not conform to original OCM design, model, and/or performance standards;
- is not produced by the OCM or is produced by unauthorized contractors;
- is an off-specification, defective, or used OCM product sold as "new" or working; or
- has incorrect or false markings and/or documentation.

To capture the movement of electronic parts and the interconnected nature of the supply chain, OTE identified five different sectors that have unique roles within the U.S. electronic part supply chain and overall defense industrial base: OCMs; authorized and independent distributors and brokers; circuit board assemblers; prime contractors and subcontractors; and DOD installations. While every sector of the supply chain sells to each other, there is a basic flow of parts and components between sectors (see Figure I-1).

[1] See the glossary in Appendix A for definitions of these parts.

[2] The definition of counterfeit parts used in the OTE study is specific to this assessment, and is broader than definitions typically used by industry.

Figure I-1: U.S. Defense Electronic Parts Supply Chain


Original Component Manufacturers (OCM)
parts
Authorized Distributors
Independent Distributors and Brokers
parts
Circuit Board Assemblers
Defense Prime Contractors and Subcontractors
Parts, subsystems, and systems
Department of Defense Depots and Installations

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Five separate but related surveys were developed in order to target the specific experiences of each sector and allow analysts to cross-reference answers. OTE designed these surveys, each approximately 80 questions and covering the 2005-2008 period, to determine:

- the scale and scope of counterfeit electronic parts in the U.S. supply chain;
- past problems with counterfeit electronic parts and their impact;
- internal procurement policies and protocols;
- testing, inspection, and inventory management procedures;
- internal and external procedures for handling counterfeit electronic parts once identified;
- authorities contacted upon discovery of a counterfeit electronic part; and
- industry and government best practices for preventing the infiltration and handling of counterfeit electronic parts.[3]

All references to “counterfeits” in this assessment mean suspected/confirmed counterfeits. OTE collected data on this basis because discussions with industry revealed that costs associated with testing to declare suspect parts “counterfeit” or “defective” are too high for some organizations to bear.

[3] Copies of the surveys are available upon request.

OTE field tested the resulting draft surveys for accuracy and usability with a variety of organizations within the five identified sectors. Once comments were received and incorporated into the surveys, the documents were sent to the Office of Management and Budget (OMB) for review and approval as required under the Paperwork Reduction Act (PRA).

After receiving OMB approval, OTE disseminated the surveys to industry and government organizations. Data collected through the surveys was supplemented with information gathered from site visits, discussions with industry and government experts, participation in related conferences and technical sessions, and reviews of previous studies and papers on counterfeit electronic parts.

A total of 387 surveys were received, representing 83 OCMs, 98 parts distributors (including brokers), 32 circuit board assemblers, 121 prime contractors and subcontractors, and 53 DOD organizations. The data collected shows the number of suspected/confirmed counterfeit part incidents rising dramatically over four years to a level approaching 10,000 annually. These parts are primarily discrete electronic components and microcircuit products.[4]

This assessment is divided into seven chapters: one chapter for each of the five identified industry and government sectors, a chapter of cross-sector analysis tying the five sectors together, and a chapter on best practices for industry and government and recommendations for the U.S. Government. There is also a glossary, appendices with additional survey data.

GENERAL REPORT FINDINGS

There is a lack of dialogue between all organizations in the U.S. defense supply chain about counterfeits. Survey data from the five sectors shows that organizations generally only discuss counterfeit part issues within their individual organizations and, to a lesser extent, with

[4] For the purposes of this study, an incident is a single encounter of a suspected/confirmed counterfeit part. An incident could involve one part or a thousand parts of a component.

their customers and immediate suppliers. This leads to a lack of information sharing throughout the supply chain which could be used to mitigate the risk of counterfeits.

There is an assumption that others in the supply chain are testing parts. Organizations within every sector rely on others in the supply chain to test and verify the authenticity of parts, and therefore conduct little testing themselves. Based on survey data, this confidence in the testing behaviors of the supply chain is unfounded.

There is a lack of traceability in the supply chain. Procurement organizations at times cannot trace purchased parts back to their points of origin with any degree of certainty. This is further compounded by the fact that many components are provided by offshore suppliers, making verification more difficult.

There is an insufficient chain of accountability within organizations. Few survey participants identified a designated person or office responsible for either addressing the risks posed by counterfeit parts or handling identified counterfeit parts. This can lead to a lack of centralized data within an organization and inconsistent counterfeit avoidance practices.

Recordkeeping on counterfeit incidents by organizations is very limited. Most organizations do not keep records of counterfeit incidents. Those that do keep records track limited data points. This can lead to a lack of institutionalized knowledge about an organization's encounters and problems with counterfeits.

Few know what authorities to contact in the federal government regarding counterfeit parts. The majority of survey participants reported having no knowledge of the federal authorities responsible for investigating counterfeit incidents, either defense- or industry-related, or where to submit reports of counterfeit parts. OTE analysts were able to pinpoint the Defense Criminal Investigative Services (DCIS) and the Federal Aviation Administration (FAA) as the federal authorities responsible for counterfeits related to defense and commercial aviation, respectively. However, OTE analysts were not able to identify a distinct federal authority responsible for counterfeits related to commercial products, including parts supporting critical infrastructure, or pinpoint legal requirements related to the handling of counterfeits in the supply chain.

Few are aware of legal requirements and liabilities regarding counterfeits. The majority of survey participants were not aware of any legal requirements or liabilities related to the management, distribution, storage, and disposal of counterfeit parts.

Stricter testing protocols and quality control practices are needed. There are wide differences in the levels and quality of testing undertaken by organizations purchasing and receiving parts. In addition, there are no existing standards for third-party testing facilities. While there are industry standards addressing testing and quality control issues, they have not been systematically embraced or enforced by the supply chain.

Most DOD organizations do not have policies in place to prevent counterfeit parts from infiltrating their supply chain. DOD organizations tend to rely solely on the Defense Federal Acquisition Regulations (DFAR) to guide their procurement practices. At the time the survey was conducted, few had developed additional procurement and testing protocols to address the problems caused by counterfeit parts.

No type of company or organization has been untouched by counterfeit electronic parts. Even the most reliable of parts sources have discovered counterfeit parts within their inventories.

Ultimately, everyone must work together to solve the problem of counterfeit parts. All sectors of the U.S. electronics supply chain need to be more open to dialogue and cooperation in order to address the issue of counterfeit parts. In addition, there needs to be better interaction between federal authorities and the supply chain in order to determine legal requirements and effective counterfeit avoidance activities.

II. Original Component Manufacturers (OCMs)

For the purposes of this study, the U.S. electronics supply chain begins with original component manufacturers (OCMs). Their products are purchased and consumed by parts distributors, circuit board assemblers, prime contractors and subcontractors, and the Department of Defense (DOD). OTE surveyed 39 manufacturers of discrete electronic components (e.g., capacitors, resistors, transistors, and diodes) and 44 manufacturers of microcircuit products to determine how counterfeiting affects them.[5]

A large percentage of OCMs reported becoming aware of counterfeit versions of their products being marketed at least once in the 2005-2008 survey period.[6] Nearly 46 percent of OCMs (18 companies) that produce discrete electronic parts stated they encountered counterfeit versions of their products. Fifty-five percent of microcircuit manufacturers (24 companies) encountered counterfeit versions of their products (see Figure II-1).

Figure II-1: Companies Encountering Counterfeit Electronics

Type of Company	Encountered Counterfeits	Did Not Encounter Counterfeits	Total
Discrete Electronic Components	18	21	**39**
Microcircuits	24	20	**44**
Total	**42**	**41**	**83**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

[5] For ease of analysis, OCMs that manufacture both discrete electronic components and microcircuits were considered two different companies.

[6] For the purposes of this assessment, the term "counterfeit part" and any variation of it, means a suspected or confirmed counterfeit part or component.

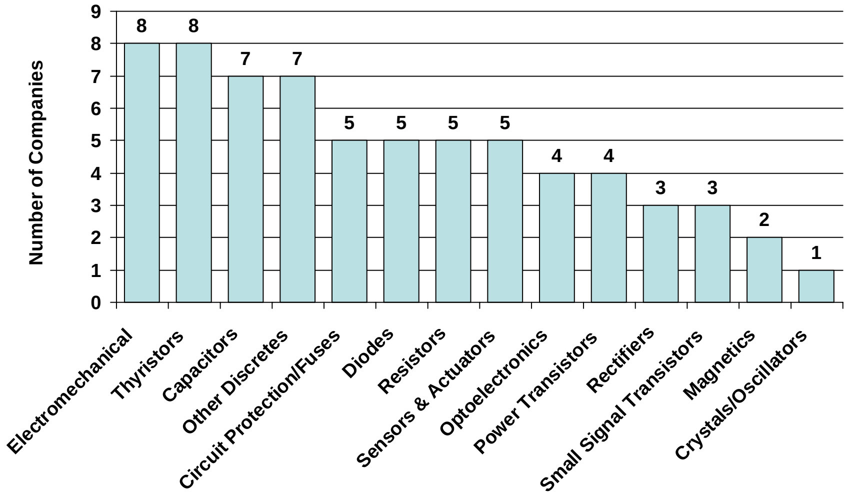
OCM CUSTOMERS

Manufacturers of discrete electronic parts and microcircuit products primarily supply original equipment manufacturers (OEMs), contract manufacturers, individual customers, prime contractors and subcontractors, and entities in the U.S. Government that incorporate parts into systems and subsystems (see Appendix B, Figures B-1 – B-2). A significant number of OCMs also sell their product to authorized distributors, independent distributors, and parts brokers, which in turn sell the components to a wide variety of customers.

COUNTERFEIT INCIDENTS

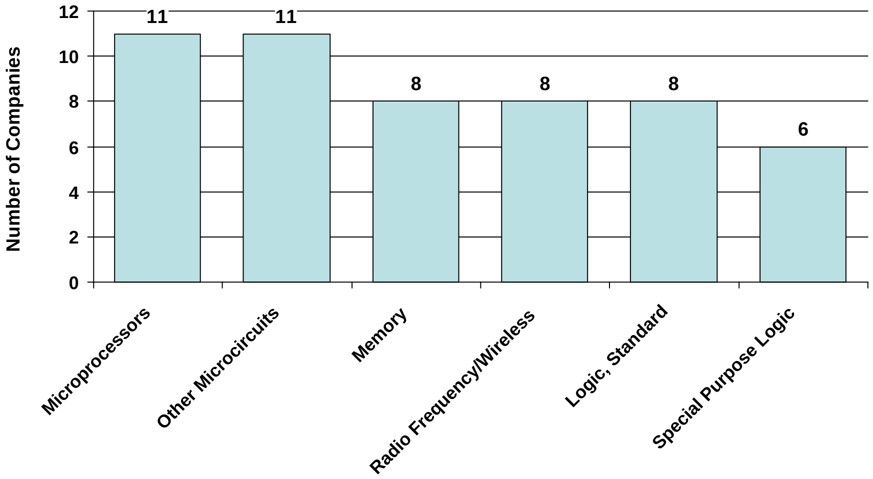
Fifty percent of OCMs have encountered counterfeit electronic parts from 2005 to 2008. Respondents indicated that counterfeit products are being discovered in all 14 discrete electronic component and six microcircuit product categories listed in the survey (see Figures II-2 and II-3). Counterfeit activity reported by manufacturers of discrete components was highest for electromechanical devices and thyristors, while manufacturers of microcircuits cited microprocessors as the most prevalent counterfeit part.

Figure II-2: Types of Manufactured Parts Suspected/Confirmed to Be Counterfeit - Discretes



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

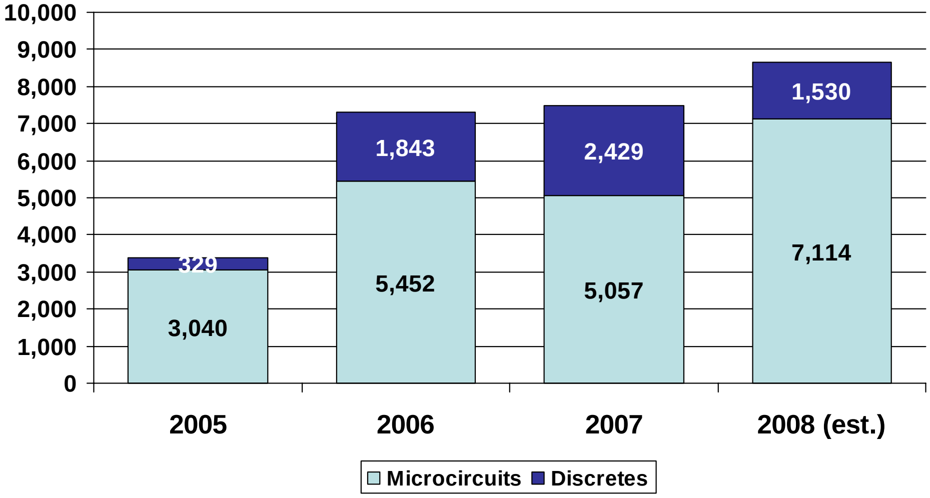
Figure II-3: Types of Manufactured Parts Suspected/Confirmed to Be Counterfeit - Microcircuits



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

The number of counterfeit incidents OCMs encountered shows the seriousness of the counterfeiting issue.[7] The number of incidents rose dramatically, more than doubling from 3,369 incidents in 2005 to 8,644 incidents in 2008 (see Figure II-4). This large increase can be attributed to a number of factors, such as a growth in the number of counterfeit parts, better detection methods, and/or improved tracking of counterfeit incidents.

Figure II-4: Total Counterfeit Incidents - OCMs (2005 – 2008)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

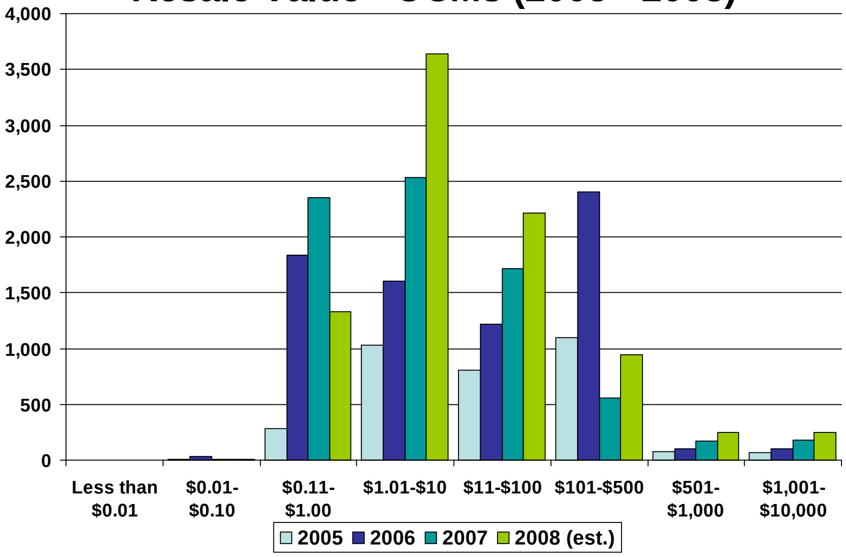
The number of incidents of counterfeit discrete components reported by OCMs soared 560 percent, from 329 cases in 2005 to 1,843 in 2006, and jumped another 32 percent between 2006 and 2007. Microcircuit OCMs also reported a sharp rise in counterfeit product being sold from 2005 to 2008, with a slight decline from 2006 to 2007.

The resale value of counterfeit products spans a wide range, from a few pennies per unit to thousands of dollars per unit. During the 2005-2008 period, most counterfeit activity is concentrated on parts selling in the 11 cents to $500 range (see Figure II-5). Respondents also

[7] For the purposes of this study, an incident is a single encounter of a suspected/confirmed counterfeit part. An incident could involve one part or a thousand parts of a component.

experienced a small but steady increase in the number of counterfeits in the $501 to $1,000 and $1,001 to $10,000 ranges.

Figure II-5: Counterfeit Incidents by Product Resale Value - OCMs (2005 - 2008)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

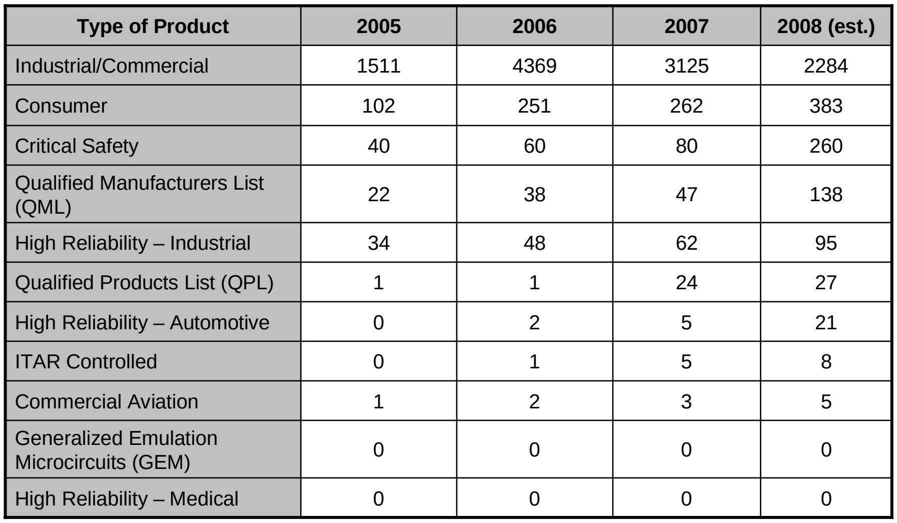
Type of Parts Counterfeited

Survey respondents reported the number of counterfeit product models they encountered by category to determine the types of parts and components most affected by counterfeits. This breakout of counterfeits by product type was difficult for most companies to provide, either because of limited recordkeeping and/or unknown applications by the ultimate end-users.

The data demonstrates that most counterfeit activity reported by OCMs is concentrated in five electronic part market sectors: industrial/commercial, consumer, critical safety, Qualified Manufacturers’ List (QML), and high reliability-industrial (see Figure II-6). The number of counterfeit incidents has increased in eight of 11 product categories.

Counterfeit versions of components on the QML and Qualified Products List (QPL) categories raise a particular concern for the U.S. defense supply chain.[8] Both categories experienced small but significant increases in the number of counterfeits over the 2005-2008 period. While the total number of counterfeit incidents reported was relatively low, QML and QPL parts are typically used in defense and national security systems. Counterfeits could therefore impact critical defense end-users and infrastructure.

Figure II-6: Type of Counterfeit Incidents - OCMs (2005-2008)



Type of Product	2005	2006	2007	2008 (est.)
Industrial/Commercial	1511	4369	3125	2284
Consumer	102	251	262	383
Critical Safety	40	60	80	260
Qualified Manufacturers List (QML)	22	38	47	138
High Reliability – Industrial	34	48	62	95
Qualified Products List (QPL)	1	1	24	27
High Reliability – Automotive	0	2	5	21
ITAR Controlled	0	1	5	8
Commercial Aviation	1	2	3	5
Generalized Emulation Microcircuits (GEM)	0	0	0	0
High Reliability – Medical	0	0	0	0

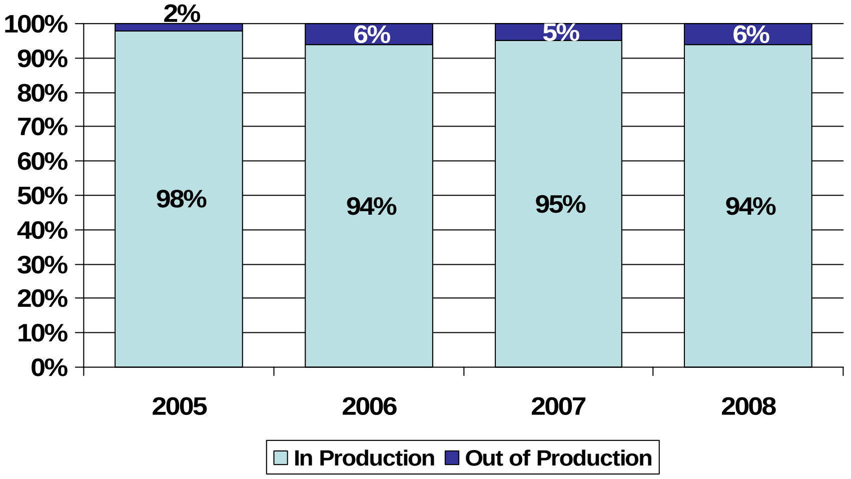
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

OCMs also identified the number of counterfeit incidents they encountered that were "in production" as opposed to "out of production."[9] For discrete electronic OCMs, approximately 94 percent of the counterfeits they encountered were of "in production" parts (see Figure II-7). In the case of microcircuit products, while the percentage decreased from 93 percent in 2005 to 68 percent in 2008, the majority of the counterfeits encountered were "in production" parts (see Figure II-8).

[8] According to the Federal Acquisition Regulations (FAR), the QML is "a list of manufacturers who have had their products examined and tested and who have satisfied all applicable qualification requirements for that product." 48 C.F.R. § 9.201 The QPL is "a list of products that have been examined, tested, and have satisfied all applicable qualification requirements." 48 C.F.R. § 2.101

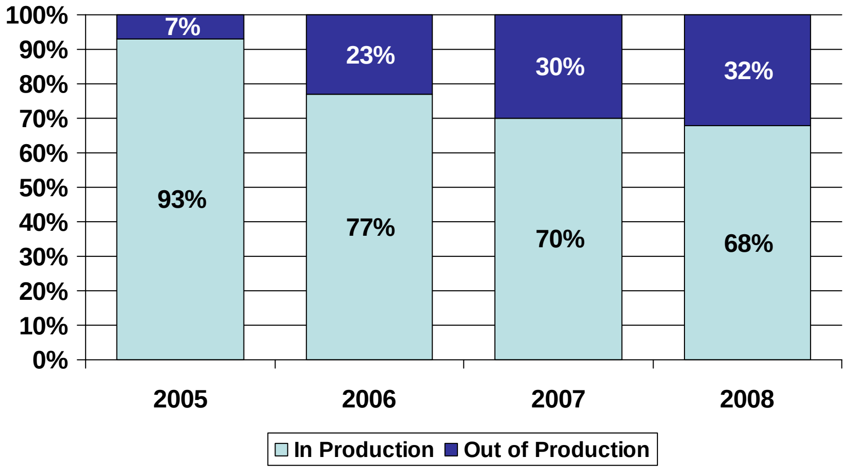
[9] For this assessment, parts produced by an after-market manufacturer are considered "out of production."

Figure II-7: Percent of Counterfeit Incidents Involving In/Out of Production Parts – Discrete Manufacturers (2005-2008)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure II-8: Percent of Counterfeit Incidents Involving In/Out of Production Parts – Microcircuit Manufacturers (2005-2008)

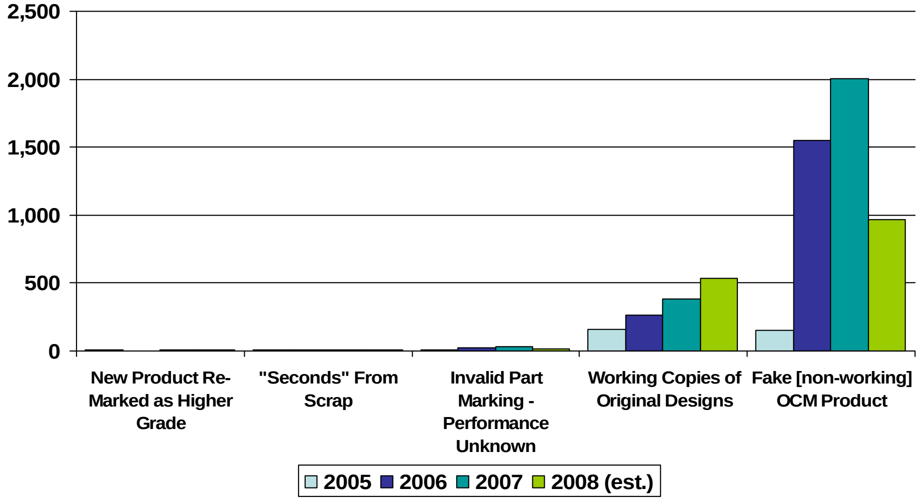


Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

TYPES OF COUNTERFEITS

Survey data suggests that the vast majority of the counterfeit discrete components and microcircuit products encountered by OCMs are rudimentary variations of the real product. With respect to discrete components, OCMs reported that most of the counterfeits they encountered involved the supply of "fake non-working product." This was followed by "working copies of the original designs" (see Figure II-9).

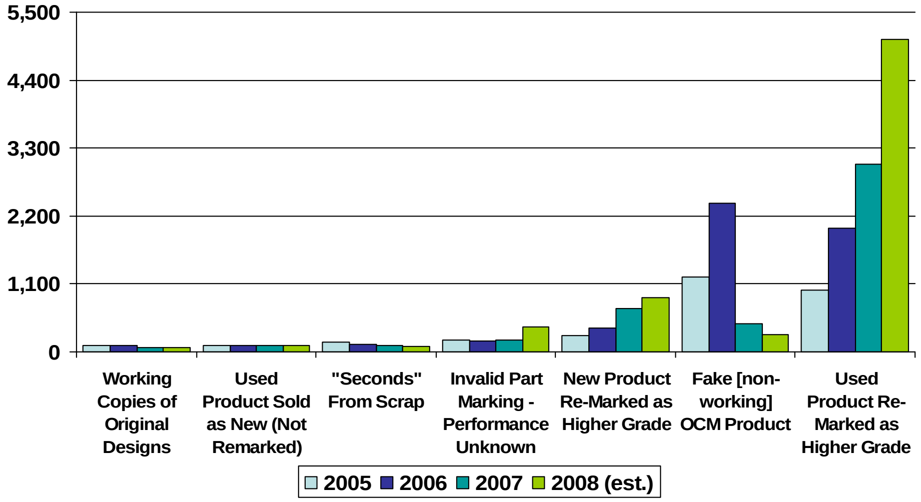
Figure II-9: Counterfeit Incidents by Type of Problem - Discretes (2005-2008)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

For microcircuit manufacturers, the most dominant type of counterfeiting activity encountered was "used product re-marked as higher grade new product" (see Figure II-10). These types of counterfeit parts may work, but will not operate at the same level as the higher grade part and may fail under stress that would be expected under normal conditions. The next most common types were "fake non-working product" and "new product re-marked as higher grade product." Like re-marked used product, re-marked new product will work, but not at the desired level of functionality.

Figure II-10: Counterfeit Incidents by Type of Problem - Microcircuits (2005-2008)



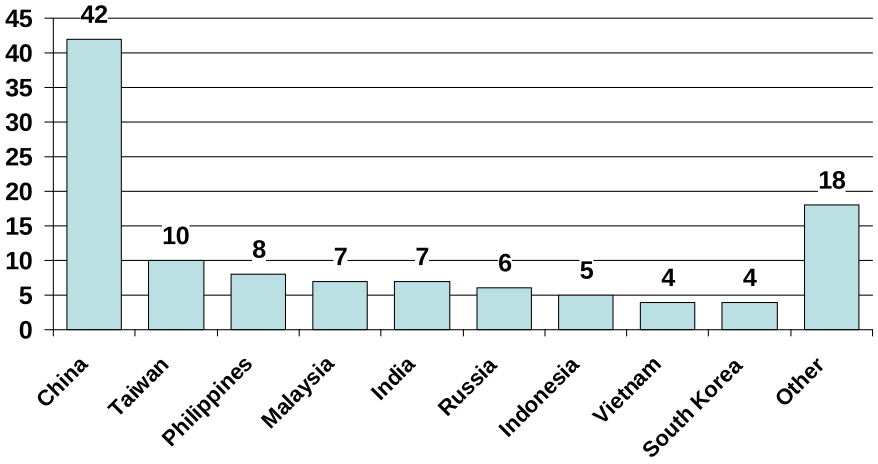
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

SOURCES OF COUNTERFEITS

Discrete component and microcircuit manufacturers were asked to identify the top five countries suspected or confirmed to be sources of counterfeit electronic parts. China was most frequently identified by OCMs as a source of counterfeits, with Asia as the most predominant regional source (see Figure II-11). Additionally, OCMs identified Russia and India as suspected sources of counterfeit components.[10] Several OCMs said it is difficult to confirm where counterfeits are coming from; their answers on where counterfeits originated were based on general information rather than their own experiences.

[10] The “Other” column in Figure II-11 is comprised of the following countries: Singapore, Thailand, Brazil, Mexico, Israel, North Korea, the United Kingdom, Paraguay, Iran, Georgia, Hungary, Chile, Romania, and Uruguay.

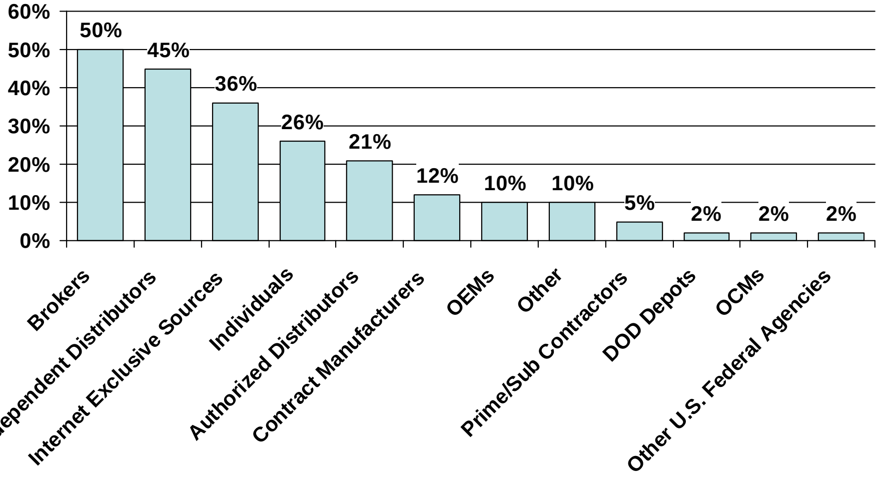
Figure II-11: OCMs' Top 10 Countries Suspected as Sources of Counterfeits (2008 est.)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Another sourcing concern is how counterfeit components are entering the supply chain. OCMs participating in the survey identified at least 12 separate entities that have sold or distributed counterfeit product, ranging from parts brokers to federal agencies (see Figure II-12).

Figure II-12: Percent of OCMs with Cases of Counterfeit Incidents Sold by Type of Entity*



*** Only includes companies who encountered counterfeits**

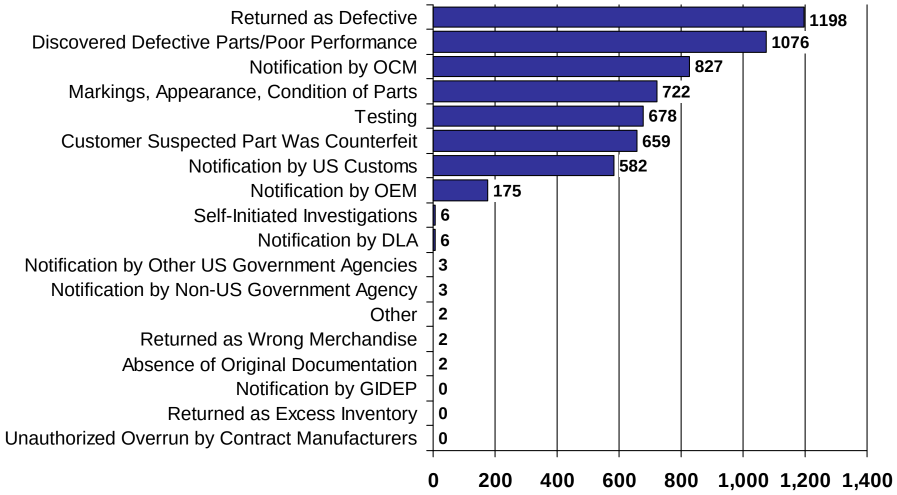
Source: U.S. Department of Commerce, Office of Technology Evaluation,
Counterfeit Electronics Survey, November 2009.

OCMs that experienced counterfeits most frequently cited parts brokers as a source of counterfeit parts, followed by independent distributors and Internet-exclusive suppliers. Of particular note is that 21 percent of affected OCMs identified authorized distributors as having sold counterfeit parts. A considerable number of OCMs found other entities selling counterfeit parts.

METHODS OF DISCOVERY

Customer feedback is a key means by which OCMs learn about counterfeit versions of their products. The majority of counterfeit parts are being discovered because they are returned as defective, exhibit poor performance, or have incorrect markings or physical appearance (see Figure II-13). A significant number of counterfeit incidents were uncovered because the customer suspected the parts were counterfeit.

Figure II-13: Counterfeit Incidents by the Method Uncovered – OCMs (2008 est.)

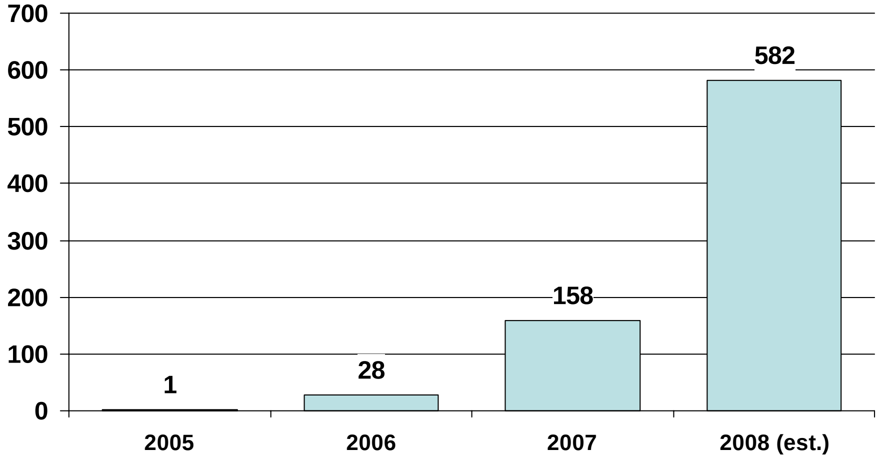


Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

OCMs became aware of few notifications of counterfeit incidents by U.S. Government agencies. OCM survey participants said they were aware of the Defense Logistics Agency (DLA) issuing six reports of counterfeit incidents, other U.S. government agencies issuing three reports, and the Government-Industry Data Exchange Program (GIDEP) issuing no reports.

The only exception to this trend was U.S. Customs and Border Protection (CBP). While OCMs said they received a low number of reports on counterfeit parts from CBP in 2005 and 2006, the number of reports rose significantly in 2007 and 2008 (see Figure II-14). This increase can in part be attributed to efforts by the Semiconductor Industry Association's (SIA) Anti-Counterfeiting Task Force, which has worked with CBP to train personnel to more effectively intercept counterfeit electronic parts entering the United States.

Figure II-14: Counterfeit Incidents Uncovered Through Notifications by U.S. Customs - OCMs



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

OCMs were also asked to report on specific methods in place for customers to use for notification of counterfeit parts. Thirty-three percent have no formal mechanism for customers to report suspected and confirmed counterfeit parts (see Figure II-15). OCMs with specific mechanisms in place employ a range of methods, including website, e-mail, hotline, sales representatives, and general phone call notification.

Figure II-15: How Customers/Authorized Distributors Notify OCMs Concerning Counterfeit Parts*

Website	35%
Hotline	25%
E-mail	13%
Sales Contacts	13%
General Phone Call	10%
Other	10%
None	33%

*** Companies were permitted to answer ‘Yes’ to multiple methods.**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

INTERNAL DATABASE TO TRACK COUNTERFEITS

OCMs also identified their efforts to formally track encounters with counterfeit parts. Sixty-seven percent of OCMs producing discrete components and 33 percent of OCMs producing microcircuit products do not maintain databases on either the counterfeit parts encountered or the incidents reported to them (see Figure II-16).

Figure II-16: Percent of Companies Who Encountered Counterfeits That Do Not Maintain a Database to Track Counterfeit Products

Discrete Manufacturers	67%
Microcircuit Manufacturers	33%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Manufacturers that collect information on counterfeit versions of their products reported tracking the following: types of products counterfeited; source countries; companies and individuals involved; and source of reporting (see Figure II-17). A smaller percentage of counterfeit databases track "other" variables including affected customers, dollar value of parts, part numbers, types of counterfeits, and CBP seizures.

Figure II-17: Variables Tracked By Internal Counterfeit Database*

Variable	Discrete Manufacturers	Microcircuit Manufacturers
Suspected/Confirmed Counterfeit Products	100%	100%
Countries of Origin	89%	95%
Known/Suspected Companies and Individuals	89%	85%
Source of Reporting	78%	95%
Other	11%	25%

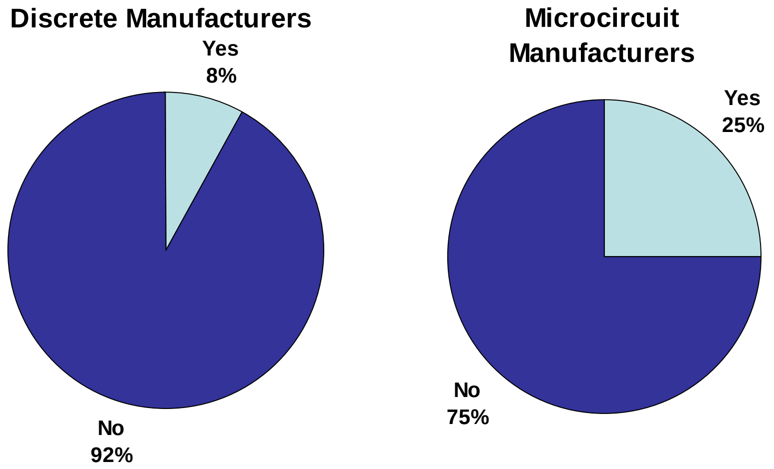
***Taken as a percent of those companies encountering counterfeits who maintain an internal database.**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

DAMAGE TO COMPANIES' REPUTATION

Most OCMs do not believe their reputations have been negatively affected by counterfeit parts. Only eight percent of discrete component manufacturers reported that their company's reputation and standing in the marketplace has been hurt by counterfeit versions of their products. A larger percent of microcircuit OCMs (25 percent) stated their companies' reputations were damaged by counterfeit versions of their products in the U.S. supply chain (see Figure II-18). One OCM said, "With counterfeit goods in the market, purchasers are not sure if they received genuine or fake goods so they tend to avoid the brand entirely."

Figure II-18: Have Counterfeits Had a Negative Effect on Your Company's Image/Reputation?



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

INVENTORY CONTROLS AND TESTING

How OCMs handle their product inventories, particularly through returns and buying back excess product, plays a role in the infiltration of counterfeit electronic parts into the U.S. supply chain. To that end, OCMs were asked a series of questions about their inventory practices and testing procedures to identify areas of possible concern.

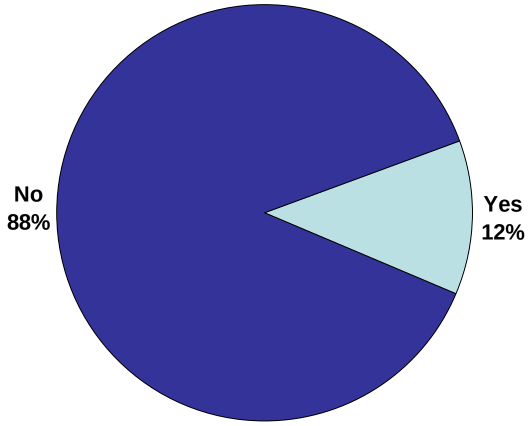
Return Policies and Re-Circulation of Parts

OCMs risk compromising inventory by accepting returns and buying excess inventory back from customers. Customers can purchase counterfeit parts from another source and, knowingly or unknowingly, return those parts to the OCMs. The risk of counterfeit parts entering the supply chain is greater if returned parts are placed into inventory without proper testing and inspection.

Ninety-six percent of OCMs reported accepting returns of discrete components or microcircuit product from customers. Sixty-three percent of OCMs surveyed acknowledged buying back excess inventory from their authorized distributors, and 25 percent said they buy back excess inventory from individual customers. Some further have very strict controls on what can be accepted as a return or is suitable for buying back, such as warranty situations or when the product is in original, unopened packaging. Overall, 61 percent of OCMs restock and re-circulate returns and excess inventory.

While seemingly reasonable, this business practice is not without risks. Seventeen percent of OCMs reported receiving counterfeit product from individual customers. Twelve percent also reported receiving counterfeit product from one of their authorized distributors (see Figure II-19).

Figure II-19: Percent of OCMs That Have Cases of Authorized Distributors Returning Counterfeit Parts



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

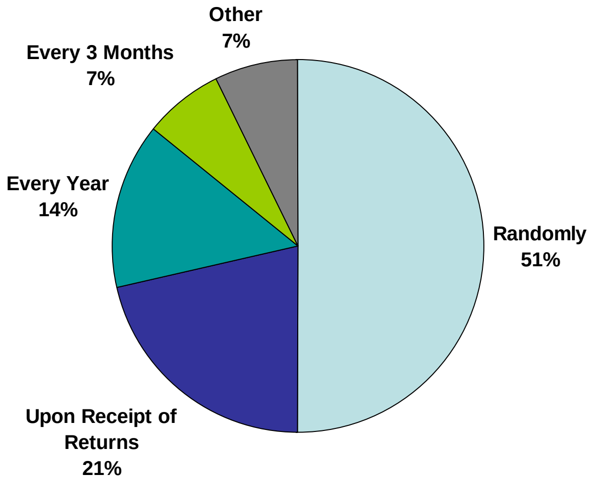
INVENTORY AUDITING PROCEDURES

As the manufacturers and primary sellers of discrete electronic components and microcircuits, OCMs have little reason to conduct inventory audits to detect counterfeit parts. Problems arise, however, when unauthentic parts returned or reacquired by OCMs are introduced into inventory without inspection. In these situations, inventory audits can be a useful tool for OCMs to discover counterfeits.

Only 18 percent of manufacturers of discrete electronic components and 16 percent of microcircuit manufacturers audit their inventories for the presence of counterfeit parts (see Appendix B, Figure B-3). In the case of OCMs that buy back excess microcircuit product from customers, only 20 percent audit their inventory for counterfeit parts. Some OCMs that do not conduct inventory audits instead test incoming parts upon receipt prior to placement in inventory. Others conduct general inventory audits instead of ones specifically aimed at detecting counterfeits.

Half of the OCMs that conduct inventory audits for counterfeits (51 percent) do so randomly. Another 14 percent conduct inventory audits for counterfeits annually, and seven percent audit quarterly. Twenty-one percent of the OCMs that reported conducting audits test returns upon receipt (see Figure II-20).

Figure II-20: Frequency of Inventory Audits for Counterfeits – OCMs*



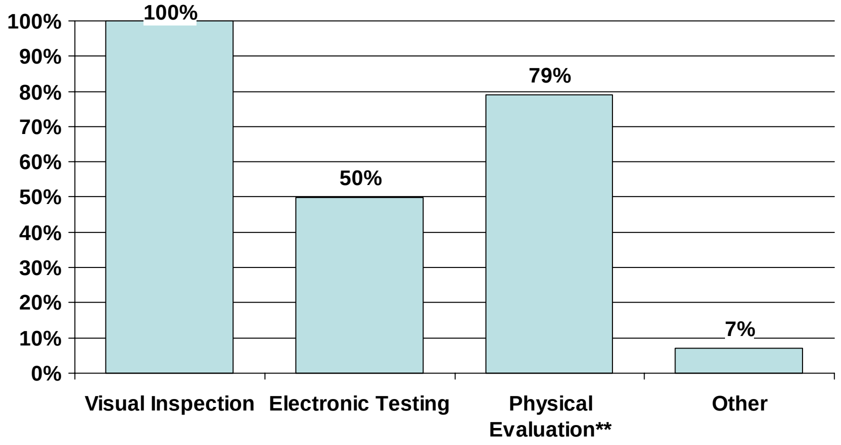
*** Only includes companies who audit their inventory for counterfeits**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

The extent of quality control and testing that companies are prepared to support using internal and external resources is another variable in OCM auditing practices. Ninety-three percent of OCMs performing inventory audits use company staff to perform the task, while seven percent rely on independent auditors. Only 15 percent of companies use independent authorities to review their auditing practices.

Several methods can be used to audit discrete electronic component and microcircuit product inventory. All OCMs that perform inventory audits conduct visual inspections, a relatively low-cost approach to ascertaining whether a part is genuine (see Figure II-21). Half of OCM survey respondents go a step further and perform electronic testing during inventory audits, and 79 percent indicated they perform physical evaluation.[11]

Figure II-21: Form of Inventory Audits for Counterfeits - OCMs*



*** Only includes companies who audit their inventory for counterfeits**

**** Physical evaluation may have been misinterpreted to mean a type of visual inspection, rather than destructive testing.**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

TESTING AND TESTING FACILITIES

OCMs identified the number of product models for which they ordered visual inspection, electrical testing, and physical evaluation. In 2008, less than a quarter of OCMs ordered visual inspections for at least one product model, and even fewer ordered electronic testing and physical evaluation (see Figure II-22). Several OCMs stated that since they manufacture genuine parts, there is no need to conduct testing on their products.

[11] The number of OCMs performing physical evaluation may be overstated because some survey respondents may have misinterpreted the term to mean a form visual inspection, rather than invasive physical examination.

Figure II-22: Percent of OCMs Ordering Testing for at Least One Product Model

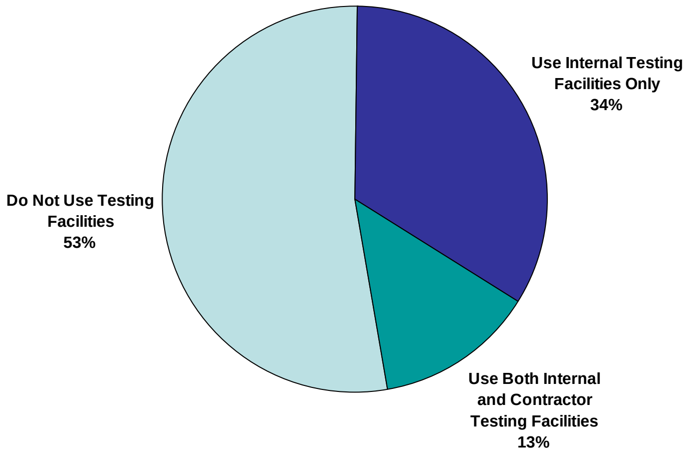
	Visual Inspection	Electronic Testing	Physical Evaluation*
Discrete Manufacturers	23%	15%	18%
Microcircuit Manufacturers	23%	16%	16%

*** Physical evaluation may have been misinterpreted to mean a type of visual inspection, rather than destructive testing**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Companies can use internal or external testing facilities to run different types of tests when checking the authenticity of a part. The majority of OCMs (53 percent) do not use any testing facilities in performing their evaluations (see Figure II-23). Alternatively, 34 percent of OCMs use internal testing labs, and 13 percent rely on both internal and external contractor-operated facilities to test electronic parts.

Figure II-23: Percent of OCMs Utilizing Testing Facilities to Detect Counterfeits



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Of the OCMs that use testing facilities, 64 percent rely on a combination of U.S.-based facilities and non-U.S. testing labs, 26 percent use only U.S.-based facilities, and 10 percent use only non-U.S. facilities. A number of OCMs have experienced testing facilities mismanaging and not properly disposing of parts that were scrapped following testing (see Appendix B, Figure B-4).

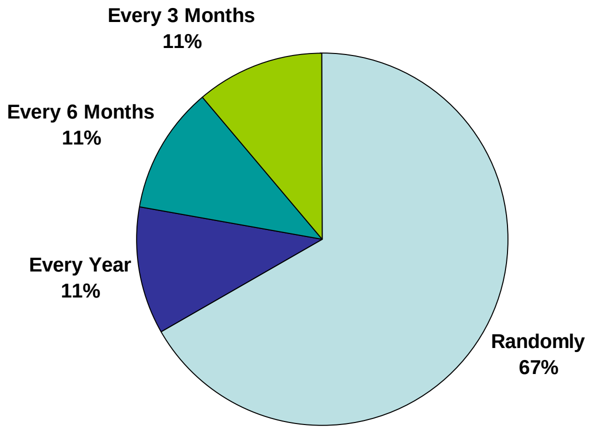
Inventory Audits of Authorized Distributors

In addition to describing their own auditing practices, manufacturers were queried about the extent to which they audit their authorized distributors. Eleven percent of OCMs (nine companies) said they audit their authorized distributors' inventory for counterfeits of their product. Some of the OCMs that answered "no" for this question conduct general inventory audits of their authorized distributors instead of counterfeit-specific audits. Others have no authorized distributors to audit. One OCM that does not audit its authorized distributors for counterfeit parts said, "Strong auditing is not needed because tainted inventory causes authorized distributors to lose business."

Sixty-seven percent of OCMs that do audit their authorized distributors do so randomly, while 33 percent conduct audits of their authorized distributors either quarterly, semi-annually, or annually (see Figure II-24). While all respondents reported performing visual inspections, none acknowledged performing electronic testing of distributor inventory. Forty-four percent perform physical evaluations and 11 percent perform other types of testing.[12] In addition, four OCMs auditing their authorized distributors have their auditing practices reviewed by independent authorities.

[12] As stated previously, the higher number of OCMs conducting physical evaluation is likely due to respondents mistaking it for a form of visual inspection.

Figure II-24: Frequency of Inventory Audits of Authorized Distributors for Counterfeits*



*** Only includes companies who audit their inventory for counterfeits**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

LEGAL AGREEMENTS WITH AUTHORIZED DISTRIBUTORS

Survey respondents were asked if they have legal agreements with their authorized distributors regarding counterfeit products. Only 12 percent of OCMs reported having such an agreement in place. Some OCMs have no legal agreements regarding counterfeit products because they have no authorized distributors.

Of those OCMs that do have such agreements, 40 percent require authorized distributors to notify them of counterfeit products. Forty percent of respondents also said their agreements restrict authorized distributor purchases of parts to OCM authorized suppliers. None of the agreements require distributors to notify federal authorities of counterfeit products they encounter, or to keep logs on counterfeit parts (see Figure II-25).

Figure II-25: Requirements Concerning Counterfeits from Legal Agreements for Authorized Distributors*

Requirement	Percent
Notification of OCM Concerning Counterfeit Products	40%
Purchase Only From OCM Authorized Sources	40%
Compliance With All Laws	20%
Inventory Checks	10%
Notification of Federal Authorities Concerning Counterfeit Products	0%
Logs of Counterfeit Products	0%

*** Percentage of those companies that have a legal agreement**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

ACTIONS TAKEN REGARDING COUNTERFEITS

OCMs were asked a series of questions about the actions they take or are willing to take regarding counterfeit electronic components: steps they take once they are notified or possess counterfeits; authorities they contact; difficulties in identifying counterfeits; related legal actions; and what is being done to mitigate the risk.

STEPS TAKEN AFTER NOTIFICATION AND POSSESSION OF COUNTERFEIT PARTS

The most common actions taken by OCMs upon notification of a counterfeit part are to notify internal company authorities and trace their supply chain (see Figure II-26).[13] Only 35 percent of OCMs inform their authorized distributors of counterfeit incidents, and even fewer notify federal authorities and industry associations, at 18 and 13 percent, respectively. Eighteen percent of OCMs take no action upon learning of counterfeit versions of their product.

[13] Some respondents answered this survey question from the perspective of what they would do if they were notified of counterfeit parts, not what they have done.

Figure II-25: Requirements Concerning Counterfeits from Legal Agreements for Authorized Distributors*

Requirement	Percent
Notification of OCM Concerning Counterfeit Products	40%
Purchase Only From OCM Authorized Sources	40%
Compliance With All Laws	20%
Inventory Checks	10%
Notification of Federal Authorities Concerning Counterfeit Products	0%
Logs of Counterfeit Products	0%

*** Percentage of those companies that have a legal agreement**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

OCMs also take action when they have physical possession of a counterfeit part. Fifty-seven percent of companies retain samples for references, and another 57 percent test parts.[14] Forty-nine percent enter information on the incident in corporate databases (see Figure II-27). A quarter of OCMs take no action when they have possession of a counterfeit part. Smaller percentages of OCMs turn suspect parts over to law enforcement, check industry or U.S. Government databases, or enter information into those databases.

Figure II-27: Steps Taken/Would be Taken After Possession of a Counterfeit Part – OCMs

Retain Samples for Reference	57%
Test Part	57%
Enter into Company Database	49%
No Steps are Taken	25%
Leave Disposal Up to Party Filing Complaint	23%
Quarantine Parts	22%
Dispose of Parts Immediately	19%
Random Inventory Testing	18%
Issue Credit	17%
Turn Over to Law Enforcement Authorities After Analysis	14%
Other	10%
Turn Over to Law Enforcement Authorities For Analysis	10%
Check Industry or USG Databases	8%
Enter into Industry or USG Databases	7%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

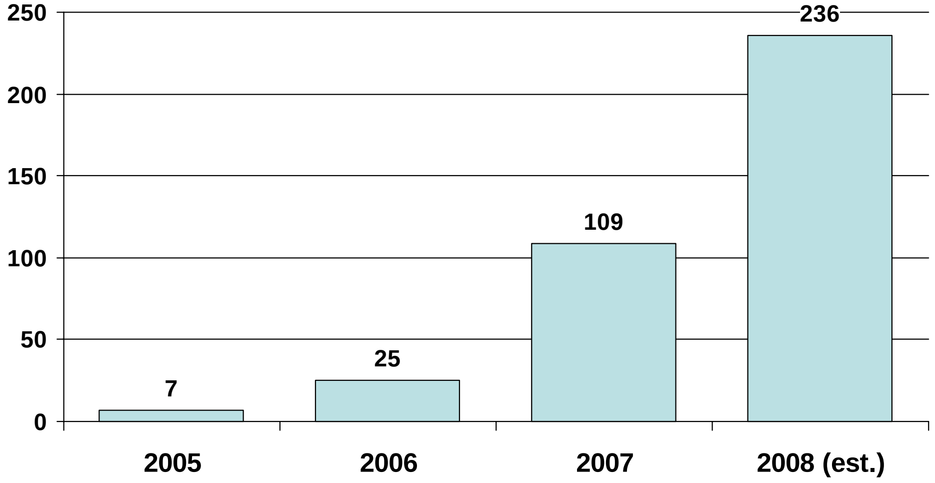
[14] Some respondents answered this survey question from the perspective of what they would do if they had possession of counterfeit parts, and not what they have done.

AUTHORITIES CONTACTED AFTER COUNTERFEIT INCIDENTS

The low percentage of OCMs that notify federal authorities when they become aware of or possess a counterfeit can be attributed in part to a lack of information on what authorities to contact. Sixty percent of OCM respondents do not know what authorities to notify in such a situation. Of those OCMs that encountered counterfeits, 36 percent do not notify federal authorities and 65 percent do not notify industry associations. One OCM stated that, “We have queried various federal authorities … for written instructions or guidance on reporting suspected/confirmed counterfeit products. We have received no responses to these queries.” Some OCMs said they do not contact any authorities about counterfeit incidents because they have never encountered a counterfeit part.

Despite the confusion about who to notify, OTE data shows that OCM reporting of counterfeit incidents has increased in recent years. In 2005, OCMs reported just seven incidents to federal agencies (see Figure II-28). That number increased steadily in subsequent years, with OCMs reporting 235 incidents in 2008.

Figure II-28: Number of Incidents Reported to Government Authorities - OCMs



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

OCMs with counterfeit parts contact CBP most often, though only 29 percent of OCMs that have counterfeits have done so.[15] An additional 12 percent contact the Government-Industry Data Exchange Program (GIDEP); 10 percent report only military grade products, and two percent report on a case-by-case basis. Two OCMs reporting to GIDEP said they only do so occasionally because the reporting process is too time and labor intensive to report every incident.

OCMs provided several reasons why 88 percent of those with counterfeits do not report to GIDEP:

- they were not aware of GIDEP or that it tracked counterfeit incidents;
- the counterfeit parts encountered were minor and did not warrant reporting;
- they do little to no work for the U.S. military and U.S. Government; and
- they do not see any business benefit in reporting to GIDEP.

OCMs identified the authorities they instruct their authorized distributors to contact regarding counterfeit parts. Sixty-six percent of OCMs tell their authorized distributors to notify their company in the event of a counterfeit incident (see Appendix B, Figure B-6). More than a quarter of OCMs do not provide authorized distributors with any instructions on what authorities to contact. Many of these OCMs do not provide notification instructions either because they have never encountered counterfeits or do not have authorized distributors.

Legal Guidance and Liabilities

OCMs were asked a series of questions on their knowledge of legal requirements, liabilities, and guidance regarding the handling of counterfeit parts. Sixty percent of OCMs reported not being aware of legal requirements for management and/or disposal of counterfeit electronic parts. Additionally, 60 percent of OCMs are not aware of liabilities related to the distribution, storage, and disposal of counterfeit parts. One OCM commented that, “Since we have never had an incidence of suspected counterfeit parts, we have not looked into legal requirements.”

[15] See Figure B-5 in Appendix B for a list of other authorities contacted by OCMs after a counterfeit incident.

A higher number of OCMs (76 percent) are not aware of written instructions or guidance from federal authorities on reporting counterfeit incidents. Yet 58 percent said they do not need guidance from the U.S. Government with regard to civil and criminal liability and penalties related to the distribution, storage, and disposal of suspected counterfeit products.

OCMs do not pursue legal action at a high rate as a method to reduce counterfeits. Only 11 OCMs incurred legal costs between 2005 and 2008 related to addressing counterfeit product issues. For these companies, counterfeit incident-related legal costs comprised 0.7 percent of their total legal costs on average.

Of the 83 surveyed OCMs, 29 percent could have filed more legal actions to address counterfeit product issues over the 2005-2008 period. These OCMs reported that the extent of the counterfeit parts problems was too small to pursue (see Figure II-29). A significant number of OCMs did not file more legal actions because the costs and time requirements were too excessive, the chance of success was low, or the perpetrators could not be found.

Figure II-29: Reasons for OCMs Not Filing More Legal Actions Related to Counterfeits*

Extent of problem was not large enough to bother	100%
Legal costs and time requirements excessive	94%
Chance of success was low	94%
Perpetrator(s) could not be found	89%
Insufficient support from U.S. Federal Authorities	33%
Did not want to make the problem public	22%
Other	17%

* Percent is out of the number of companies that could have filed more legal actions.

Source: U.S. Department of Commerce, Office of Technology Evaluation,
Counterfeit Electronics Survey, November 2009.

Difficulty Identifying Counterfeit Parts

Considering the increase in the proliferation of counterfeit parts, OCMs were asked if they find it difficult to identify counterfeit components and if they are better able to identify counterfeits today than they were five years ago. Interestingly, 78 percent of OCMs do not find it difficult to identify counterfeits. Most of these companies said problems with errors in part markings, codes, and labels of counterfeits are easy to detect.

For the 22 percent of OCMs that find it difficult to identify counterfeits, most stated this was because counterfeiters are getting better at copying part markings and making high-quality counterfeits. A few OCMs do not have the equipment and infrastructure to test parts at the level necessary to detect counterfeits. One OCM said, “We don't even try to identify counterfeit parts.”

Although most OCMs do not find it difficult to identify counterfeits, only 47 percent are better able to identify counterfeits today than they were five years ago. These OCMs pointed to increased awareness, improved security, and counterfeit avoidance procedures implemented within the past five years as the reasons for their success. A few OCMs said they are better able to identify counterfeits today because they have taken steps to improve part traceability.

Conversely, 53 percent of OCMs do not believe they are better able to identify counterfeit parts today. Most said they have never encountered counterfeit components, or are not doing anything differently than they were five years ago. A few OCMs said the Internet has increased the proliferation of counterfeits. Some manufacturers are not better able to identify counterfeits because there is a lack of internal and external intelligence on the issue.

Reasons for Counterfeits Entering the U.S. Supply Chain

Survey respondents were asked to provide the prime reasons why counterfeit parts enter the U.S. supply chain (see Figure II-30). The top two reasons identified by OCMs for the proliferation of counterfeit parts were the reliance by brokers and independent distributors on gray market parts, at 42 and 37 percent, respectively.[16] These responses were closely followed by less stringent inventory management by parts brokers and independent distributors.

[16] A gray market is the trade of parts through distribution channels which, while legal, are unofficial, unauthorized, or unintended by OCMs.

Figure II-30: OCMs' Top Ten Reason For Counterfeits Entering the Supply Chain

Greater reliance by brokers on gray market parts	42%
Greater reliance by independent distributors on gray market parts	37%
Less stringent inventory management by parts brokers	36%
Less stringent inventory management by independent distributors	28%
Insufficient chain of accountability	27%
Insufficient buying procedures	23%
Purchase of excess inventory on the open market	23%
Inadequate part purchase planning by OEMs	23%
Inadequate part purchase planning by contract manufacturers	23%
Greater reliance on contract manufacturers for procurement	23%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Internal Actions Taken to Prevent Infiltration of Counterfeits

OCMs were asked about the internal and external steps they have taken to prevent the infiltration of counterfeits. More than a third of discrete electronic component and microcircuit manufacturers are revising internal procedures to more carefully evaluate customer returns (see Figure II-31). Many OCMs are also revising procedures on the disposal of "seconds," defective parts, and production overruns, training staff, and conducting testing on inventory. Relatively few companies are taking technological steps such as adding security features into parts. More than a third of discrete electronic component and microcircuit OCMs have taken no internal actions to prevent the proliferation of counterfeits.

Figure II-31: Internal Actions Taken to Prevent Infiltration of Counterfeits – OCMs

Action	Discrete Manufacturers	Microcircuit Manufacturers
No internal actions taken	38%	32%
Revising procurement procedures to more carefully screen/audit/evaluate authorized returns from customers	36%	34%
Revising company procedures for disposal of “seconds,” defective parts, and production overruns	26%	41%
Training staff on the negative economic and safety impacts of counterfeit products	26%	36%
Performing screening and testing on inventory	26%	27%
Embedding new security measures in new product lines	8%	16%
Embedding new security measures in existing product lines	8%	16%
Other	5%	11%
Adding security markings to existing inventory	3%	9%

Source: U.S. Department of Commerce, Office of Technology Evaluation *Counterfeit Electronics Survey*, November 2009.

Externally, discrete electronic component and microcircuit manufacturers take different approaches to preventing counterfeit part infiltration. The largest percentage of discrete component OCMs (46 percent) take no external actions (see Figure II-32). Approximately a quarter of discrete component OCMs educate their customers on risks associated with gray market products and/or prohibit their authorized distributors from buying back excess inventory from customers.

In contrast, half of microcircuit OCMs educate their customers on the risks of purchasing gray market products. Significant percentages of microcircuit OCMs also prohibit authorized distributors from buying back excess inventory from customers, tighten contractual obligations of contract manufacturers, and educate customers on the negative impacts of buying counterfeits. Fewer microcircuit manufacturers than discrete component manufacturers take no external actions.

Figure II-32: External Actions Taken to Prevent Infiltration of Counterfeits – OCMs

Action	Discrete Manufacturers	Microcircuit Manufacturers
Educating customers about risks associated with gray market products	28%	50%
No external actions taken	46%	25%
Prohibiting authorized distributors from buying back excess inventory from their customers	23%	43%
Educating customers on the negative economic and safety impacts of counterfeit products	18%	39%
Tightening contractual obligations of contract manufacturers with regard to disposal of “seconds,” defective parts, and overruns	15%	41%
Referring customers to authorized after-market manufacturers	15%	36%
Referring customers to companies that could identify suitable substitute products or re-engineer system components	15%	23%
Other	10%	7%
Prohibiting authorized distributors from buying back excess inventory on the gray market	5%	7%

Source: U.S. Department of Commerce, Office of Technology Evaluation
Counterfeit Electronics Survey, November 2009.

OCMs, as the manufacturers of discrete electronic components and microcircuits, primarily encounter counterfeits through customer returns. Although these companies are often seen as the “victim” of counterfeits, they also have a responsibility in maintaining a secure supply chain as they sell product to every sector of the supply chain, including unauthorized distributors. Yet most OCMs do not actively share information on counterfeit incidents or component specifications with other industry sectors, which could aid in the detection of counterfeit parts. As they have played an effective role in training CBP staff in identifying suspicious shipments, OCMs need to take additional actions such as revising in-house procedures to address issues with returns, buy backs, and the disposal of scrap parts, and cooperate with other industry segments to reduce the problem.

III. DISTRIBUTORS: AUTHORIZED AND UNAUTHORIZED

Distributors are crucial in the electronics supply chain, providing a bridge between electronic component manufacturers and consumers. They often work as a sales arm of original component manufacturers (OCMs), marketing and selling OCM products. Many distributors also act as independent middle men, tracking down hard to find or “out of production parts” for their customers. These companies deal in all types of electronic parts, from discrete electronic components and microcircuits to bare and assembled circuit boards. OTE surveyed 98 distributors of the electronics supply chain to gain their perspective on counterfeit electronics.

Companies were asked to classify themselves as one of three types of distributors: authorized distributors, independent distributors, or brokers. Authorized distributors are companies that have exclusive rights with an OCM or original equipment manufacturer (OEM) to market, store, and ship OCM/OEM products, subject to legal conditions set by the manufacturers. Conversely, independent distributors and brokers sell parts acquired from various entities without an exclusive OCM/OEM agreement to do so. Independent distributors tend to maintain inventories and have controlled environments for parts storage. Brokers tend to be smaller firms and normally do not have inventory or controlled environments.

For this study, independent distributors and brokers are combined into a single category called “unauthorized distributors.” The term “unauthorized distributors” is not intended to imply that these companies are engaged in illicit activities, but rather that they are not party to a legal agreement to distribute OCM/OEM products. It is important to note, however, that many authorized distributors also act as unauthorized distributors to some degree, buying and selling electronic parts outside of their OCM/OEM authorized product lines to meet customer needs.

Throughout much of the electronics industry, authorized distributors have anecdotally been seen as trusted sources of supply, providing authentic parts with extremely low risk of product substitutions or counterfeits. Unauthorized distributors, however, are assumed to be more risky and have less control over the quality of the product they sell. OTE survey data shows that these preconceptions confuse the true nature of the counterfeiting problem.

Many authorized distributors assume the parts they acquire directly from OCMs are legitimate and do not require testing. However, survey data shows that some authorized distributors also assume parts purchased outside of their OCM agreements are legitimate and do not require careful screening. This practice, combined with buying back excess inventory from customers, has introduced counterfeits into the inventories of authorized distributors.

As compared to authorized distributors, unauthorized distributors are more diverse in their purchasing and screening activities. Some operations simply try to locate parts requested by customers and do not test or vet their sources for quality. Others procure parts through carefully assembled supplier lists and undertake some of the most stringent quality controls in the electronics industry. Many reputable unauthorized distributors are trying to break the preconceptions of their segment of the industry by implementing stringent procurement, testing, and auditing requirements.

Of the 98 distributors participating in the survey, 55 percent encountered counterfeit products.[17] Of these, the vast majority were unauthorized distributors. Overall, 44 of 53 unauthorized distributors encountered counterfeits, whereas only 10 of 45 authorized distributors reported encountering counterfeits (see Figure III-1).

Figure III-1: Companies Encountering Counterfeit Electronics

Type of Company	Encountered Counterfeits	Did Not Encounter Counterfeits	Total
Authorized Distributor	10	35	**45**
Unauthorized Distributor	44	9	**53**
Total	**54**	**44**	**98**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

[17] For the purposes of this assessment, the term “counterfeit part” and any variation of it, means a suspected or confirmed counterfeit part or component.

Source of Parts

Distributors were asked to identify the sources of the discrete electronic components, microcircuits, bare circuit boards, and assembled boards that they buy and sell. Based on their responses, authorized and unauthorized distributors primarily purchase discrete electronic components and microcircuits, with few dealing in bare and assembled circuit boards.

Authorized distributors receive the vast majority of their parts from OCMs and other authorized distributors (see Figure III-2). It is not uncommon, however, for authorized distributors to purchase parts outside of the OCM supply chain in order to fulfill customer requirements – 58 percent purchase parts from other sources. Specifically, 47 percent of authorized distributors procure parts from independent distributors, 29 percent procure from brokers, and 27 percent procure from Internet-exclusive sources.

Unauthorized distributors utilize a diverse range of suppliers to fulfill customer requirements, more so than authorized distributors. They primarily purchase parts from fellow independent distributors and brokers, although a large number acquire parts from OCMs, authorized distributors, and OEMs, as well.

Figure III-2: Percent of Distributors Purchasing Parts From Different Suppliers

Type of Supplier	Authorized Distributors	Unauthorized Distributors
OCMs	98%	79%
Authorized Distributors	78%	91%
Independent Distributors	47%	94%
Brokers	29%	92%
OEMs	11%	85%
Internet-Exclusive Sources	27%	58%
Contract Manufacturers	7%	66%
DOD Depots	2%	11%
DOD Manufacturing Centers	2%	9%
DOD Surplus	4%	4%
DLA	2%	2%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

CUSTOMERS FOR PARTS

Distributors, as the bridge between electronics manufacturers and part consumers, sell parts to all segments of the electronics supply chain, both in the United States and abroad. All 98 distributors surveyed sell to customers in the United States and 87 sell to non-U.S. customers. These customers are predominantly contract manufacturers, OEMs, other distributors, and prime/sub contractors. Slightly over half of distributors sell parts to individual customers and OCMs, while 32 percent sell to Internet-exclusive sources.[18]

Since U.S. Government end-users depend on electronic components for mission critical or safety applications, their use of distributors is particularly important to understand. A significant portion of authorized and unauthorized distributors sell parts to U.S. Government customers (see Figure III-3). The number of authorized and unauthorized distributors that conduct business with the U.S. Government is relatively the same.

Figure III-3: Percent of Distributors Selling Parts to U.S. Government Customers

Customer	Authorized Distributors	Unauthorized Distributors
Department of Defense	47%	42%
Other U.S. Federal Agencies	44%	40%
State/Local Governments	47%	38%
Other U.S. National Security Agencies	38%	34%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

COUNTERFEIT INCIDENTS

As stated previously, 53 percent of distributors documented at least one counterfeit incident from 2005-2008.[19] For the purposes of this study, a single incident can involve a single counterfeit part or thousands of parts. Distributors have encountered counterfeit versions of nearly every variety of discrete electronic component, microcircuit, bare circuit board, and assembled circuit

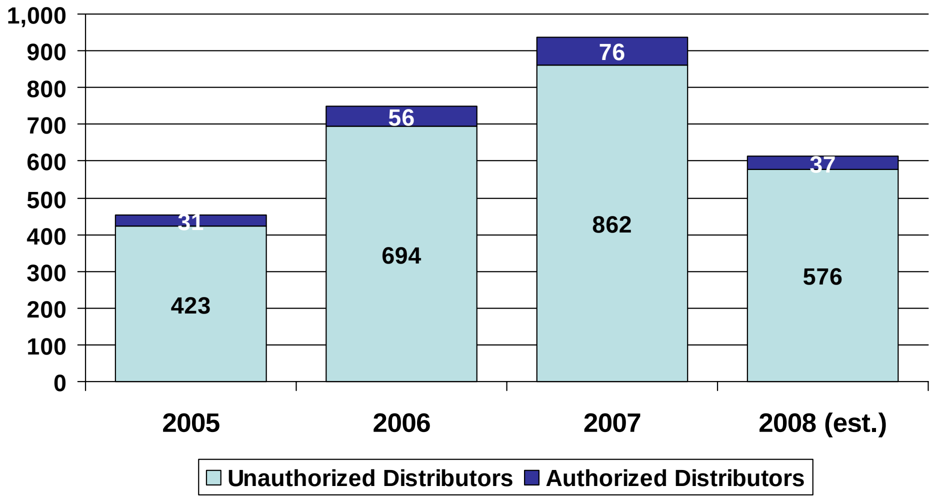
[18] See Appendix C, Figures C-1 through C-4 for a break-out of distributor customers by part type.

[19] For the purposes of this study, an incident is a single encounter of a suspected/confirmed counterfeit part. An incident could involve one part or a thousand parts of a component.

board (see Figures C-5 – C-8 in Appendix C). Multiple distributors found counterfeit versions of all types of discrete electronic components listed in the survey, of which capacitors and diodes were the most common. Distributors also found counterfeit versions of all types of microcircuits listed in the survey, of which microprocessors and memory were the most common.

From 2005 to 2007, distributors documented an increasing number of counterfeits, with incidents increasing 114 percent over the two-year period (see Figure III-4). The exact cause of this increase is unknown, but it may be a result of a variety of factors, including increased awareness about counterfeits, better documentation, more stringent testing, and/or higher levels of counterfeit activity. The decline in the number of incidents for 2008 is most likely because companies provided estimates for the year which was not over at the time the survey was conducted.

Figure III-4: Total Counterfeit Incidents - Distributors (2005 – 2008)

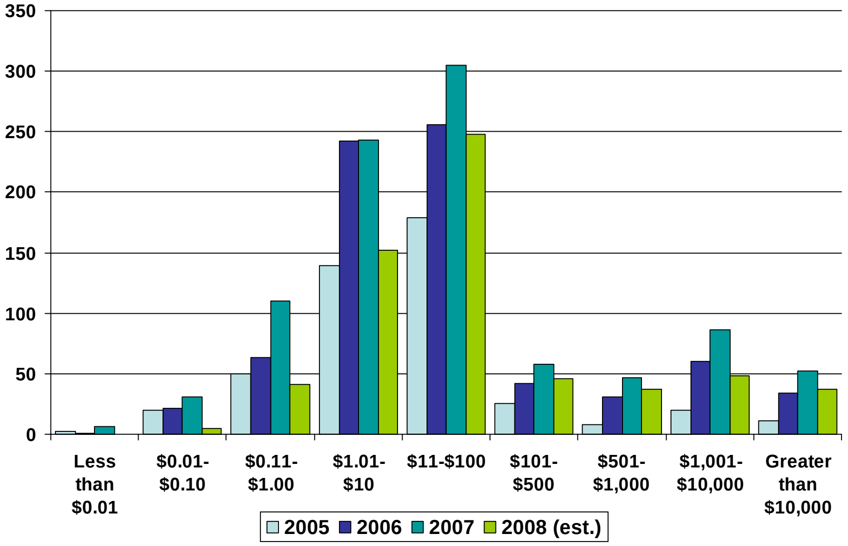


Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Unauthorized distributors encountered the vast majority of counterfeit incidents amongst all distributors surveyed. Although the total number of incidents for authorized distributors was dramatically lower in comparison, their incident rate doubled from 2005 to 2007.

A breakdown of incidents by product resale value shows that most counterfeit parts encountered by distributors were in the $1 to $100 range (see Figure III-5). This is to be expected, as survey data shows that distributors deal mostly in discrete electronic components and microcircuits, which are generally priced lower than circuit boards. Overall, counterfeit incidents increased steadily in nearly all value groups from 2005 to 2007. Thus, although the primary concentration of counterfeits has been in relatively low value parts, distributors encountered counterfeits of all prices at an increasing rate.

Figure III-5: Counterfeit Incidents by Product Resale Value - Distributors (2005 - 2008)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

TYPES OF PARTS COUNTERFEITED

Discrete electronic components and microcircuits have a wide variety of applications, from cell phones and medical equipment to navigation systems on military aircraft. Distributors have found counterfeits throughout the electronics supply chain, covering commercial, industrial, and defense applications. In the OTE survey, distributors classified the counterfeit products they encountered by their primary end-use (see Figure III-6).

Many distributors had difficulty providing this information, since components can have multiple end-uses and many distributors do not know the ultimate end-use of the parts they sell. Despite these limitations, counterfeit incidents increased in all 11 product categories listed in the survey. In addition, the product types being counterfeited have expanded over the period and shifted into higher value categories. In 2005, 71 percent of counterfeit incidents involved parts used for industrial/commercial applications. By 2008, however, counterfeits in nearly all categories had increased dramatically, causing incidents involving industrial/commercial parts to fall to 44 percent of the reported total.

Figure III-6: Type of Counterfeits Incidents - Distributors (2005-2008)

Type of Product	2005	2006	2007	2008 (est.)
Industrial/Commercial	212	422	645	499
Consumer	48	91	128	142
High Reliability – Industrial	13	32	89	136
Qualified Products List (QPL)	11	37	73	110
Qualified Manufacturers List (QML)	7	28	56	106
High Reliability – Medical	1	21	57	105
Commercial Aviation	5	10	9	16
Critical Safety	1	1	11	16
High Reliability – Automotive	2	4	3	4
ITAR Controlled	0	0	3	0
Generalized Emulation Microcircuits (GEM)	0	0	0	2

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Of particular concern is the sharp increase in counterfeit incidents of electronic parts on the Qualified Products List (QPL) and Qualified Manufacturers List (QML).[20] These parts, which are widely used in military applications, may be subject to less scrutiny when purchased by DOD

[20] According to the Federal Acquisition Regulations (FAR), the QML is “a list of manufacturers who have had their products examined and tested and who have satisfied all applicable qualification requirements for that product.” 48 C.F.R. § 9.201 The QPL is “a list of products that have been examined, tested, and have satisfied all applicable qualification requirements.” 48 C.F.R. § 2.101

entities. Therefore, an increase in QML and QPL counterfeits from 18 incidents in 2005 to 216 incidents in 2008 should be a cause for concern.

Another concern for military applications is the large number of authorized and unauthorized distributors that encountered counterfeit incidents and sold parts to the U.S. Government (see Figure III-7). While this does not mean that these companies intentionally or actually sold government agencies counterfeit parts, it highlights a higher probability of counterfeits entering U.S. Government inventories.

Figure III-7: Percent of Distributors With Counterfeit Incidents Selling Parts to U.S. Government Customers

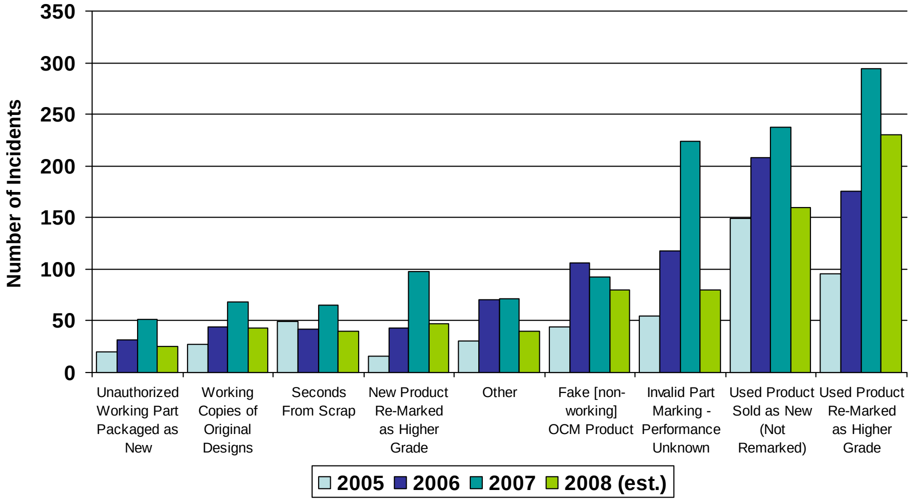
Customer	Authorized Distributors (10 Companies)	Unauthorized Distributors (44 Companies)
Department of Defense	60%	41%
Other U.S. Federal Agencies	70%	43%
State/Local Governments	60%	36%
Other U.S. National Security Agencies	60%	36%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

TYPE OF PROBLEMS AND METHOD OF DISCOVERY

Counterfeiters utilize a variety of methods to create and modify electronic components. Of the nine categories of counterfeits listed in the OTE survey, distributors encountered every type of counterfeit between 2005 and 2008 (see Figure III-8). The most frequent counterfeit parts were “re-marked as a higher grade part” or “used product that was sold as new.” There were also a large number of parts identified as counterfeit based on invalid part markings or because they were non-working fake parts.

Figure III-8: Counterfeit Incidents by Type of Problem - Distributors (2005-2008)

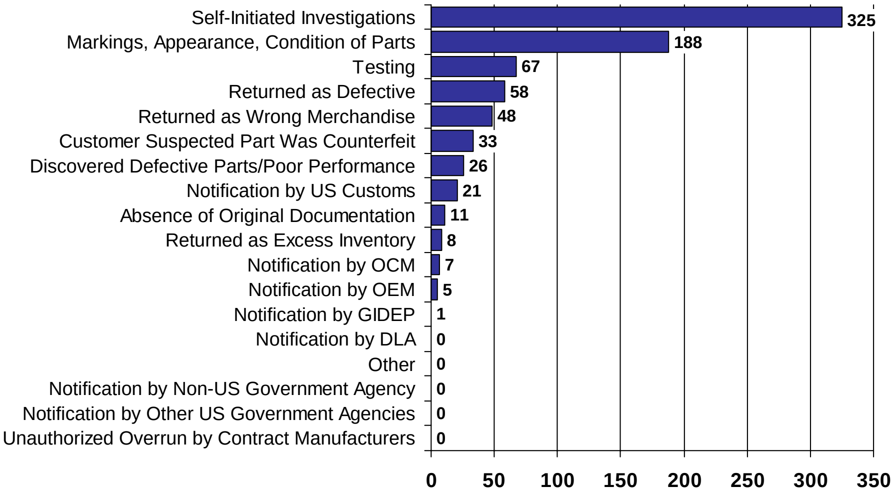


Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Distributors uncovered counterfeit components through many different methods (see Figure III-9). In most cases, they are discovered through distributors' self-initiated investigations, which increased 171 percent from 2005 to 2008. It is unclear from the data what these investigations entail. The appearance and condition of parts also helped distributors identify large numbers of counterfeits.

Conversely, distributors reported rarely uncovering counterfeits as a result of notifications from OCMs, OEMs, or U.S. Government sources, although notifications from U.S. Customs and Border Protection (CBP) have been steadily increasing. In 2005, no counterfeit incidents were uncovered as a result of a CBP notification; by 2008, 21 incidents were uncovered through this method.

Figure III-9: Counterfeit Incidents by the Method Uncovered – Distributors (2008 est.)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

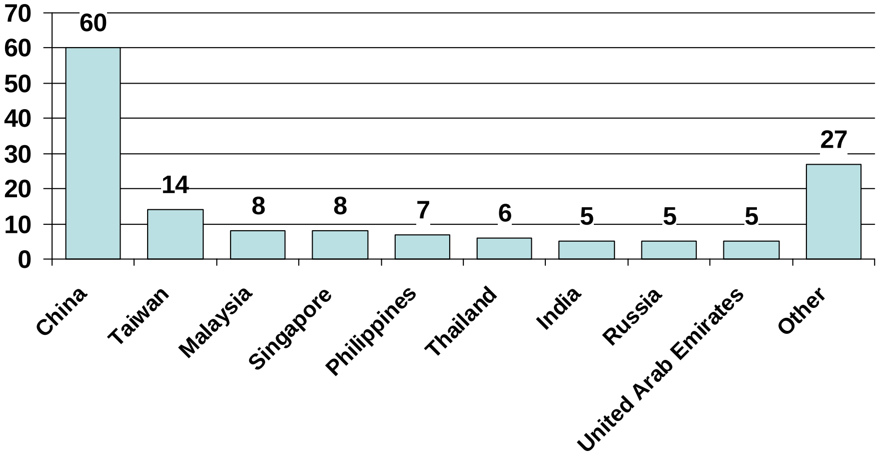
Top Countries Suspected As Sources of Counterfeits

Identifying the origin of counterfeit parts is an important step in understanding their penetration of the U.S. supply chain. Each distributor identified the top five countries suspected as a source of counterfeit parts. China was cited most often, with other Southeast Asian countries (Taiwan, Malaysia, and Singapore) also cited as top sources (see Figure III-10).[21] There were no significant changes in the countries suspected as primary sources of counterfeits between 2005 and 2008.

Interestingly, distributors cited the United States and Canada four times each as sources of counterfeits. Three distributors specifically mentioned encountering companies set up in the United States and Canada to sell parts from China in order to avoid association with parts from that region.

[21] The “Other” column in Figure III-10 is comprised of the following countries: United States, Israel, Canada, Indonesia, Vietnam, Brazil, the United Kingdom, North Korea, Pakistan, Cambodia, Germany, Czech Republic, and South Africa.

Figure III-10: Distributors' Top 10 Countries Suspected as Sources of Counterfeits (2008 est.)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

DAMAGE TO COMPANY REPUTATION

The sale of counterfeit parts, even inadvertently, can harm the business relationships between distributors and their clients. Authorized and unauthorized distributors have experienced significantly different degrees of negative effects on their company image and reputation as a result of counterfeits. Only nine percent of authorized distributors believe their reputation has been damaged as a result of counterfeits. These companies either lost key customers or had their reputation tarnished as a result of the sale of counterfeit parts.

On the other hand, 45 percent of unauthorized distributors have experienced negative effects to their reputation due to counterfeit parts. Most unauthorized distributors claim that some "unethical and/or unknowledgeable brokers" have created a "guilt by association mentality," which has tarnished the entire industry's reputation. Many unauthorized distributors have implemented quality control measures in order to separate themselves from less scrupulous distributors. Even so, they are still viewed negatively because they do not have product lines authorized by OCMs. One company stated that "although there are different levels of distributors, uneducated customers have lumped [us] with other distributors who do not have adequate controls or processes in place."

INTERNAL DATABASE TO TRACK COUNTERFEITS

Of those distributors that encountered counterfeit parts, a high percentage do not maintain an internal database to keep track of incidents (see Figure III-11). Seventy percent of authorized distributors that encountered counterfeits do not have a database to keep track of these incidents. Unauthorized distributors are much more likely to maintain a tracking database, although 34 percent of those that encountered counterfeits do not do so. Many authorized and unauthorized distributors noted that they report to industry databases rather than tracking incidents internally.

Figure III-11: Percent of Companies Who Encountered Counterfeits Who Do Not Maintain a Database to Track Counterfeit Products

Authorized Distributors	70%
Unauthorized Distributors	34%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Those companies that maintain databases track a number of different variables (see Figure III-12). The number of companies with an internal database that track each variable is high. Some distributors track "other" variables, which include product date codes, part numbers, and part images.

Figure III-12: Variables Tracked by Internal Counterfeit Database*

Variable	Authorized Distributors	Unauthorized Distributors
Suspected/Confirmed Counterfeit Products	71%	90%
Countries of Origin	71%	62%
Known/Suspected Companies and Individuals	71%	97%
Source of Reporting	57%	79%
Other	14%	31%

***Taken as a percent of those companies encountering counterfeits who maintain an internal database.**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

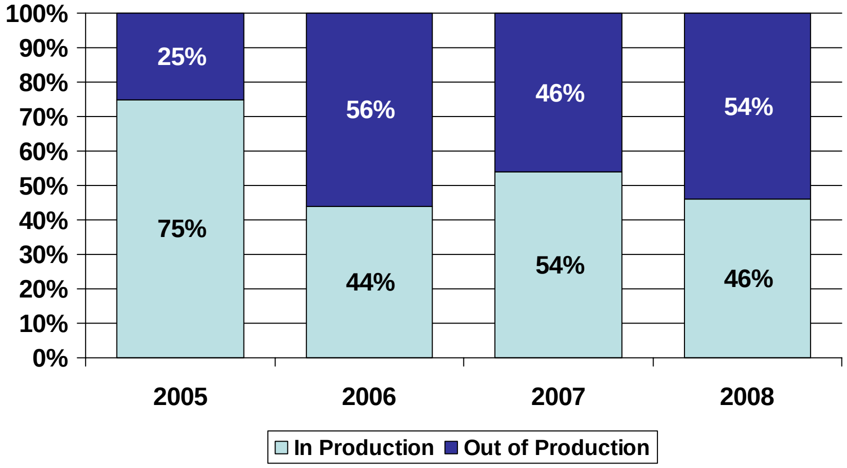
COUNTERFEIT PARTS IN/OUT OF PRODUCTION

Companies were asked to identify the percentage of counterfeit incidents that involved "in production" and "out of production" parts from 2005-2008. "In production" parts are those that are being actively produced by OCMs. Product models no longer produced by the OCM are considered "out of production."[22]

In 2005, 75 percent of counterfeits encountered by authorized distributors were "in production" parts. By 2008, the majority of counterfeit parts they encountered were "out of production" (see Figure III-13). Authorized distributors have agreements to sell active OCM products, which account for the substantial percentages of counterfeit parts that were "in production." As stated previously, however, 58 percent of authorized distributors acknowledged purchasing parts from sources other than OCMs, a practice that can bring "out of production" counterfeit parts into inventories.

[22] For this assessment, parts produced by an after-market manufacturer are considered "out of production."

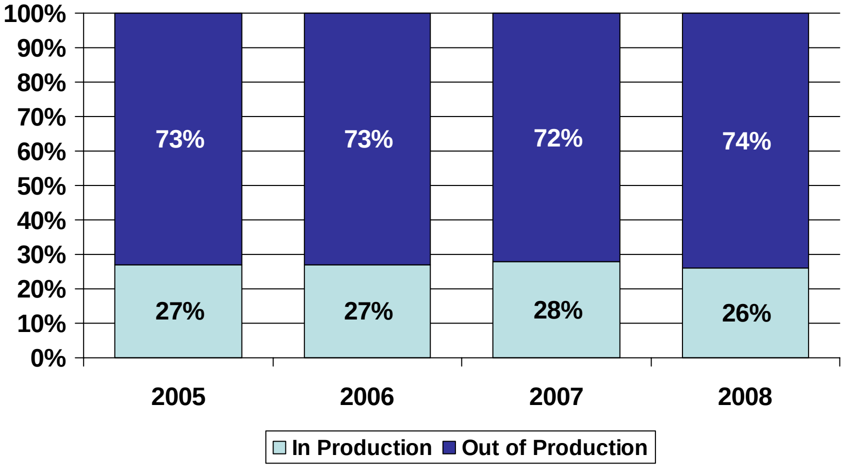
Figure III-13: Percent of Counterfeit Incidents Involving In/Out of Production Parts – Authorized Distributors (2005-2008)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Unauthorized distributors encountered considerably more counterfeit “out of production” products than authorized distributors. Over the four-year period, the split remained relatively unchanged with approximately 73 percent of counterfeit parts “out of production” and approximately 27 percent “in production” (see Figure III-14). Generally, unauthorized distributors specialize in harder to find or “out of production” parts, which explains the significantly higher percentage of “out of production” counterfeit parts encountered.

Figure III-14: Percent of Counterfeit Incidents Involving In/Out of Production Parts – Unauthorized Distributors (2005-2008)



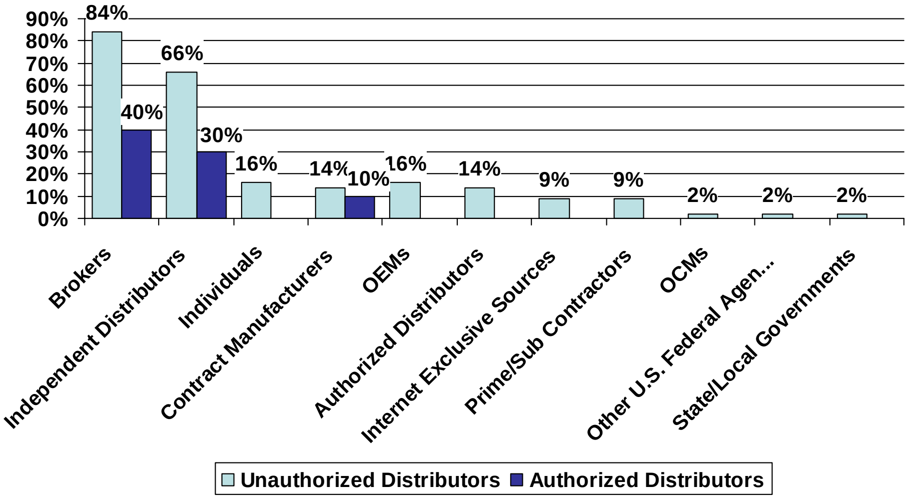
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

COUNTERFEIT PARTS SOLD BY SPECIFIC ENTITIES

Distributors identified the types of companies that were found to be sources of counterfeits (see Figure III-15). Authorized distributors primarily cited brokers (40 percent) and independent distributors (30 percent) as sources of counterfeit parts. A small percentage also mentioned contract manufacturers as sellers of counterfeits, the only other category identified by authorized distributors.

Eighty-four percent of unauthorized distributors identified brokers as a source of counterfeit components, while 66 percent identified independent distributors as having sold counterfeits. Smaller but significant percentages of unauthorized distributors also cited individuals, contract manufacturers, OEMs, and authorized distributors as sources of counterfeit components. Overall, unauthorized distributors mentioned receiving counterfeit parts from every supply chain entity listed in the OTE survey.

Figure III-15: Percent of Distributors with Cases of Counterfeit Incidents Sold by Type of Entity*



*** Only includes companies who encountered counterfeits**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

INVENTORY CONTROL AND TESTING

The way companies handle parts after receipt can determine if counterfeit components enter a company's inventory. OTE asked authorized and unauthorized distributors a series of questions in order to understand their inventory management practices.

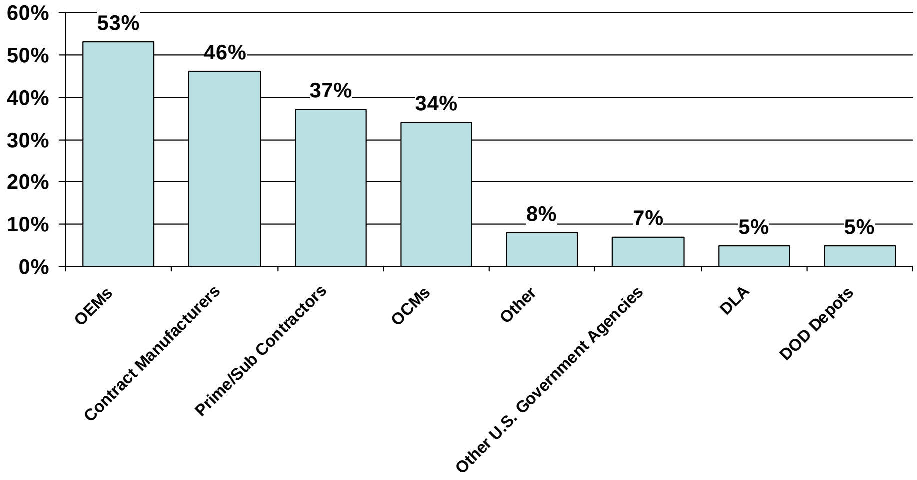
RETURN POLICIES AND RE-CIRCULATION OF PARTS

All of the distributors surveyed accept returns from their customers. While nothing is inherently wrong with this practice, returns are an avenue through which counterfeit parts can be re-circulated if screening procedures are not in place. As seen in Figure III-9, there were 106 incidents in 2008 in which customers returned "defective" or "wrong merchandise" that were found to be counterfeit product.

In addition to customer returns, many distributors buy back excess inventory from their customers. Unlike returns, buy backs of excess inventory involve purchases of products that were sold to but not utilized by the customer. Sixty-six percent of unauthorized distributors and

29 percent of authorized distributors buy back excess inventory from their customers. Authorized and unauthorized distributors most commonly buy excess inventory from OEMs and contract manufacturers, although they purchase significant amounts from many other groups (see Figure III-16).

Figure III-16: Percent of Distributors Buying Back Excess Inventory by Type of Customer



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

The danger in accepting returns and buying back excess inventory occurs when those parts are placed in inventory without inspection. Fifty-one percent of authorized distributors and 61 percent of unauthorized distributors said that they restock or re-circulate returns and buy backs (see Figure III-17). Only a small number of these distributors, however, mentioned that they require these parts to undergo quality control and screening before they are re-circulated. This is particularly important considering 16 percent of authorized distributors and 39 percent of unauthorized distributors have documented cases of individual customers returning counterfeit products.

Figure III-17: Inventory Control and Return Policies

	Authorized Distributors	Unauthorized Distributors
Accept Returns From Customers	100%	100%
Buy Back Excess Inventory From Customers	29%	66%
Restock/Re-circulate Returns or Excess Inventory From Customers	51%	61%
Have Cases of Individual Customers Returning Counterfeits	16%	39%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

PRE-STOCK TESTING

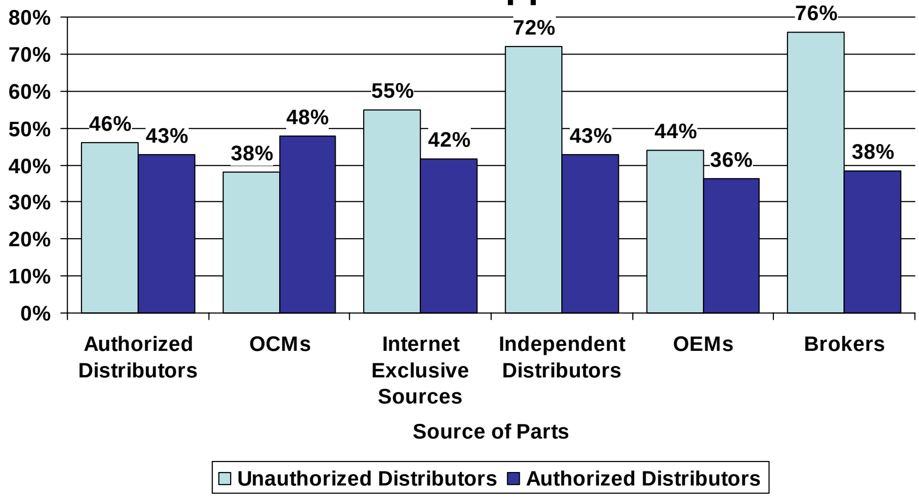
When distributors purchase electronic components, the vast majority conduct some form of testing prior to placing parts in their inventories. This can be an effective method to uncover counterfeits before shipments are forwarded to customers. Eighty-seven percent of distributors do some level of pre-stock testing, whether it is visual inspections of parts or packages, confirmation of pedigree paperwork, electronic testing, or physical evaluation.

Distributors do not hold all parts to the same standard while conducting pre-stock testing. Some distributors test based upon potential risk, subjecting product from brokers and independent distributors to more stringent levels of testing than product from OCMs or OEMs. This risk-based testing may be more cost beneficial and save time for the buyer, but it also conveys a level of trust for certain suppliers that can allow counterfeits to enter the supply chain.

Distributors were asked to indicate what percentage of parts purchased from different suppliers they tested. This information was cross-referenced with each distributor’s supplier information in order to count only those companies that procured parts from each type of supplier. Although nearly the same numbers of authorized and unauthorized distributors conduct some form of pre-stock testing, many more unauthorized distributors test parts from a wider range of their suppliers (see Figure III-18).

For example, only 38 percent of authorized distributors test the parts they buy from brokers before they stock them, while 76 percent of unauthorized distributors do the same. Similarly, 43 percent of authorized distributors conduct pre-stock testing on parts from independent distributors, while 72 percent of unauthorized distributors do so. The low levels of testing by authorized distributors are surprising considering industry concerns about the reliability of parts supplied by brokers and independent distributors. Approximately half of authorized and unauthorized distributors do not test products purchased from Internet-exclusive suppliers, which is troubling considering the potential risks involved with this type of procurement.

Figure III-18: Percent of Distributors Conducting Pre-Stock Testing on Parts From Different Suppliers*

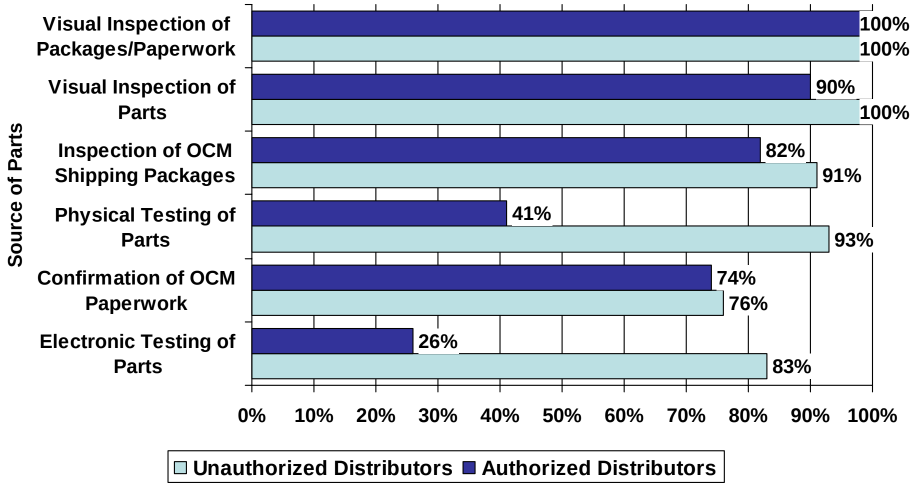


*** Only includes the companies that purchased from each supplier.**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Pre-stock testing can involve many methods, but authorized and unauthorized distributors are primarily performing different levels of visual inspection (see Figure III-19). All distributors that test parts prior to placing them in inventory perform a visual examination of the packages and paperwork, with slightly fewer visually inspecting the parts. A lesser number of companies electronically test parts before stocking them; authorized distributors, in particular, rarely go to these lengths.[23] Most pre-stock testing involves visual inspection rather than more costly, invasive electronic or physical/destructive testing.[24]

Figure III-19: Percent of Distributors Conducting Each Type of Pre-Stock Testing*



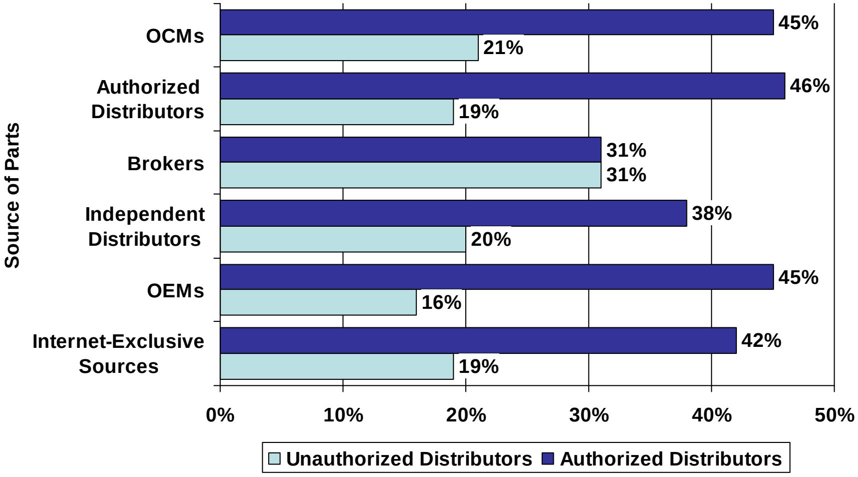
*** Percentage is taken out of the companies that do any type of pre-stock testing**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

If distributors do not test the products themselves, they may seek verification of part conformance from their suppliers. Overall, less than half of distributors require their suppliers to provide verification from testing facilities that the parts they purchased are genuine and conform to OCM performance specifications (see Figure III-20). Unauthorized distributors rarely require verification of OCM performance from their suppliers. This may be because they conduct a significant amount of internal pre-stock testing.[25] Conversely, authorized distributors are twice as likely as unauthorized distributors to require verification of the performance of parts purchased from OCMs, OEMs, Internet exclusive sources, and other authorized distributors, which may be due in part to their low levels of internal pre-stock testing.

[23] Authorized distributors may not conduct electronic testing because most of their parts are acquired from OCMs, and therefore consider such testing unnecessary.
[24] The number of distributors performing physical evaluation may be overstated because some survey respondents may have misinterpreted the term to mean a form visual inspection, rather than invasive physical examination.
[25] This data was cross-referenced to only include those distributors that purchased from each supplier.

Figure III-20: Percent of Distributors That Require Verification of OCM Performance Specifications by Testing Facilities by Type of Supplier*



*** Only includes the companies that purchased from each supplier.**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

CO-MINGLING OF INVENTORY AND AUDITING PRACTICES

Once a part is placed into inventory, it may be further scrutinized through inventory audits for counterfeits. These audits are heavily dependent upon the traceability of parts. If distributors co-mingle identical parts from different suppliers in the same bin, it may be difficult to identify part pedigree and locate all counterfeits. Twenty-three percent of unauthorized distributors and nine percent of authorized distributors co-mingle inventory. In their comments, however, many distributors state that every part is kept in its own packaging and each lot of parts receives an “individual inventory label” to maintain traceability to the part’s supplier. In these circumstances, inventory remains traceable and co-mingling does not present as great a risk.

There is a significant disparity between authorized and unauthorized distributors when it comes to inventory audits for counterfeits. While 63 percent of unauthorized distributors conduct inventory audits specifically to check for counterfeits, only 29 percent of authorized distributors do the same.

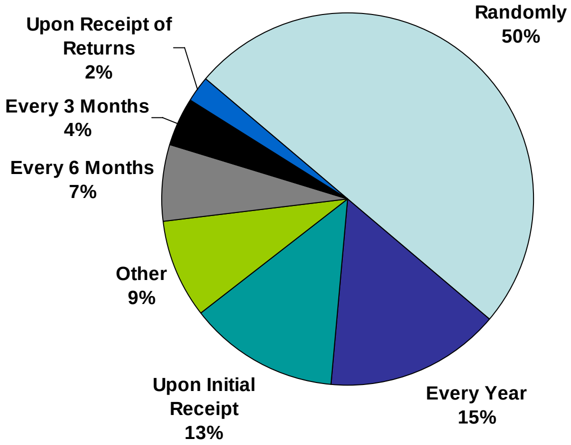
Distributors that do not audit their inventory provided a few common explanations:

- They purchase only from 'trusted sources,' namely OCMs or OEMs;
- All parts are inspected before they are stocked, "eliminating the need for inventory audits;" and
- Inventory audits are performed, but there are no specific procedures to identify potential counterfeits.

Notwithstanding valid reasons for not conducting inventory audits, survey data shows that the level of pre-stock testing undertaken by distributors may not be enough to uncover all counterfeit parts before they are placed in inventory.

Half of the 46 authorized and unauthorized distributors conducting inventory audits for counterfeits perform them on a random basis rather than at regularly scheduled intervals (see Figure III-21). Companies did not provide details as to under what conditions or how often random audits occur. Fifteen percent conduct inventory audits annually, the most commonly reported scheduled timeframe. These inventory audits are most frequently done by company staff, although 13 percent of distributors hire independent auditors.

Figure III-21: Frequency of Inventory Audits for Counterfeits – Distributors*

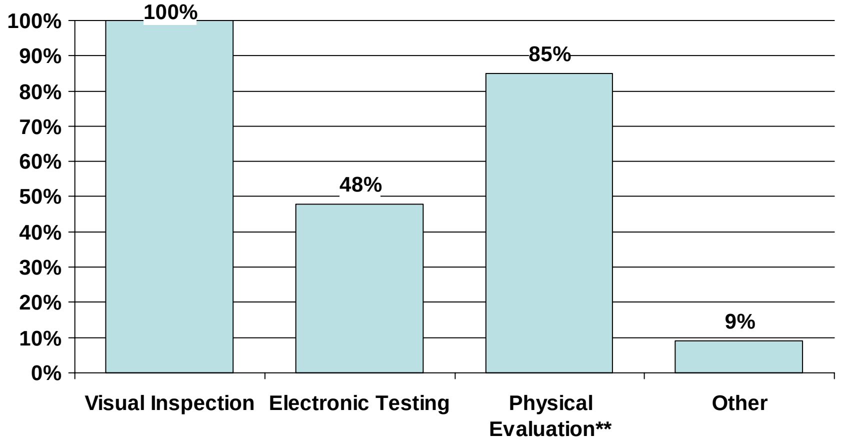


*** Only includes companies who audit their inventory for counterfeits**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Visual inspection is conducted by 100 percent of distributors performing inventory audits (see Figure III-22). Forty-eight percent go beyond visual inspection and conduct electronic testing of parts, while 85 percent said they perform physical evaluations during audits.[26]

Figure III-22: Form of Inventory Audits for Counterfeits - Distributors*



*** Only includes companies who audit their inventory for counterfeits**

**** Physical evaluation may have been misinterpreted to mean a type of visual inspection, rather than destructive testing**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

TESTING OF PARTS

Distributors identified the number of product models that were scheduled for visual inspection, electronic testing, and physical evaluation. According to survey data, authorized distributors ordered considerably less testing than unauthorized distributors in 2008 (see Figure III-23). Only 27 percent of authorized distributors ordered one or more product models to be visually inspected, whereas 62 percent of unauthorized distributors did the same. Even fewer authorized distributors ordered more comprehensive electrical or physical testing.

[26] As stated previously, the higher number of distributors conducting physical evaluation is likely due to respondents mistaking it for a form of visual inspection.

Figure III-23: Percent of Distributors Testing at Least One Product Model by Test Type in 2008

	Visual Inspection	Electronic Testing	Physical Evaluation*
Authorized Distributors	27%	9%	11%
Unauthorized Distributors	62%	57%	58%

*** Physical evaluation may have been misinterpreted to mean a type of visual inspection, rather than destructive testing**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Visual inspection is the most basic type of testing performed to authenticate parts. There are a wide range of visual criteria that companies use to detect counterfeit components. All of the distributors that conduct visual inspection examine the part number of the product (Figure III-24). Most also check trademarks and the date and place of manufacture to determine part authenticity. Beyond these, however, markedly fewer authorized distributors examine other visual criteria, particularly marking techniques, surface texture, serial number, bar codes, and covert markings. Very few distributors, especially authorized distributors, inspect embedded authenticity data in product circuitry or radio frequency identification (RFID).

Figure III- 24: Percent of Distributors Utilizing Visual Inspection Criteria*

Criteria	Authorized Distributors	Unauthorized Distributors
Part Number	100%	100%
Trademarks	81%	94%
Date of Manufacture	64%	98%
Place of Manufacture	72%	92%
Marking Techniques	58%	98%
Surface Texture	42%	98%
Serial Number	50%	86%
Bar Coding	58%	73%
Covert Markings	31%	82%
Holograms	11%	73%
Embedded Authenticity Data	8%	22%
RFID	6%	20%
Other	3%	16%

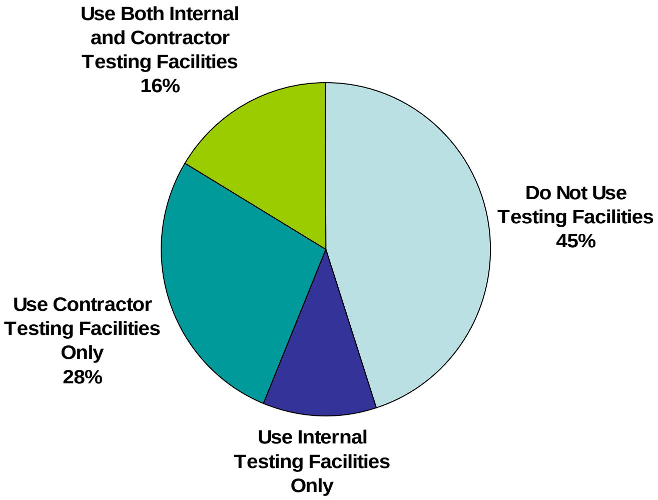
*** As a percent of companies utilizing at least one of the criteria**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Testing Facilities

Numerous companies provide outside testing services to distributors. Many authorized and unauthorized distributors also have internal facilities designed to conduct in-depth testing of the parts they purchase. Fifty-five percent of distributors utilized at least one type of testing facility to detect counterfeit products (see Figure III-25). Twenty-eight percent of distributors have counterfeit testing performed exclusively at contractor-operated testing facilities. Sixteen percent of distributors utilized both contractor-operated and internal testing facilities, while 11 percent only use internal facilities. The vast majority of these testing facilities are located in the United States.

Figure III-25: Type of Testing Facilities Utilized by Distributors



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Testing facilities do not always uncover counterfeit parts. Eighteen distributors, or 33 percent of those using testing facilities to detect counterfeits, encountered problems at U.S.-based contractor-operated facilities. Ten of these distributors had parts tested and approved by a contractor, and then sent to the customer where the parts later failed. Company comments suggest there are inconsistent standards and practices at testing facilities across the United States. One distributor described a common problem with testing facilities, stating that "one test lab actually provided test data showing [a] pass for a counterfeit product that did not pass the same test in another lab." In addition, some found outright forgeries of testing documentation where the testing facility claimed that a test was performed but was not.

Actions Taken Regarding Counterfeits

There are many actions a distributor may take if a counterfeit part is identified. Survey respondents were asked about what steps they take after becoming aware of or gaining possession of counterfeit parts, such as notifying federal authorities, taking legal action, and testing inventory.

Steps Taken After Notification of Counterfeit Parts Being Shipped

Authorized and unauthorized distributors identified very different levels of action that are taken when they are notified that they have shipped counterfeit parts (see Figure III-26).[27] These notifications can come from many different places, including testing houses, suppliers, and customers. Both types of distributors would pull back inventory, notify internal authorities, and locate select inventory in response to a counterfeit incident. However, nearly twice as many unauthorized distributors perform these steps as authorized distributors. In fact, 36 percent of authorized distributors do not take any steps after being notified of a counterfeit incident.

These distributors provided a variety of reasons for not taking any steps after being notified of a counterfeit incident. Most claim that since they have not encountered any counterfeits thus far, they do not need to put policies in place to deal with these problems. Authorized distributors, in particular, claimed that since they "work within the [authorized distribution] channel, these requirements are not an issue."

Distributors also react differently concerning information sharing related to counterfeit incidents. While 70 percent of unauthorized distributors notify industry associations about counterfeits,

[27] Some respondents answered this survey question from the perspective of what they would do if they were notified of counterfeit parts, and not what they have done.

only 29 percent of authorized distributors do the same. While information sharing may be relatively high amongst industry association members, distributors rarely notify federal authorities about the counterfeits they encounter.

Figure III-26: Steps Taken/Would be Taken After Notification of a Counterfeit Being Shipped – Distributors

Step Taken	Authorized Distributors	Unauthorized Distributors
Pull Back Inventory	44%	87%
Notify Internal Company Authorities	44%	77%
Locate Select Inventory	42%	72%
Trace Supply Chain	29%	74%
Notify Industry Associations	29%	70%
Perform Random Testing	22%	51%
Inform OCM	33%	40%
Inform Authorized Distributors	24%	38%
No Steps Are Taken	36%	2%
Notify Federal Authorities	22%	9%
Other	13%	11%
Wait for Additional Complaints	0%	9%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

The actions taken are much the same after distributors have physical possession of suspected/confirmed counterfeit parts (see Figure III-27). Forty-nine percent of authorized distributors and six percent of unauthorized distributors do not take any steps once they have possession of counterfeits.[28] When they do take action, most unauthorized distributors issue credit to their customers, enter the incident into a company database, test the part, or check industry or U.S. Government databases, while half as many authorized distributors take such actions.

Beyond these measures, 58 percent of unauthorized distributors and 20 percent of authorized distributors enter counterfeit incidents into industry or U.S. Government databases. These

[28] Some respondents answered this survey question from the perspective of what they would do if they had possession of counterfeit parts, and not what they have done.

counterfeits, however, are rarely turned over to law enforcement authorities for analysis, especially in the case of unauthorized distributors. Overall, most measures taken after the possession of counterfeit products are internal, with less focus on outside communication or information sharing with the overall industry or government authorities.

Figure III-27: Steps Taken/Would be Taken After Possession of a Counterfeit Part - Distributors

Step Taken	Authorized Distributors	Unauthorized Distributors
Issue Credit	42%	87%
Enter into Company Database	38%	83%
Test Part	36%	66%
Check Industry or USG Databases	27%	66%
Quarantine Parts	36%	47%
Retain Samples for Reference	22%	57%
Enter into Industry or USG Databases	20%	58%
Random Inventory Testing	27%	47%
Dispose of Parts Immediately	11%	49%
No Steps are Taken	49%	6%
Other	18%	21%
Turn Over to Law Enforcement Authorities For Analysis	24%	8%
Turn Over to Law Enforcement Authorities After Analysis	18%	6%
Leave Disposal Up to Person Filing Complaint	9%	13%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey,* November 2009.

DATABASES CHECKED FOR COUNTERFEIT INFORMATION

Many distributors monitor or check databases for information related to counterfeits. Eighty-five percent of unauthorized distributors check at least one database for counterfeits information, while only 36 percent of authorized distributors do the same (Figure III-28). Most distributors check ERAI's database for counterfeits information[29]. The Government-Industry Data Exchange Program (GIDEP) and the Independent Distributors Electronics Association (IDEA) databases are also utilized, but to a lesser extent.

[29] ERAI is an affiliation of electronic distributors (www.erai.com).

This disparity between authorized and unauthorized distributors is due in part to the fact that unauthorized distributors maintain databases, such as IDEA and Brokerlynx.com, that are intended exclusively for the independent distributor/brokerage industry. According to OTE survey data and research, authorized distributors do not have any information sharing networks or industry associations exclusive to their segment of the industry for counterfeit electronics.

Figure III-28: Databases Checked for Information Concerning Counterfeits*

Database	Authorized Distributors (16 companies)	Unauthorized Distributors (45 companies)
ERAI	44%	96%
GIDEP	50%	27%
IDEA	0%	42%
Other	25%	9%
FAA – AVS-20 Website	19%	7%
Brokerlynx.com	0%	7%

*** Only includes those companies checking at least one database.**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey,* November 2009.

AUTHORITIES CONTACTED AFTER COUNTERFEIT INCIDENTS

Fifty-eight percent of distributors do not know what authorities to contact when they encounter a counterfeit product. One distributor said "there are currently no known reporting methods to government agencies…only industry ones." This sentiment is clearly reflected in the data regarding the authorities that distributors with counterfeits contacted (see Figure III-29).

Based on these comments, it is not surprising that very few counterfeit incidents were reported to government authorities. From 2005 to 2008, the number of reported incidents increased, but overall remained very low.[30] In 2005, only four incidents of counterfeit products were reported

[30] See Appendix C, Figure C-9 for the number of counterfeit incidents reported to government authorities by distributors per year.

to government authorities. By 2008, 15 incidents were reported, representing only two percent of counterfeit incidents encountered by distributors that year.

Figure III-29: Authorities Notified After Counterfeit Incidents – Distributors*

None at All	65%
ERAI	13%
Independent Distributors Electronics Association (IDEA)	13%
Government-Industry Data Exchange Program (GIDEP)	11%
Customs & Border Protection (CBP)	6%
Federal Bureau of Investigation (FBI)	6%
Other	6%
State/Local Authorities	4%
Federal Trade Commission (FTC)	4%
Defense Logistics Agency (DLA)	4%
Department of Justice (DOJ)	4%
DMEA	4%
Department of Transportation (DOT)	4%

*** Only includes those companies with counterfeit incidents**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

The absence of government contact information has prompted many distributors to place the impetus on getting their money back rather than reporting incidents. One unauthorized distributor said they do "not know what to do and many times we must return the parts back to our vendor to get our money back." Another distributor said they were ignored by government authorities, claiming that numerous attempts to make contact "have fallen on deaf ears."

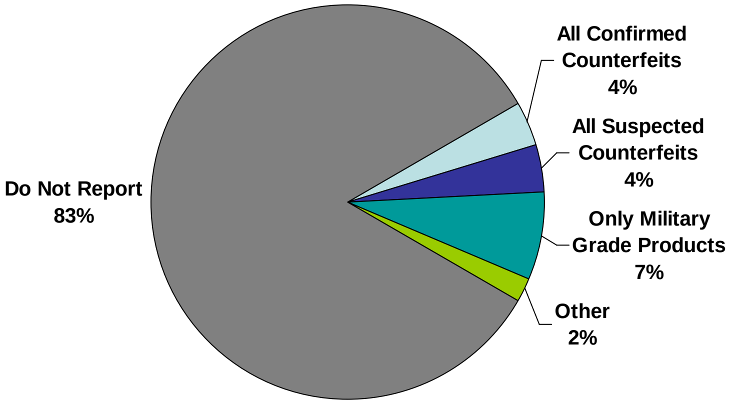
GIDEP is the main U.S. Government-supported database that tracks nonconforming products and materials, including counterfeit parts incidents.[31] Of the 54 distributors that encountered counterfeits, only nine reported incidents to GIDEP (see Figure III-30). The distributors that submit alerts to GIDEP reported a variety of counterfeits incidents.

Companies not reporting to GIDEP provided a variety of explanations as to why they decided not to do so. Nearly half of non-reporters were not aware of GIDEP or its function. One distributor explained that they "would be happy to participate if we were aware of these

[31] "Government-Industry Data Exchange Program," Defense Standardization Program Journal, Jan/Mar 2008.

programs." This sentiment was echoed by other respondents. Other companies indicated their counterfeit issues were not a large enough issue for them to report to GIDEP.

Figure III-30: Level of Reporting to GIDEP for Distributors Encountering Counterfeits



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Distributors also have to work with their customers to deal with counterfeit components that were sold to them. In case of a problem, 77 percent of distributors tell their customers to notify their company in the event of a counterfeit incident (see Figure III-31). Most companies do not instruct their customers to contact any government or industry authority. Another 16 percent of distributors do not provide any guidance to their customers on how to respond in the event of a counterfeit incident.

Figure III-31: Authorities Customers are Told To Contact in Case of Counterfeit Incidents

My Company (Survey Respondent)	77%
None	16%
Government-Industry Data Exchange Program (GIDEP)	9%
State/Local Authorities	8%
Customs & Border Protection (CBP)	6%
DMEA	5%
ERAI	5%
IDEA	4%
Defense Logistics Agency (DLA)	4%
Department of Energy (DOE)	4%
Federal Bureau of Investigation (FBI)	4%
Federal Trade Commission (FTC)	4%
Department of Justice (DOJ)	4%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Legal Guidance and Liabilities

Distributors were asked various questions related to their awareness of legal liabilities and guidance related to counterfeit products. Only 21 percent of distributors claim they are aware of any legal requirements for the management and/or disposal of counterfeit parts. A higher number of distributors (38 percent) indicated awareness of their liabilities related to the distribution, storage, and disposal of counterfeit parts.

Overall, 19 percent of distributors are aware of written instructions or guidance from federal authorities on reporting counterfeit products, although none were specifically cited. The majority of distributors (58 percent) reported that they need guidance from federal authorities regarding civil and criminal liabilities and penalties related to distribution, storage and disposal of suspected counterfeit parts.

Reporting to Industry Associations

As previously indicated, distributors report counterfeits to industry associations at a much higher rate than they report to government agencies. Those authorized distributors that report do so to a wide range of associations, the most common being the National Electronic Distributors

Association (see Figure III-32). Unauthorized distributors, on the other hand, primarily contact ERAI and IDEA. Fifty-six percent of authorized distributors and 23 percent of unauthorized distributors do not report counterfeit incidents to any industry groups.

Figure III-32: Percent of Distributors Reporting to Industry Associations

Industry Association	Authorized Distributors	Unauthorized Distributors
ERAI	11%	68%
Do Not Notify Industry Organizations	56%	23%
Independent Distributors Electronics Association (IDEA)	7%	59%
National Electronic Distributors Association	20%	4%
Other	4%	2%
Electronic Industries Association	9%	4%
Semiconductor Industry Association (SIA)	7%	2%
Brokerlynx.com	0%	8%
Alliance for Gray Market & Counterfeit Abatement (AGMA)	4%	4%
Aerospace Industries Association (AIA)	4%	2%
Government Electronic Industries Association	4%	0%
U.S. Chamber of Commerce	2%	2%
Quality Brands Protection Committee (Chinese Government)	2%	0%
Electronic Components, Assemblies & Materials Association	2%	0%
National Association of Manufacturers	2%	0%
Association of Connecting Electronic Industries (IPC)	2%	0%
Society of Automotive Engineers	2%	0%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey,* November 2009.

Difficulty Identifying Counterfeits

Considering documented increases in the frequency and sophistication of counterfeit activity, distributors were asked whether or not they found it difficult to identify counterfeit parts. Distributors were almost evenly split, with 46 percent finding identification difficult and 54 percent not having difficulties.

Authorized distributors that do not find it difficult to identify counterfeits believe the risk inherent in the authorized supply chain is low, since they purchase directly from manufacturers or other authorized suppliers. They believe this practice reduces/eliminates the chance for counterfeit penetration. These distributors also said they demand certificates of conformance from their suppliers to ensure the traceability of parts.

Unauthorized distributors not having difficulty identifying counterfeits have a different perspective than that of authorized distributors. They attribute their success to robust incoming testing procedures and advanced equipment, such as x-ray and de-capsulation machines. In particular, these distributors emphasized the importance of a highly trained staff who are well versed in types of counterfeits and methods of testing. In addition, many unauthorized distributors have confidence that adhering to the IDEA 1010-A standard will help identify counterfeits before they get to customers.[32]

Authorized distributors having difficulty identifying counterfeits cited testing techniques as a key reason. Many do not have any protocols for identifying counterfeits beyond packaging and documentation. These authorized distributors also admitted it is "difficult to identify counterfeit parts via visual inspection" and do not perform any electronic or destructive testing.

Those unauthorized distributors having difficulty identifying counterfeits point to the increased efficiency of counterfeiters in disguising parts. Better marking and finishing techniques on the part of counterfeiters has made identifying parts with traditional methods, such as chemical washing, increasingly difficult.[33] They also emphasize that the only way to confirm part authenticity is through expensive and time-consuming electrical testing, which some say they cannot afford. Finally, one distributor said that OCMs are "generally not supportive in providing sufficient quality and technical data" to unauthorized distributors, making it more difficult to verify part authenticity.

To understand how distributors have coped with counterfeits, survey respondents were asked whether or not they were better able to control the infiltration of counterfeits today as opposed to five years ago. Seventy-nine percent of distributors were better able to control counterfeits, but many emphasized the task's inherent difficulty.

[32] IDEA Standard 1010-A specifically deals with inspection procedures and has a section on unacceptable characteristics for electronic components. More information on this standard is available at http://www.idofea.org/products.

[33] A chemical wash involves rubbing the surface of a part with acetone or a similar chemical to test the authenticity of a part's markings. If the markings come off during the wash, the part is likely counterfeit.

Authorized distributors that have made progress controlling counterfeit infiltration credited better incoming inspection procedures and documentation requirements. More of these companies are requiring in-depth visual inspections of discrete electronic components, microcircuits, and bare and assembled circuit boards than they did five years ago. Awareness of the problem has also increased through training and the number of industry organizations created to combat counterfeits.

Unauthorized distributors emphasized the importance of advanced inspection equipment in identifying counterfeit products, particularly de-capsulation and x-ray machines. Increased use of the Internet and photograph databases has also allowed companies to access more information previously unavailable. In addition, many unauthorized distributors have altered procurement practices by creating trusted supplier lists and eliminating suppliers from regions with high counterfeiting activity, particularly Asia.

Most authorized distributors that are not better able to control counterfeits have not altered their inspection procedures from five years ago and have not encountered any counterfeits. Unauthorized distributors that have the same issue say that the increased volume and complexity of the counterfeit products have actually increased their counterfeit problem over the past five years.

Reasons for Counterfeits Entering the U.S. Supply Chain

Distributors provided their opinion of the prime reasons why counterfeit products are entering the U.S. supply chain (see Figure III-33). There were a wide range of responses, but most distributors pointed to less stringent inventory management and greater reliance on gray market parts by unauthorized distributors.[34] Many companies also identified the insufficient chain of accountability within the electronics supply chain as well as inadequate part purchase planning by OEMs and contract manufacturers.

[34] A gray market is the trade of parts through distribution channels which, while legal, are unofficial, unauthorized, or unintended by OCMs.

Figure III-33: Distributors' Top Ten Reason For Counterfeits Entering the Supply Chain

Less stringent inventory management by parts brokers	58%
Greater reliance by brokers on gray market parts	52%
Greater reliance by independent distributors on gray market parts	49%
Insufficient buying procedures	48%
Less stringent inventory management by independent distributors	47%
Insufficient chain of accountability	46%
Inadequate part purchase planning by OEMs	44%
Inadequate part purchase planning by contract manufacturers	44%
Greater reliance by OEMs on gray market parts	39%
Insufficient inventory control	39%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

A number of distributors provided reasons for the penetration of counterfeits beyond those included in the survey. One authorized distributor said that OCMs "create shortages by minimizing production," creating opportunities for counterfeiters to sell fake parts to those looking for a cheap product. Other unauthorized distributors blamed law enforcement officials for not pursuing companies that sell counterfeits through various Internet sites and search engines.

Another reason provided by respondents was the inability/unwillingness of companies to remove counterfeit products or electronic waste from the supply chain.[35] On this point, one unauthorized distributor said the focus on simply getting refunds for non-working products keeps counterfeits in the supply chain. Counterfeits are often returned to their source and re-sold, rather than being destroyed or turned over to law enforcement. Many distributors also cited insufficient or ineffective steps taken by foreign governments to disrupt counterfeiting operations within their borders, where many alleged counterfeiters are located. The shipment of electronic waste to China for disposal was also cited as a problem; electronic waste has turned into an abundance of discrete electronic components and microcircuits for counterfeit parts.

[35] Electronic waste, or e-waste, are products that have been discarded or disposed of after use. Often times this electronic waste is exported and stripped for parts rather than destroyed.

INTERNAL ACTIONS TAKEN TO PREVENT INFILTRATION OF COUNTERFEITS

Most distributors take some internal actions in order to prevent the infiltration of counterfeits into their inventory (see Figure III-34). Eighty-five percent of unauthorized distributors and 64 percent of authorized distributors are revising procedures to more carefully evaluate returns from customers and related restocking/re-circulation. The second most common internal action taken has been to increase training for staff concerning the negative economic and safety impacts of counterfeits. Very few distributors are performing screening and testing on inventory to check for counterfeit products already within their supply.

However, 31 percent of authorized distributors and nine percent of unauthorized distributors are not taking any internal actions to prevent the infiltration of counterfeits. Five of these companies, four authorized distributors, and one unauthorized distributor, have encountered counterfeits in the past. These companies did not provide a rational for not taking any such precautions.

Figure III-34: Internal Actions Taken to Prevent Infiltration of Counterfeits - Distributors

	Authorized Distributors	Unauthorized Distributors
Revising procurement procedures to more carefully screen/audit/evaluate authorized returns from customers	64%	85%
Training staff on the negative economic and safety impacts of counterfeit products	42%	85%
Revising company procedures for disposal of "seconds," defective parts, and production overruns	31%	55%
No internal actions taken	31%	9%
Other	9%	15%
Embedding new security measures in existing product lines	11%	9%
Performing screening and testing on inventory	7%	9%
Adding security markings to existing inventory	4%	4%

Source: U.S. Department of Commerce, Office of Technology Evaluation,
Counterfeit Electronics Survey, November 2009.

External Actions Taken to Prevent Infiltration of Counterfeits

In addition to internal actions, distributors were asked about actions taken externally to prevent the infiltration of counterfeits into the supply chain (see Figure III-35). Most of those taking preventative steps are educating customers about the risks of gray market products and the negative impact of counterfeits. Four distributors are also working with ERAI, IDEA, and/or the NEDA to coordinate industry-wide anti-counterfeiting efforts.

Overall, very few distributors made an effort to control counterfeits externally, based on the list of eight actions that were provided. Forty-two percent of authorized distributors and 17 percent of unauthorized distributors do not take any external actions related to counterfeits. Of these, 10 have encountered counterfeit incidents in the past.

Figure III-35: External Actions Taken to Prevent Infiltration of Counterfeits - Distributors

	Authorized Distributors	Unauthorized Distributors
Educating customers about risks associated with gray market products	47%	66%
Educating customers on the negative economic and safety impacts of counterfeit products	36%	66%
Referring customers to companies that could identify suitable substitute products or re-engineer system components	31%	28%
No external actions taken	42%	17%
Referring customers to authorized after-market manufacturers	27%	17%
Tightening contractual obligations of contract manufacturers with regard to disposal of “seconds,” defective parts, and overruns	13%	9%
Prohibiting authorized distributors from buying back excess inventory on the gray market	20%	2%
Other	4%	6%
Prohibiting authorized distributors from buying back excess inventory from their customers	11%	0%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Overall, distributors represent an extremely diverse segment of the electronics industry with varying levels of supply chain security and quality control procedures. Authorized distributors generally trust their procurement practices without a great deal of testing since they obtain most of their inventory from OCMs. However, many seemingly apply the same level of trust to the inventory they procure from other suppliers. Unauthorized distributors are mixed in their practices, but are generally more proactive in regards to testing and sharing information with industry. Despite this, many unauthorized distributors simply procure and sell parts without quality controls or maintaining part traceability, contributing to the negative stigmas that permeate their sector. Distributors need to continue to develop and/or implement testing procedures and standards, increase part traceability, and increase reporting to government authorities.

IV. Circuit Board Assemblers

Circuit board assemblers provide an important service within the electronics supply chain. At a basic level, they integrate discrete electronic components, microcircuits, and small assembled circuit boards onto bare circuit boards used by their customers to create subsystems and systems for a variety of applications. Because assemblers purchase large quantities of electronic parts and manufacture electronic products, OTE surveyed this segment of the supply chain to gain perspective on their encounters with counterfeit electronics. In total, 32 circuit board assemblers were included in the final results.

Of the 32 circuit board assemblers surveyed, 34 percent encountered counterfeit electronic parts to some degree (see Figure IV-1).[36]

Figure IV-1: Companies Encountering Counterfeit Electronics

Type of Company	Encountered Counterfeits	Did Not Encounter Counterfeits	Total
Circuit Board Assembler	11	21	**32**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Source of Parts

Circuit board assemblers identified the types of parts (discrete electronic components, microcircuits, bare circuit boards, and assembled circuit boards) they buy and type of suppliers used to purchase them. Based on their responses, these companies primarily purchase discrete electronic components, microcircuits, and bare circuit boards, although many also purchase assembled circuit boards (see Appendix D, Figures D-1 through D-4).

[36] For the purposes of this assessment, the term "counterfeit part" and any variation of it, means a suspected or confirmed counterfeit part or component.

According to survey data, circuit board assemblers primarily purchase parts from authorized distributors, original component manufacturers (OCMs), and independent distributors (see Figure IV-2). More than half of circuit board assemblers (66 percent) purchase electronic parts from original equipment manufacturers (OEMs) and a significant percentage (28 percent) purchase from sources operating exclusively on the Internet. Only one circuit board assembler acquired parts from Department of Defense (DOD) organizations, specifically the Defense Logistics Agency (DLA).

Figure IV-2: Percent of Circuit Board Assemblers Purchasing Parts From Different Suppliers

Type of Supplier	Percent of Circuit Board Assemblers
Authorized Distributors	97%
OCMs	91%
Independent Distributors	88%
OEMs	66%
Internet-Exclusive Sources	28%
Contract Manufacturers	9%
Brokers	9%
DLA	3%
DOD Depots	0%
DOD Manufacturing Centers	0%
DOD Surplus	0%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

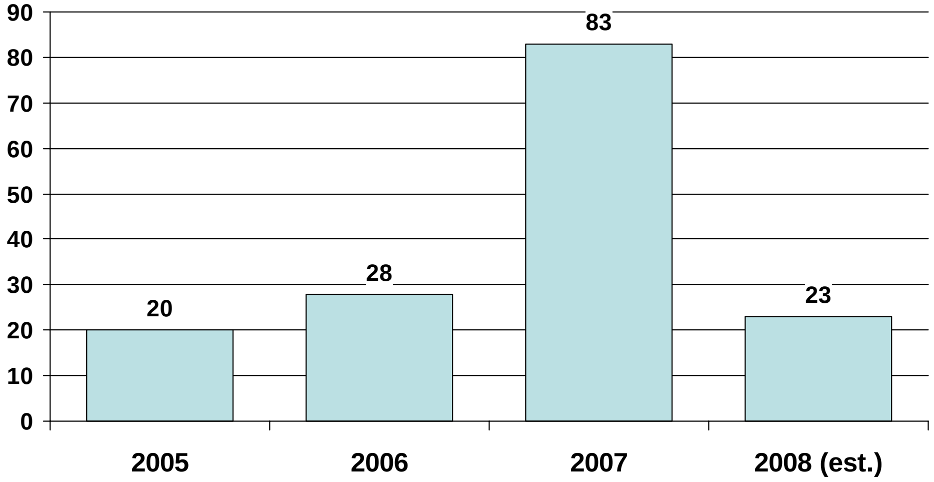
COUNTERFEIT INCIDENTS

Companies were asked to identify the number of counterfeit incidents they encountered from 2005 to 2008.[37] As indicated previously, 34 percent of circuit board assemblers (11 companies) encountered counterfeit electronic components. During the reporting period, these companies encountered numerous types of counterfeit discrete electronic components, microcircuits, and assembled circuit boards (see Figures D-5 through D-7 in Appendix D).

[37] For the purposes of this study, an incident is a single encounter of a suspected/confirmed counterfeit part. An incident could involve one part or a thousand parts of a component.

For the most part, circuit board assemblers encountered a relatively steady level of counterfeits from 2005 to 2008 (see Figure IV-3). In 2007, however, one company reported 50 separate incidents of counterfeit electronic components, skewing the totals for that year. The cause of this spike is unknown, but it may be a result of a variety of factors such as increased awareness, better documentation, more stringent testing, and/or higher levels of counterfeit activity. Overall, circuit board assemblers did not document a high number of counterfeit incidents relative to other sectors of the electronics supply chain.

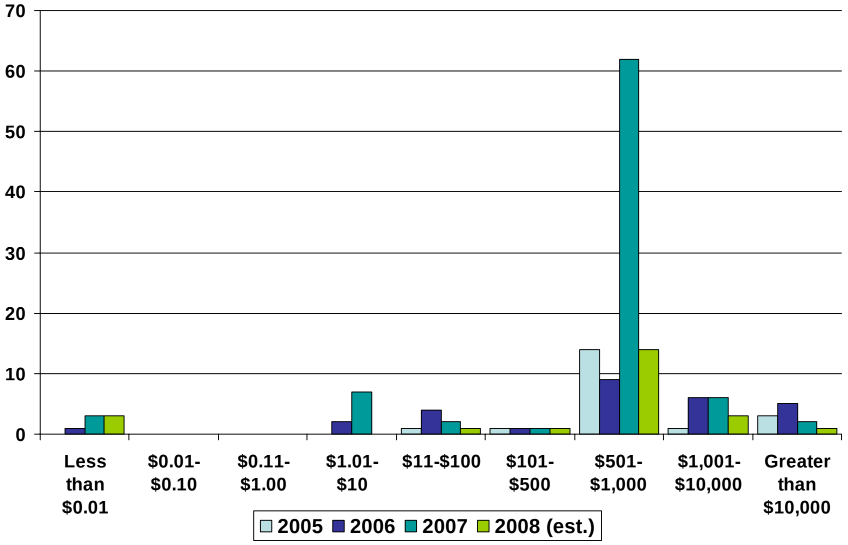
Figure IV-3: Total Counterfeit Incidents - Circuit Board Assemblers (2005 – 2008)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

A breakdown of incidents by product resale value over the 2005-2008 period shows that most counterfeits encountered by circuit board assemblers cost between the $501 to $1,000 (see Figure IV-4). Once again, the large increase in incidents in 2007 within this pricing range can be attributed to one company. Circuit board assemblers uncovered counterfeit versions of more expensive parts partially as a result of their experiences with counterfeit assembled circuit boards, as opposed to cheaper discrete components and microcircuits.

Figure IV-4: Counterfeit Incidents by Product Resale Value - Circuit Board Assemblers



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

TYPE OF PARTS COUNTERFEITED

Circuit board assemblers identified counterfeit parts throughout the electronics supply chain for commercial, industrial, and defense applications. These components have a wide variety of applications, from cell phones and medical equipment to navigation and weapon systems on military aircraft. In the OTE survey, circuit board assemblers were asked to classify the counterfeit products they encountered by their primary end-use (see Figure IV-5).

Some companies had difficulty providing this information, since many components have multiple end-uses and many assemblers do not know the ultimate end-use of the circuit boards they sell. Despite these limitations, some trends were apparent in the survey data. Circuit board assemblers encountered a high number of counterfeit components controlled under the International Traffic in Arms Regulations (ITAR), industrial/commercial parts, and parts on the

Qualified Manufacturers List (QML). ITAR-controlled and QML components are used primarily in military applications and may be subject to less scrutiny when purchased.[38]

Figure IV-5: Type of Counterfeit Incidents - Circuit Board Assemblers (2005-2008)

Type of Product	2005	2006	2007	2008 (est.)
ITAR Controlled	14	9	59	8
Industrial/Commercial	10	11	31	8
Qualified Manufacturers List (QML)	7	4	34	9
High Reliability – Industrial	0	1	4	3
Qualified Products List (QPL)	2	1	2	1
Critical Safety	1	2	2	1
High Reliability – Medical	0	3	1	0
Consumer	1	0	0	0
Commercial Aviation	0	0	0	0
High Reliability – Automotive	0	0	0	0
Generalized Emulation Microcircuits (GEM)	0	0	0	0

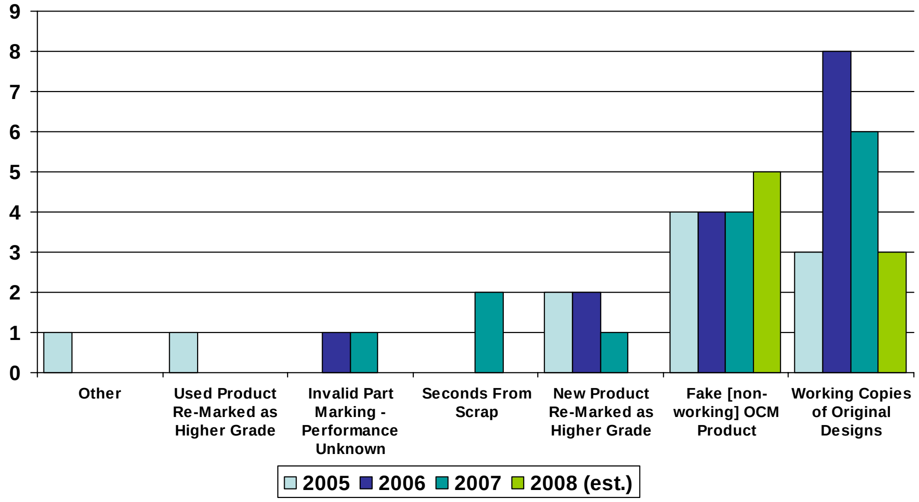
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

TYPE OF PROBLEMS AND METHOD OF DISCOVERY

Counterfeiters utilize a plethora of methods to create and modify electronic components. Circuit board assemblers primarily encountered “working copies of original designs” and “fake [non-working] OCM product” (see Figure IV-6). Counterfeit components that are working copies of genuine parts can be particularly dangerous because while they might not fail upon installation, they may fail under stressful conditions, such as high temperatures or exposure to radiation.

[38] According to the Federal Acquisition Regulations (FAR), the QML is “a list of manufacturers who have had their products examined and tested and who have satisfied all applicable qualification requirements for that product.” 48 C.F.R. § 9.201 The QPL is “a list of products that have been examined, tested, and have satisfied all applicable qualification requirements.” 48 C.F.R. § 2.101

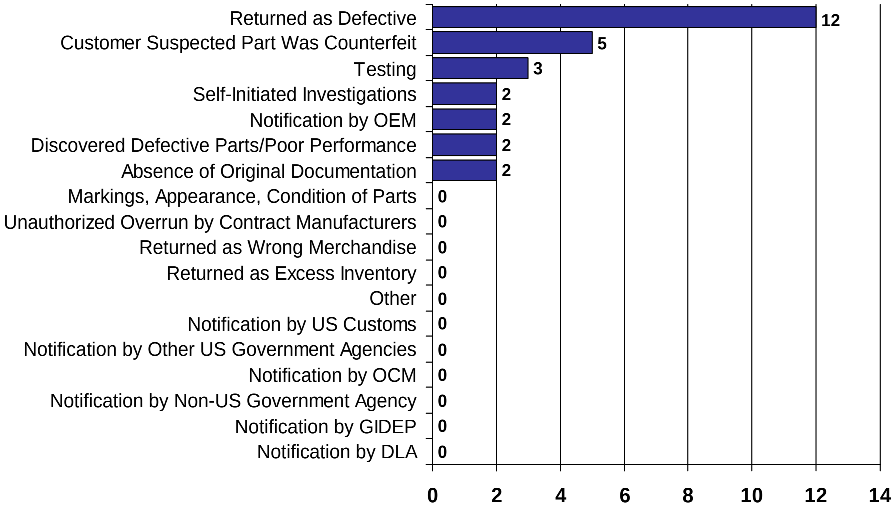
Figure IV-6: Counterfeit Incidents by Type of Problem (2005-2008)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Likewise, many circuit board assemblers did not keep detailed records of how they uncovered counterfeit parts, either through company purchases or returns by customers. From 2005 to 2008, assemblers identified counterfeit parts purchased primarily through inconsistencies in the markings, appearance, or condition of parts, as well as through testing (see Figure IV-7). During the same period, circuit board assemblers did not learn of any counterfeits they purchased as a result of notifications from any U.S. Government agencies.

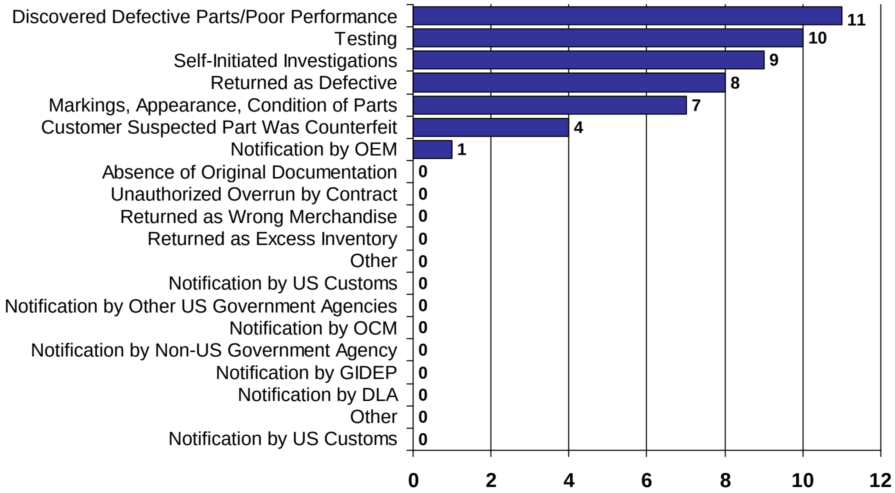
Figure IV-7: Purchased Counterfeits by the Way Uncovered – Circuit Board Assemblers (2005-2008)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Limited record keeping was also apparent in how companies uncovered counterfeits of products they manufactured. During the 2005-2008 period, customers or end-users most often returned products as defective. In addition, some assemblers identified counterfeits in manufactured products upon testing (see Figure IV-8). Over the same four-year period, assemblers were not aware of any notifications of counterfeit versions of their manufactured products from U.S. Government agencies.

Figure IV-8: Manufactured Products Counterfeited by the Way Uncovered - Circuit Board Assemblers (2005-2008)



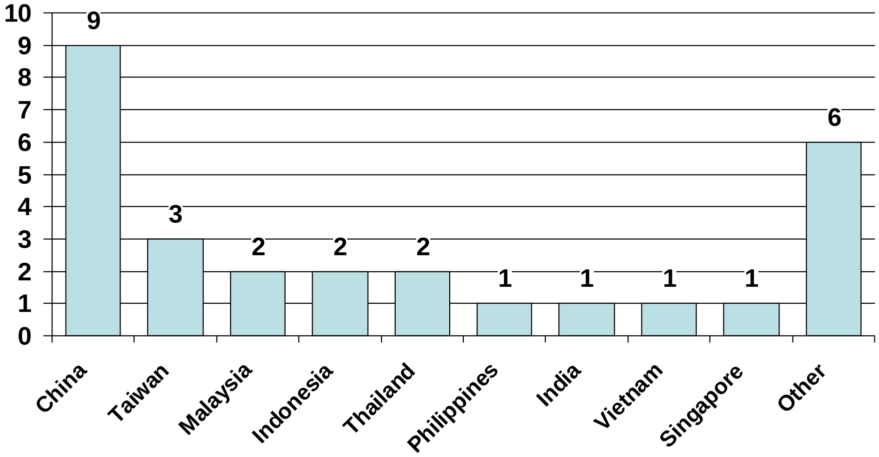
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Top Countries Suspected As Sources of Counterfeits

Identifying the origin of counterfeit parts is a key step toward mitigating their infiltration into the U.S. supply chain. Each assembler was asked to identify the top five countries suspected as a source of counterfeit parts. China was the country cited most often by respondents, with Southeast Asia as the main regional source (see Figure IV-9).[39] There were no significant changes in the top countries suspected as sources of counterfeits between 2005 and 2008.

[39] The "Other" column in Figure IV-9 is comprised of the following countries: the United States, Cambodia, Haiti, Jordan, Mexico, and North Korea.

Figure IV-9: Circuit Board Assemblers' Top 10 Countries Suspected as Sources of Counterfeits (2008 est.)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

DAMAGE TO COMPANIES' REPUTATION

The sale of products containing counterfeit parts, even inadvertently, can harm circuit board assemblers' relationships with their clients. Only two companies, however, believed their reputations have been negatively affected by counterfeits. These companies inadvertently passed on products with counterfeit parts to customers, prompting investigations and recalls. Companies that have not had issues with their reputations mostly credit their lack of experience with counterfeit parts.

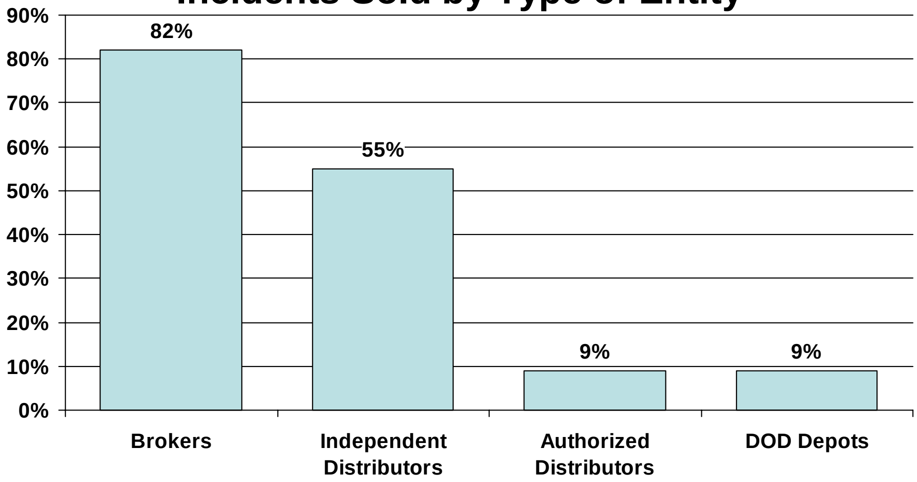
INTERNAL DATABASE TO TRACK COUNTERFEITS

Nine of the 11 circuit board assemblers that encountered counterfeits do not maintain an internal database to record incidents. Without a formal tracking system in place, these companies have no way to identify trends or problems with counterfeits that may arise over time. So, although there were only a small number of counterfeit incidents reported by circuit board assemblers in the OTE survey, most do not keep detailed records to accurately report their exposure.

Counterfeit Parts Sold by Specific Entities

Circuit board assemblers were asked to identify entities that sold them counterfeit parts (see Figure IV-10). Circuit board assemblers that encountered counterfeit parts said brokers and independent distributors were the most common supply sources of counterfeits. A few assemblers received counterfeits from authorized distributors and DOD depots.

Figure IV-10: Percent of Circuit Board Assemblers with Cases of Counterfeit Incidents Sold by Type of Entity*



*** Only includes companies who encountered counterfeits**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Inventory Control and Testing

The actions taken by circuit board assemblers once they have obtained and placed parts into their inventories can affect the risk of counterfeit parts continuing through the supply chain. To better understand the behaviors and risks, circuit board assemblers were asked a series of questions relating to their inventory control and testing procedures.

Return Policies and Re-circulation of Parts

Eighty-four percent, or 27 of the 34 circuit board assemblers surveyed, accept returns from their customers (see Figure IV-11). Although a rational business practice, returns are a potential avenue through which counterfeit parts enter the supply chain if not carefully tested before placed in inventory.

Figure IV-11: Inventory Control and Return Policies

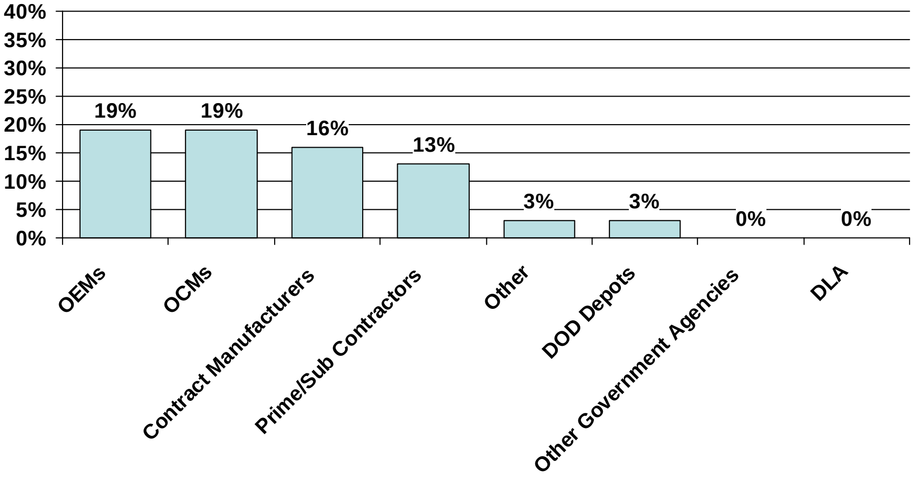
	Circuit Board Assemblers
Accept Returns From Customers	84%
Buy Back Excess Inventory From Customers	16%
Restock/Re-circulate Returns or Excess Inventory From Customers	13%
Have Cases of Individual Customers Returning Counterfeits	3%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Sixteen percent of circuit board assemblers buy back excess inventory from their customers. Unlike returns, buy backs of excess inventory are purchases of products that were sold to but not utilized by the customer. Circuit board assemblers most commonly buy excess inventory from OEMs and OCMs, although they purchase significant amounts from many other groups (see Figure IV-12).

As stated before, the risk in taking returns and buying back excess inventory occurs if those parts are placed into inventory without inspection, as non-authentic parts can be returned in lieu of legitimate product. Thirteen percent of circuit board assemblers restock or re-circulate parts once accepted back. Only a small number of assemblers require these parts to undergo quality control screening before they are re-circulated.

Figure IV-12: Percent of Circuit Board Assemblers Buying Back Excess Inventory by Type of Customer



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

PRE-STOCK TESTING

Testing components prior to placing them in inventory can be an effective method to discover counterfeits before they are incorporated into circuit boards and sent to customers. Seventy-two percent of assemblers conduct some level of pre-stock testing, whether visual inspection of parts or packages, confirmation of pedigree paperwork, electronic testing, or physical evaluation.

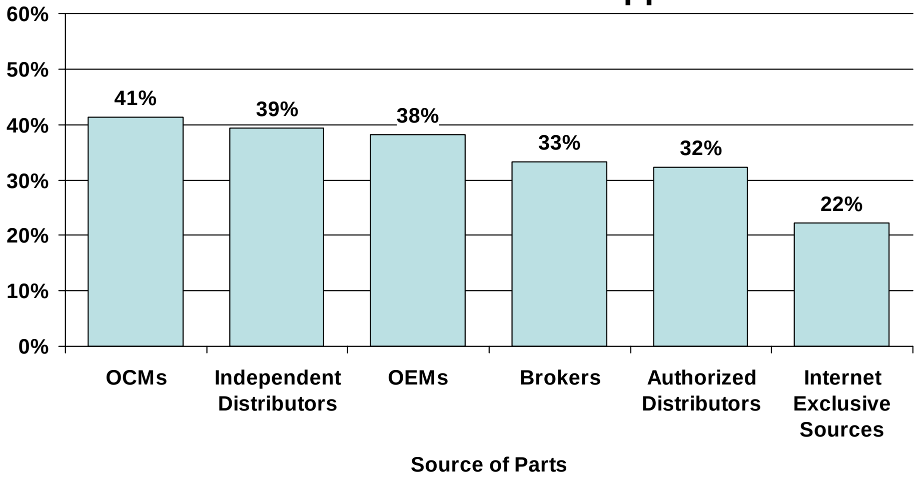
Assemblers were also asked to indicate what percentage of parts they tested from different suppliers.[40] Despite 72 percent of circuit board assemblers stating that they conduct some level of pre-stock testing, when broken out by type of supplier the levels of testing are significantly lower (see Figure IV-13).

For the two types of suppliers considered riskiest by the industry, 39 percent of assemblers conduct pre-stock testing for parts from independent distributors and 33 percent do so for parts

[40] This data was cross-referenced with each assembler's supplier information in order to count only those companies that procured parts from each type of supplier.

from brokers. These testing levels contrast with the 55 percent of assemblers with counterfeits who knew of independent distributors selling counterfeit parts and the 82 percent who knew of brokers doing the same.

Figure IV-13: Percent of Circuit Board Assemblers Conducting Pre-Stock Testing on Parts From Different Suppliers*



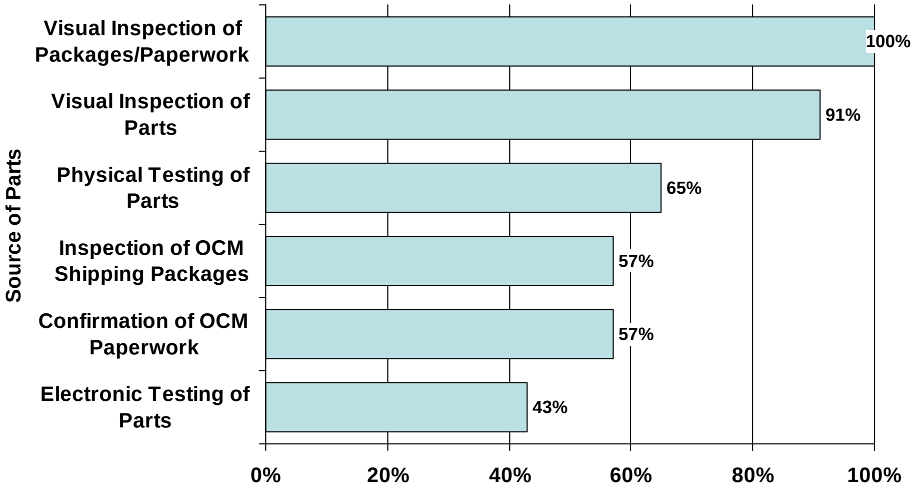
*** Only includes the companies that purchased from each supplier.**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Pre-stock testing can involve many procedures, but circuit board assemblers primarily perform different levels of visual inspection rather than electronic or physical testing (see Figure IV-14).[41] All assemblers that test parts prior to placing them in inventory perform visual examinations of packages and paperwork, with 91 percent visually inspecting the parts themselves. Only 43 percent of companies that conduct pre-stock testing electronically evaluate parts before placing them into inventory. Electronic testing, unlike visual inspection, involves evaluating the performance of the parts and is a more robust and costly method of authentication.

[41] The number of assemblers performing physical evaluation may be overstated because some survey respondents may have misinterpreted the term to mean a form visual inspection, rather than invasive physical examination.

Figure IV-14: Percent of Circuit Board Assemblers Conducting Pre-Stock Testing by Type of Testing*



*** Percentage is taken out of the companies that do any type of pre-stock testing**

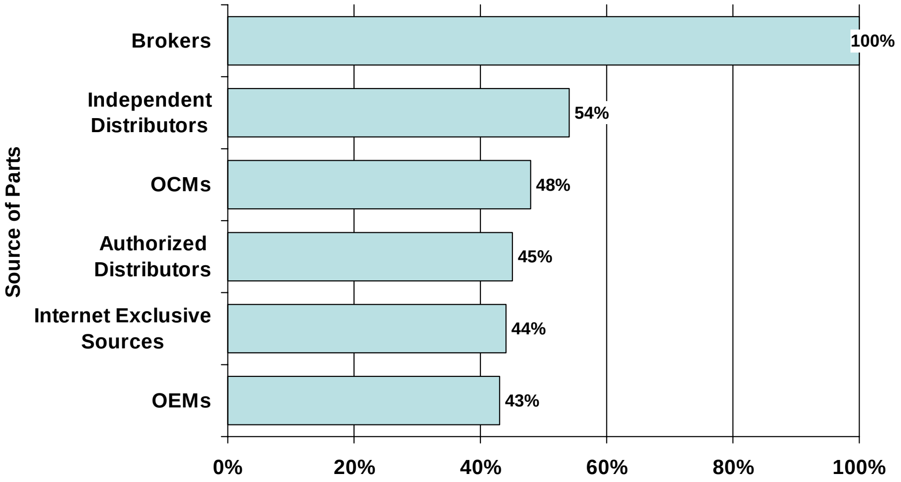
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Many circuit board assemblers said it is “not practical” to inspect for counterfeit components because of the large volume of parts they acquire and the potential costs of the inspection process. When there is an issue, one assembler explained that it “takes out the problem part, throws it away, and replaces it with another part.”

Circuit board assemblers may seek verification of the part conformance from their suppliers in addition to or in place of internal testing.[42] All assemblers that purchased parts from brokers required verification from testing facilities that the parts purchased are genuine and conform to OCM performance specifications (see Figure IV-15). However, assemblers do not hold any other type of supplier to this high of a standard. In particular, only 44 percent of Internet-exclusive sources and 54 percent of independent distributors were required to provide this verification.

[42] This data was cross-referenced with each assembler’s supplier information in order to count only those companies that procured parts from each type of supplier.

Figure IV-15: Percent of Circuit Board Assemblers That Require Verification of OCM Performance Specifications by Testing Facilities by Type of Supplier*



*** Only includes the companies that purchased from each supplier.**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

CO-MINGLING OF INVENTORY AND AUDITING PRACTICES

Once an electronic part has been placed into inventory, the inventory may be further scrutinized for counterfeits through periodic audits. The effectiveness of these audits is heavily dependent upon the traceability of parts. If circuit board assemblers co-mingle identical parts from different suppliers in the same bin, it may be difficult to identify counterfeit parts or remove them all. Seventy-two percent of assemblers co-mingle identical parts from multiple suppliers in the same bin. A few survey respondents assign parts individual identification and maintain traceability of the parts they co-mingle.

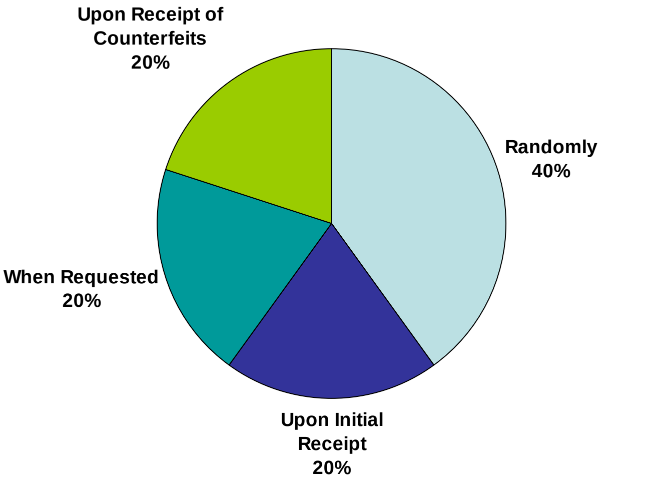
Sixteen percent of circuit board assemblers audit their inventory for counterfeit products. The low percentage of inventory audits, combined with the overall low level of pre-stock testing, indicates that assemblers generally assume that the parts they purchase are genuine.

Assemblers that do not audit their inventory provided a few similar explanations:

- Inventory audits are performed, but there are no specific procedures to identify potential counterfeits;
- Inventory audits are not performed because "all inspections are done when parts arrive;" and
- Do not perform inventory audits at any level.

None of the assemblers audit their inventory for counterfeits on a regularly scheduled basis (see Figure IV-16). For the most part, audits only occur when certain conditions are met, specifically if a counterfeit is identified, when requested by a customer, or when a part is first received. Forty percent of assemblers conduct inventory audits on a random basis.

Figure IV-16: Frequency of Inventory Audits for Counterfeits - Circuit Board Assemblers*

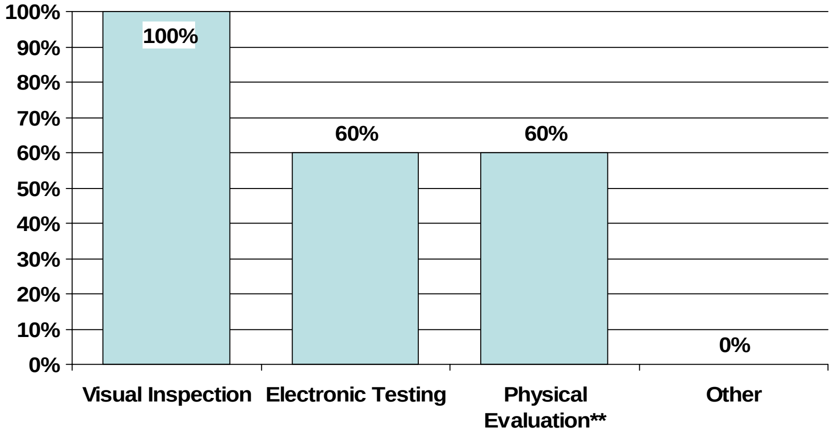


*** Only includes companies who audit their inventory for counterfeits**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

As with pre-stock testing, circuit board assemblers mainly perform visual inspections of parts during inventory audits. Sixty percent of assemblers that conduct audits also perform electronic testing and physical evaluation (see Figure IV-17). As stated previously, physical evaluation was likely mistaken by survey respondents as a form of visual inspection.

Figure IV-17: Form of Inventory Audits for Counterfeits - Circuit Board Assemblers*



*** Only includes companies who audit their inventory for counterfeits**

**** Physical evaluation may have been misinterpreted to mean a type of visual inspection, rather than destructive testing**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

TESTING OF PARTS

Circuit board assemblers were asked to identify the number of product models ordered visual for inspection, electronic testing, and physical evaluation. Less than half of assemblers ordered any testing for at least one product model (see Figure IV-18). The largest percent of assemblers (34 percent) ordered at least one product model to undergo visual inspection.

Figure IV-18: Percent of Circuit Board Assemblers Ordering Testing for at Least One Product Model

	Visual Inspection	Electronic Testing	Physical Evaluation*
Circuit Board Assemblers	34%	16%	28%

*** Physical evaluation may have been misinterpreted to mean a type of visual inspection, rather than destructive testing**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Visual inspection is the most basic type of parts testing performed to authenticate parts. There is a wide range of visual inspection criteria that companies rely on to verify part authenticity. All of the circuit board assemblers that conduct visual inspection examine the part number of the product, and a majority check the product for trademarks (Figure IV-19). A little over half of assemblers that perform visual inspection check the date of manufacture and bar coding. Even fewer assemblers look at covert markings, holograms, or embedded authenticity data to confirm part authenticity.

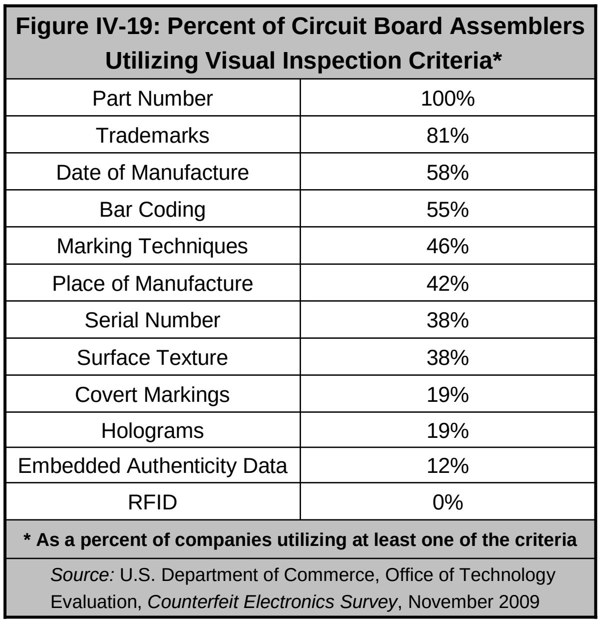


Figure IV-19: Percent of Circuit Board Assemblers Utilizing Visual Inspection Criteria*

Part Number	100%
Trademarks	81%
Date of Manufacture	58%
Bar Coding	55%
Marking Techniques	46%
Place of Manufacture	42%
Serial Number	38%
Surface Texture	38%
Covert Markings	19%
Holograms	19%
Embedded Authenticity Data	12%
RFID	0%

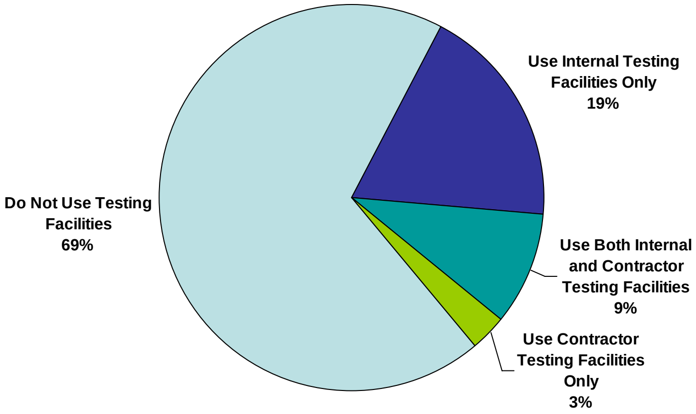
*** As a percent of companies utilizing at least one of the criteria**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009

TESTING FACILITIES

Circuit board assemblers can choose to have electronic parts tested either internally or by companies that provide external testing services. Sixty-nine percent of assemblers, however, do not utilize any facilities, internal or contractor-operated, to test for counterfeits (see Figure IV-20). Only 19 percent of assemblers maintain internal testing facilities for testing, while fewer use contractor-operated facilities or a combination of internal and external facilities. Most of these testing facilities are located in the United States.

Figure IV-20: Type of Testing Facilities Utilized by Circuit Board Assemblers



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Actions Taken Regarding Counterfeits

There are many actions a company may pursue when confronted with counterfeit electronic parts, such as notifying federal authorities, taking legal action, and testing inventory. Circuit board assemblers were asked a series of questions about these actions: the steps they take once they are notified of and when they possess counterfeits; which authorities they contact; their perceived difficulty in identifying counterfeits; and what is being done to mitigate the risk.

Steps Taken After Notification of Counterfeit Parts Being Shipped

It is important to understand how assemblers react or would react when notified that they have shipped a counterfeit part. These notifications can come from many different places, including testing houses, suppliers, and customers. For the most part, circuit board assemblers take internal actions if they are notified of shipping counterfeit parts.[43] The majority of circuit board

[43] Some respondents answered this survey question from the perspective of what they would do if they were notified of counterfeit parts, and not what they have done.

assemblers stated they pull back inventory, notify internal company authorities, and locate select inventory (see Figure IV-21). Only 13 percent of assemblers go beyond their company to notify industry associations and nine percent notify authorities in the federal government.

Figure IV-21: Steps Taken/Would be Taken After Notification of a Counterfeit Being Shipped – Circuit Board Assemblers

Pull Back Inventory	69%
Notify Internal Company Authorities	66%
Locate Select Inventory	66%
Trace Supply Chain	57%
Inform Authorized Distributors	50%
Inform OCM	47%
Perform Random Testing	41%
No Steps Are Taken	19%
Notify Industry Associations	13%
Notify Federal Authorities	9%
Other	9%
Wait for Additional Complaints	6%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Circuit board assemblers take similar approaches after taking possession of a counterfeit of a purchased component or a counterfeit of an assembled circuit board they manufactured.[44] If assemblers encounter a counterfeit component purchased from a supplier, they most often request a credit and return the parts to the OCM or distributor (see Figure IV-22). Very few assemblers turn the parts over to law enforcement or enter the incident into industry or U.S. Government databases. Curiously, 53 percent stated that they enter the incident into a company database, yet on a previous survey question 82 percent of assemblers with counterfeits said they do not have such a database.

[44] Some respondents answered this survey question from the perspective of what they would do if they had possession of counterfeit parts, and not what they have done.

Figure IV-22: Steps Taken After Possession of a Purchased Counterfeit Component – Circuit Board Assemblers

Request credit from OCM or parts distributor	69%
Return parts to OCM or parts distributor	59%
Enter incident into company database	53%
Conduct random testing of parts in inventory	41%
No steps are taken	31%
Test part/send for evaluation	38%
Quarantine parts away from regular inventory	28%
Disposal of parts almost immediately	25%
Check industry or USG databases for similar incidents	19%
Retain samples of counterfeit parts for reference	16%
Turn over to law enforcement authorities after analysis	16%
Turn over to law enforcement authorities for analysis	13%
Leave disposal to part filing complaint	9%
Other	9%
Enter incident into industry or USG database	6%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

If a counterfeit gets integrated into a manufactured product and is identified by a customer, the majority of assemblers issue a credit (see Figure IV-23). Assemblers also frequently return the counterfeit part of the manufactured product to their distributor or OCM that supplied it to them. Very few companies engage law enforcement authorities or industry databases, which severely limits the flow of information about counterfeits.

Figure IV-23: Steps Taken/Would be Taken After Possession of a Counterfeit Manufactured Product – Circuit Board Assemblers

Issue Credit	63%
Return to Distributor or OCM	56%
Enter into Company Database	50%
Test Part	44%
Random Inventory Testing	44%
No Steps are Taken	31%
Quarantine Parts	22%
Retain Samples for Reference	22%
Check Industry or USG Databases	16%
Dispose of Parts Immediately	16%
Turn Over to Law Enforcement Authorities For Analysis	13%
Turn Over to Law Enforcement Authorities After Analysis	13%
Enter into Industry or USG Databases	9%
Other	9%
Leave Disposal Up to Party Filing Complaint	6%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Circuit board assemblers that did not take any actions related to counterfeits (31 percent) did not provide their explanations. For the most part, assemblers that have not had a previous incident with counterfeits have not prepared for that contingency. One company stated that "if or when [an incident] ever does [occur] we will then decide a course of action."

AUTHORITIES CONTACTED AFTER COUNTERFEIT INCIDENTS

Only 22 percent of circuit board assemblers know which authorities to contact if they encounter counterfeit components. With this in mind, it is not surprising that 73 percent of assemblers that encountered counterfeits did not report these incidents to any government authorities. Those that notify authorities did so to a wide-range of authorities, such as state/local authorities, Government-Industry Data Exchange Program (GIDEP), IDEA, DLA, NASA, and their customers (see Figure IV-24).

Figure IV-24: Authorities Notified After Counterfeit Incident – Circuit Board Assemblers*

None at All	73%
Customer	9%
State/Local Authorities	9%
Government-Industry Data Exchange Program (GIDEP)	9%
Defense Logistics Agency (DLA)	9%
NASA	9%
Other	9%

*** Only includes those companies with counterfeit incidents**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

GIDEP was originally designed to "support government systems readiness, logistic effectiveness, productivity and cost reduction through timely retrieval, storage and distribution of data among government and industry organizations."[45] GIDEP provides many services and tools for its members, among which is a database to report incidents of counterfeit electronics.

Of the 11 circuit board assemblers that encountered counterfeits, only two reported incidents to GIDEP. Those companies that did not report to GIDEP provided a variety of explanations as to why they decided not to do so. Assemblers generally put the responsibility for reporting counterfeit incidents on their parts suppliers or their customer. One company stated they "return counterfeit parts to the supplier that sold the parts to us so they can report the incident to GIDEP." Other assemblers are not aware of GIDEP or do not have accurate information about its function. One assembler did not report because they believed that only OCMs report to GIDEP.

Reporting to Industry Associations

Circuit board assemblers do not typically share information about counterfeit incidents with other assemblers or members of the electronics industry. Ninety-one percent of assemblers do not report to any industry associations (see Figure IV-25). Those that report do not favor one particular industry association, but notify many different individual organizations.

[45] Jim Stein, "The Government-Industry Data Exchange Program," Defense Standardization Program Journal, Jan/Mar 2008: 5.

Figure IV-25: Percent of Circuit Board Assemblers Reporting to Industry Associations

Do Not Notify Industry Organizations	91%
National Association of Manufacturers	6%
ERAI	3%
Independent Distributors Electronics Association (IDEA)	3%
National Electronic Distributors Association	3%
Electronic Industries Association	3%
Semiconductor Industry Association (SIA)	3%
Alliance for Gray Market & Counterfeit Abatement (AGMA)	3%
Aerospace Industries Association (AIA)	3%
Government Electronic Industries Association	3%
Electronic Components, Assemblies & Materials Association	3%
Association of Connecting Electronic Industries (IPC)	3%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

AUTHORITIES CUSTOMERS SHOULD CONTACT

As stated previously, circuit board assemblers rely on their customers and parts' suppliers to handle counterfeit parts, and do not provide much guidance to their customers on what authorities should be contacted. Half of circuit board assemblers tell their customers to contact their company, and 44 percent do not provide their customers with any direction in the event of a counterfeit incident (see Figure IV-26). Only a small number of assemblers direct their customers to contact external authorities, such as GIDEP and DLA.

Figure IV-26: Authorities Customers are Told To Contact in Case of Counterfeit Incidents

My Company (Survey Respondent)	50%
None	44%
Government-Industry Data Exchange Program (GIDEP)	6%
Defense Logistics Agency (DLA)	6%
Other	6%
Federal Aviation Administration (FAA)	3%
State/Local Authorities	3%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Legal Guidance and Liabilities

Circuit board assemblers are generally unaware of any legal responsibilities and liabilities concerning counterfeit parts. Only 19 percent of assemblers are aware of any legal requirements for the management and/or disposal of counterfeit parts. Sixteen percent of assemblers are aware of written instructions or guidance from federal authorities on reporting counterfeit products, although none were specifically cited. A higher number of assemblers, 31 percent, are aware of their liabilities related to the distribution, storage, and disposal of counterfeit parts.

Despite the high percentages of circuit board assemblers were unaware of their legal responsibilities and liabilities, only 44 percent of assemblers stated that they need guidance from federal authorities regarding civil and criminal liabilities and penalties related to distribution, storage and disposal of suspected counterfeit parts. Some circuit board assemblers said they did not need guidance because they have not encountered a counterfeit component.

Difficulty Identifying Counterfeits

Circuit board assemblers were asked to indicate if they found it difficult to identify counterfeit parts, and if they are better able to identify counterfeits now than they were five years ago. Overall, 62 percent of assemblers said they find it difficult to identify counterfeit parts, while 38 percent did not.

Both companies that have and do not have difficulty identifying counterfeits rely heavily upon testing their manufactured products at the final assembly stage, rather than testing the components before they are integrated. Many assemblers stated something similar to the fact that “other than the obvious visual difference or [if a product] fails an electronic test at an assembled circuit board level, we would not be able to determine if it is counterfeit.” If the board passes this final test and is sent to the customer, these companies expect their customers to “check the boards we build for them and let us know if there is a problem.”

Fifty-nine percent of assemblers believe they are better able to identify counterfeit components today as opposed to five years ago. These companies stated they are more careful in selecting their suppliers today than they were in the past, particularly when it comes to independent distributors and brokers. In addition, increased awareness and knowledge of the problem has caused some assemblers to put internal policies into place to mitigate the risks associated with counterfeit components.

The majority of assemblers that say they are not able to better control counterfeit components today have no knowledge or experience with the problem. Some also stated that they have not changed any of their procedures in the past five years.

REASONS FOR COUNTERFEITS ENTERING THE U.S. SUPPLY CHAIN

Circuit board assemblers provided reasons why counterfeit products enter the U.S. supply chain (see Figure IV-27). Most assemblers pointed to less stringent inventory management and greater reliance on gray market parts by unauthorized distributors.[46] Assemblers also pointed out inadequate parts production, insufficient notice of part production termination, inadequate part purchase planning by OEMs, and an insufficient chain of accountability.

Figure IV-27: Circuit Board Assemblers' Top Ten Reason For Counterfeits Entering the Supply Chain

Less stringent inventory management by parts brokers	63%
Greater reliance by brokers on gray market parts	59%
Purchase of excess inventory on the open market	50%
Greater reliance by independent distributors on gray market parts	47%
Inadequate parts production by OCMs	44%
Insufficient notice to customers of part production termination	44%
Inadequate part purchase planning by OEMs	41%
Less stringent inventory management by independent distributors	38%
Insufficient chain of accountability	38%
Greater reliance by contract manufacturers on gray market parts	31%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

[46] A gray market is the trade of parts through distribution channels which, while legal, are unofficial, unauthorized, or unintended by OCMs.

INTERNAL ACTIONS TAKEN TO PREVENT INFILTRATION OF COUNTERFEITS

To prevent counterfeits from infiltrating their supply chain, 41 percent of circuit board assemblers perform additional screening and testing on current inventories (see Figure IV-28). Some companies also train staff and revise their procurement procedures for returns in order to reduce the risk of counterfeit parts. Thirty-four percent of assemblers, however, are not taking any actions within their own company to prevent counterfeits. Many of these companies believe they do not need to revise any internal procedures since they have not encountered a counterfeit part.

Figure IV-28: Internal Actions Taken to Prevent Infiltration of Counterfeits – Circuit Board Assemblers

Performing screening and testing on inventory	41%
No internal actions taken	34%
Training staff on the negative economic and safety impacts of counterfeit products	28%
Revising procurement procedures to more carefully screen/audit/evaluate authorized returns from customers	25%
Revising company procedures for disposal of "seconds," defective parts, and production overruns	22%
Revising procurement procedures to reduce purchases from independent distributors and brokers	13%
Other	9%
Embedding new security measures in existing product lines	3%
Adding security markings to existing inventory	0%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

EXTERNAL ACTIONS TAKEN TO PREVENT INFILTRATION OF COUNTERFEITS

Fewer assemblers take external actions to prevent the infiltration of counterfeit parts than those that take internal actions. Fifty-nine percent of circuit board assemblers take no actions outside of their company (see Figure IV-29). Only 41 percent take any external steps to prevent counterfeit part infiltration, usually educating customers about the risks of gray market products or referring customers to companies that could identify substitute products.

Figure IV-29: External Actions Taken to Prevent Infiltration of Counterfeits – Circuit Board Assemblers

No external actions taken	59%
Educating customers about risks associated with gray market products	28%
Referring customers to companies that could identify suitable substitute products or re-engineer system components	25%
Educating customers on the negative economic and safety impacts of counterfeit products	16%
Referring customers to authorized after-market manufacturers	9%
Prohibiting authorized distributors from buying back excess inventory on the gray market	6%
Tightening contractual obligations of contract manufacturers with regard to disposal of “seconds,” defective parts, and overruns	3%
Other	3%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Circuit board assemblers, as integrators of electronic components, are an “invisible” part of the supply chain. They are not manufacturers of electronic parts and components, nor are they end-users of the final assembled circuit boards. These companies are intermediaries, and as such do not always experience the negative effects that counterfeit parts have on the rest of the supply chain. Circuit board assemblers generally do not focus on testing for counterfeits, often assuming that their suppliers have provided them with the proper parts. When they do conduct testing for counterfeits, it is typically a form of visual inspection on the incoming parts. While completed circuit boards are tested after assembly, this testing is usually for performance. In fact, most assemblers discovered counterfeits through customer returns. Although assemblers encountered relatively few counterfeits, their low levels of testing, documentation, and auditing may obscure the extent of the problem.

V. PRIME CONTRACTORS AND SUBCONTRACTORS

Prime contractors and subcontractors have a unique position in the supply chain, as they consume electronic components for use in systems and subsystems but are not the end-user of these products. OTE surveyed 121 companies to capture their perspective of counterfeit electronics in the supply chain.

Respondents were asked to identify themselves as prime contractors, subcontractors, or both. Prime contractors direct and manage the delivery of large projects or products, while subcontractors provide parts, subsystems, and/or systems to a prime contractor. Half of the respondents identified themselves as both prime contractors and subcontractors. This dual role makes separate analysis of the behaviors and experiences of prime contractors and subcontractors complicated. For ease of analysis, all companies were analyzed together and are referred to as contractors in this assessment.

Of the 121 contractors, 26 percent (31 companies) reported having encountered counterfeit electronic components (see Figure V-1).[47]

Figure V-1: Companies Encountering Counterfeit Electronics

Type of Company	Encountered Counterfeits	Did Not Encounter Counterfeits	Total
Prime/Sub Contractor	31	90	**121**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

[47] For the purposes of this assessment, the term "counterfeit part" and any variation of it, means suspected or confirmed counterfeit part or component.

SOURCE OF PARTS

Contractors identified the types of suppliers used to purchase discrete electronic components, microcircuits, bare circuit boards, and assembled circuit boards. These companies primarily purchase discrete electronic components and microcircuits, although a majority of contractors also purchase bare and assembled circuit boards.

Contractors purchased the majority of parts from the original component manufacturers (OCMs) and the OCMs' authorized distributors (see Figure V-2). However, over three-quarters of contractors purchased parts from independent distributors, more than half purchased from parts brokers, and one quarter purchased parts from Internet-exclusive sources. There are even a small number of contractors that purchased parts from various elements of the Department of Defense (DOD). It is clear that contractors procure their parts from a variety of sources.

Figure V-2: Percent of Prime/Sub Contractors Purchasing Parts From Different Suppliers

Type of Supplier	Percent of Prime/Sub Contractors
OCMs	89%
Authorized Distributors	89%
Independent Distributors	77%
Brokers	56%
Internet-Exclusive Sources	26%
OEMs	22%
Contract Manufacturers	17%
DOD Depots	11%
DLA	11%
DOD Manufacturing Centers	7%
DOD Surplus	7%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Most contractors purchase parts directly from OCMs or from authorized and independent distributors with accompanying OCM purchase documents, making the authenticity of the parts easier to verify. A large number of contractors, however, said they procure parts at times without purchase documentation, making authenticity harder to determine (see Figures B-1 – B-4 in Appendix B). A few contractors acknowledged purchasing used parts pulled from circuit boards or used microcircuit die placed in a new package.

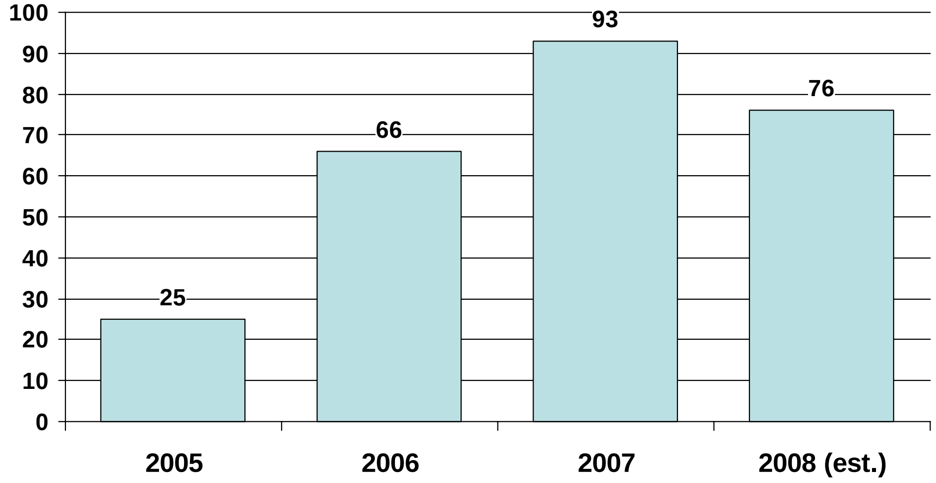
COUNTERFEIT INCIDENTS

As indicated previously, 26 percent of contractors have encountered counterfeit electronic components. From 2005 to 2008, these 31 companies encountered counterfeits for numerous types of discrete electronic components, microcircuits, bare circuit boards, and assembled circuit boards (see Figures B-5 through B-8 in Appendix B). Counterfeits of discrete electronic components and microcircuits were the most prevalent electronic parts mentioned by contractors.

The survey responses indicated an increase in counterfeit incidents during the 2005-2007 period among contractors (see Figure V-3).[48] This trend could be due to an increase in the number of counterfeits being purchased, but it could also be due to an improvement in recordkeeping by contractors or better detection and testing methods. The lower number of counterfeit incidents in 2008 is most likely because contractors provided estimates.

[48] For the purposes of this study, an incident is a single encounter of a counterfeit component. An incident could involve one part or a thousand parts of a component.

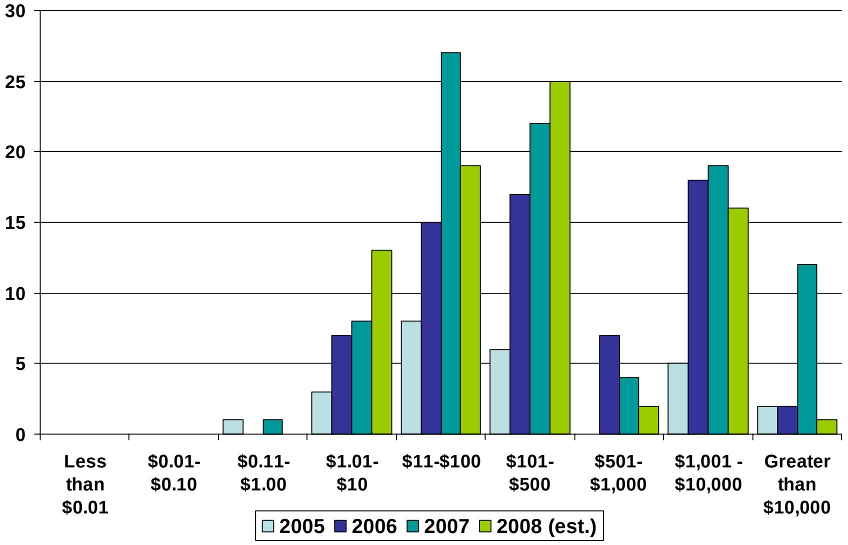
Figure V-3: Total Counterfeit Incidents - Prime/Sub Contractors (2005 – 2008)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

A further review of incidents by product resale value shows that most of the counterfeit parts encountered by contractors were in the $11 to $500 range, where there has been a relatively steady increase in the number of incidents from 2005 to 2008 (see Figure V-4). Also of note are the high numbers of incidents in the $1,000 to $10,000 range. Thus, counterfeiters are targeting electronic components of all prices, and not just the more common components with small- to mid-price levels.

Figure V-4: Counterfeit Incidents by Product Resale Value - Prime/Sub Contractors (2005 - 2008)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Types of Parts Counterfeited

While the focus of this assessment is on the U.S. defense supply chain, the electronic components being counterfeited have a wide variety of purposes. These parts can be used in systems as diverse as cell phones, commercial aircraft, and weapon platforms. Survey respondents were asked to identify the number of counterfeit product models by product category, in order to determine the types of products most affected by counterfeits.

This type of information proved difficult to identify because electronic components can be used in many different types of products. Some contractors were unable to link the counterfeits that were encountered to a specific product category. Other contractors, particularly subcontractors, did not know the ultimate end-use of the items they produced.

Contractors provided enough information to identify some trends (see Figure V-5). The majority of counterfeit product models discovered were concentrated in the industrial/commercial product category. Of particular concern are the increasing numbers and fluctuation of counterfeits in the Qualified Manufacturers List (QML) and Qualified Products List (QPL) product categories.[49] QML and QPL products are used primarily in military and defense applications. Counterfeits in these product categories could adversely affect the readiness and effectiveness of the warfighter on the battlefield.

Figure V-5: Type of Counterfeit Incidents - Prime/Sub Contractors (2005-2008)

Type of Product	2005	2006	2007	2008 (est.)
Industrial/Commercial	6	58	40	48
Qualified Manufacturers List (QML)	13	7	24	8
Consumer	3	3	8	6
Qualified Products List (QPL)	2	0	12	6
Commercial Aviation	3	3	5	6
High Reliability – Industrial	2	0	9	5
ITAR Controlled	1	0	0	3
High Reliability – Medical	0	0	0	0
Critical Safety	0	0	0	0
High Reliability – Automotive	0	0	0	0
Generalized Emulation Microcircuits (GEM)	0	0	0	0

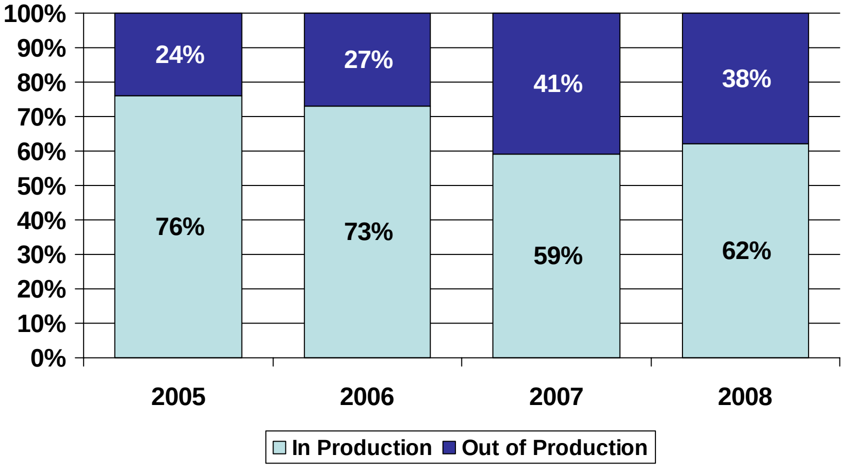
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Contractors also indicated the percent of counterfeit parts encountered that were versions of parts “in production” or “out of production” by the OCM (see Figure V-6).[50] Contractors have primarily encountered counterfeits of “in production” parts, even though the percentage has been decreasing since 2005. This is somewhat surprising, considering the need for obsolete, “out of production” parts for older defense systems. It also indicates that parts cannot be trusted as authentic just because the OCM and/or authorized distributor produce them.

[49] According to the Federal Acquisition Regulations (FAR), the QML is “a list of manufacturers who have had their products examined and tested and who have satisfied all applicable qualification requirements for that product.” 48 C.F.R. § 9.201 The QPL is “a list of products that have been examined, tested, and have satisfied all applicable qualification requirements.” 48 C.F.R. § 2.101

[50] For this assessment, parts produced by an after-market manufacturer are considered “out of production.”

Figure V-6: Percent of Counterfeit Incidents Involving In/Out of Production Parts – Prime/Sub Contractors (2005-2008)



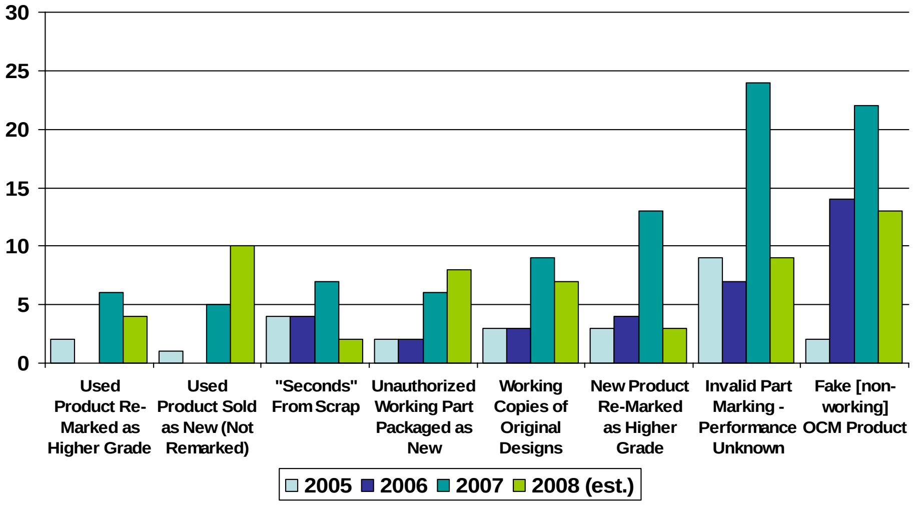
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

TYPES OF COUNTERFEITS AND METHODS OF DISCOVERY

Counterfeiters use many different methods to produce counterfeit electronic components, making detection more difficult. Contractors found a variety of different types of counterfeits from 2005 to 2008, though no particular counterfeiting method has increased or decreased in occurrence (see Figure V-7). Contractors encountered "fake [non-working] OCM product" more frequently than any other type; these incidents consisted primarily of microcircuits.

A significant number of counterfeit incidents reported by contractors were of "invalid part markings with unknown performance." This means the parts were identified as possible counterfeits based on their markings, so the actual type of counterfeit was unknown. As with the "fake [non-working] OCM product," the parts with invalid part markings were overwhelmingly microcircuits.

Figure V-7: Counterfeit Incidents by Type of Problem Prime/Sub Contractors (2005-2008)

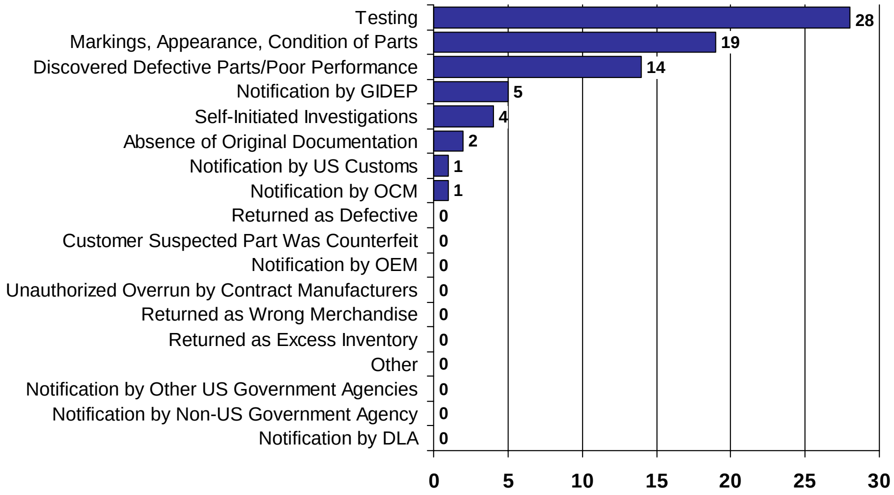


Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Survey respondents also identified the means by which they discover counterfeit electronic components (see Figure V-8). Contractors primarily uncover counterfeit parts through their own efforts: testing, identifying incorrect appearance of parts, and discovering defective or poor performance. There have been a few instances of discovery by notification through the Government-Industry Data Exchange Program (GIDEP), U.S. Customs, or OCMs. Contractors were not aware of discovering counterfeit parts through notification from their customers.

Fifty-four percent of the surveyed contractors had no specific method in place for customers to use for notification of counterfeit parts (Figure B-9 in Appendix B). Some contractors do not have a method in place because they have never received customer notification of counterfeits. For contractors that did have specific notification channels in place, those methods included website, e-mail, hotline, and general phone call notification.

Figure V-8: Counterfeit Incidents by the Method Uncovered – Prime/Sub Contractors (2008 est.)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

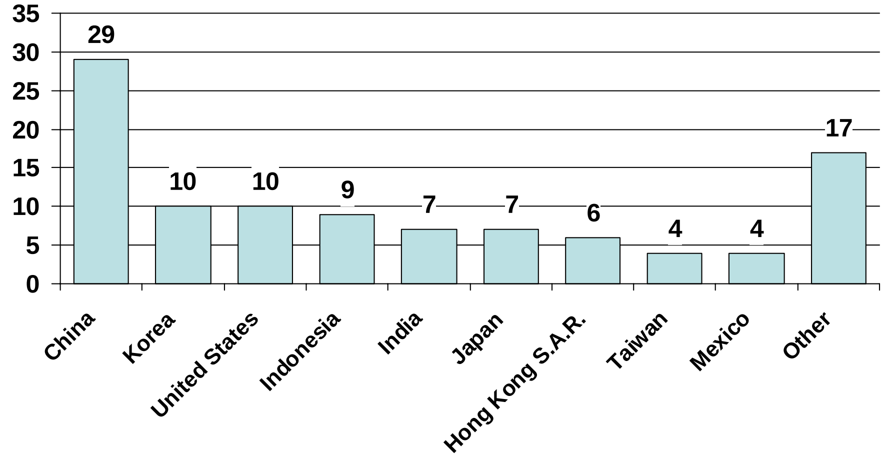
SOURCES OF COUNTERFEITS

Survey respondents were asked to identify countries suspected or confirmed to be sources of counterfeit electronic components. Overwhelmingly, contractors identified China as the main suspected source of counterfeits, with Asia as the largest regional source (see Figure V-9). Additionally, contractors identified the United States and Mexico as sources of counterfeit parts.[51]

It is important to note that these countries are suspected sources of counterfeit parts. Many contractors commented that they could not confirm the geographic source of the counterfeits they encountered, and that their responses were their opinions. Some contractors only knew the supplier company in the United States, and did not know where the supplier obtained the counterfeit component.

[51] The “Other” column of Figure V-9 is comprised of the following countries: Russia, Malaysia, the Philippines, Thailand, North Korea, Pakistan, Argentina, Costa Rica, Brazil, and Paraguay.

Figure V-9: Prime/Sub Contractors' Top 10 Countries Suspected as Sources of Counterfeits (2008 est.)

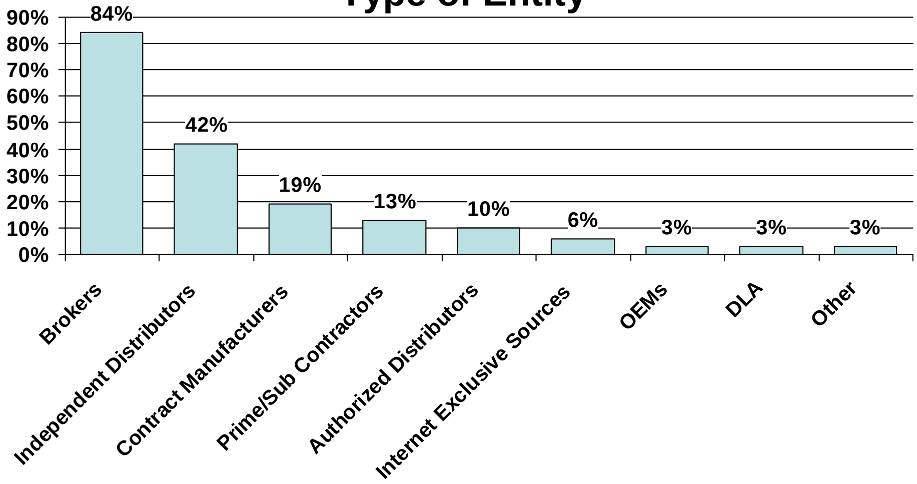


Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Contractors were asked if they had documented cases of counterfeit parts being sold by specific entities to determine how the counterfeit components are entering the supply chain. Of those contractors that have experienced counterfeits, 84 percent identified brokers and 42 percent identified independent distributors (see Figure V-10).

While brokers and independent distributors were identified as the primary sources of counterfeit parts, contractors identified all supply chain entities as having sold counterfeit components. Ten percent of contractors that encountered counterfeits, for example, identified authorized distributors as a source of counterfeit parts, while three percent mentioned Original Equipment Manufacturers (OEMs) and the Defense Logistics Agency (DLA). Thus a part cannot be assumed to be authentic merely because it comes from a source other than a broker or independent distributor.

Figure V-10: Percent of Prime/Sub Contractors with Cases of Counterfeit Incidents Sold by Type of Entity*



*** Only includes companies who encountered counterfeits**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

INTERNAL DATABASES TO TRACK COUNTERFEITS

Of the contractors that encountered counterfeit electronic components, 68 percent do not maintain a specific database to track those counterfeits. Some contractors that do not have specific databases for counterfeits maintain larger databases for non-conforming parts or general defects or rely on industry databases. The majority of contractors without an internal counterfeit database, however, did not explain why they did not have one.

Those contractors with an internal counterfeit database (32 percent) keep track of a number of different variables (see Figure V-11). The majority use their databases to track suspected/confirmed counterfeit products. A smaller percentage of counterfeit databases track “other” variables including GIDEP documents, part numbers, quantities, and dates of receipt.

Figure V-11: Variables Tracked By Internal Counterfeit Database*

Variable	Prime/Sub Contractors
Suspected/Confirmed Counterfeit Products	83%
Source of Reporting	72%
Known/Suspected Companies and Individuals	67%
Countries of Origin	61%
Other	28%

***Taken as a percent of those companies encountering counterfeits who maintain an internal database.**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Damage to Reputation

Contractors indicated their reputations have not been greatly impacted by counterfeits in the U.S. supply chain. Only seven percent of surveyed contractors reported a negative impact by counterfeit activities. While steps were taken to correct or mitigate the problems caused by counterfeits, customers maintained negative impressions of the contractors after changes were made.

A few contractors experienced damage to their reputations because of proactive efforts to stop counterfeits, particularly through disclosure of incidents through databases. These actions can cause these contractors to face unwarranted scrutiny from customers and the rest of the supply chain. One company said reporting suspect counterfeits to GIDEP and industry associations can cause customers and authorities to think the reporting company "may have more counterfeit part issues than do other companies."

INVENTORY CONTROL AND TESTING

The behavior of companies once they have obtained parts and placed them in inventory can be a factor in determining if counterfeits are likely to get integrated into systems. To identify areas of possible concern, contractors were asked questions relating to their inventory control and testing procedures.

RETURNS, EXCESS INVENTORY, AND RE-CIRCULATION OF PARTS

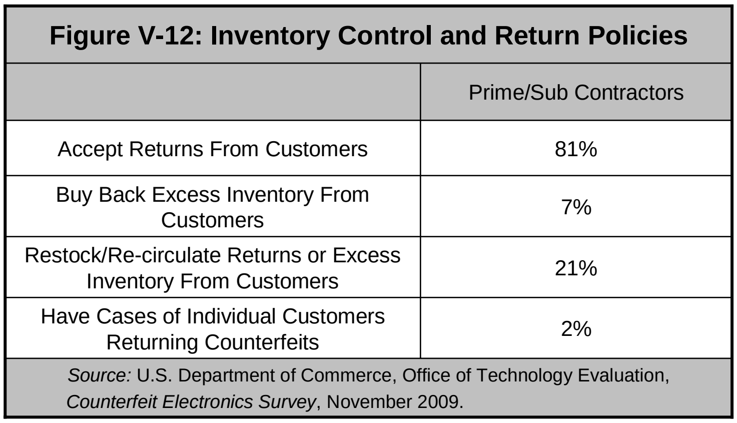
Customer returns and the buying back of excess inventory are two ways that counterfeit parts can enter a contractor's inventory. A customer could purchase counterfeit parts from an alternate source and, either intentionally or unintentionally, return or sell them back to a contractor. If they are placed back into inventory, these counterfeit parts could then be unknowingly sold to a different customer.

Eighty-one percent of contractors accept returns from their customers, and seven percent of contractors buy back excess inventory from customers.[52] Some contractors further clarified their responses by saying they only accept returns for service or warranty repairs, or only buy back excess inventory in their commercial business divisions.

As stated previously, the risk in accepting returns comes from placing those returns back in regular inventory without careful inspection. Twenty-one percent of survey respondents re-circulate returns and/or excess inventory from customers. Only two percent of contractors said they had cases of individual customers returning counterfeit parts.

[52] See Figure B-10 in Appendix B for a break-out of contractors that buy back excess inventory by customer type.

Figure V-12: Inventory Control and Return Policies



	Prime/Sub Contractors
Accept Returns From Customers	81%
Buy Back Excess Inventory From Customers	7%
Restock/Re-circulate Returns or Excess Inventory From Customers	21%
Have Cases of Individual Customers Returning Counterfeits	2%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

PRE-STOCK TESTING

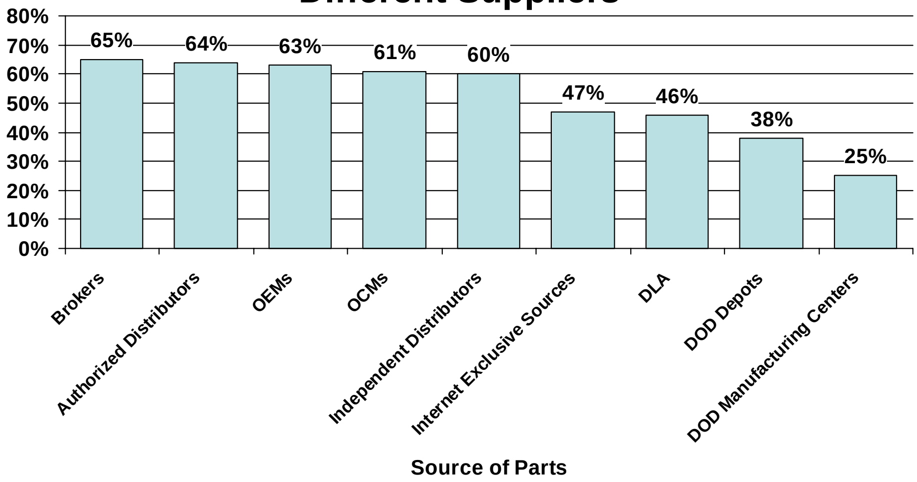
Testing purchased parts before placing them in inventory, or pre-stock testing, is an effective way to locate counterfeits and remove them from the supply chain. This testing can include visual inspection of parts and packaging, electrical testing to ensure functionality, and/or physical or destructive evaluation to ensure authenticity.

The majority of contractors (87 percent) conduct some form of pre-stock testing of incoming parts. The amount of parts tested within a shipment differs among contractors, with some testing 100 percent of incoming parts and others testing only a sample. Some contractors have routine procedures for how many parts to test, while others have varied procedures depending on contract specifications.

Contractors were asked to indicate the percent of incoming parts tested from different suppliers. This information was compared with data on the types of suppliers from which they purchase to determine the percent of contractors that test parts procured from specific suppliers (see Figure V-13). Based on this, 65 percent of contractors purchasing parts from brokers conduct pre-stock testing on those parts. This level appears possibly problematic, considering 84 percent of contractors knew of brokers selling counterfeit components.

The lower levels of testing for Internet-exclusive sources (47%) and DOD entities (25-46%) might indicate that contractors have a level of trust in those suppliers. Given the unknown nature of many online suppliers, this trust could prove problematic if suppliers do not conduct any parts testing themselves.

Figure V-13: Percent of Prime/Sub Contractors Conducting Pre-Stock Testing on Parts From Different Suppliers*



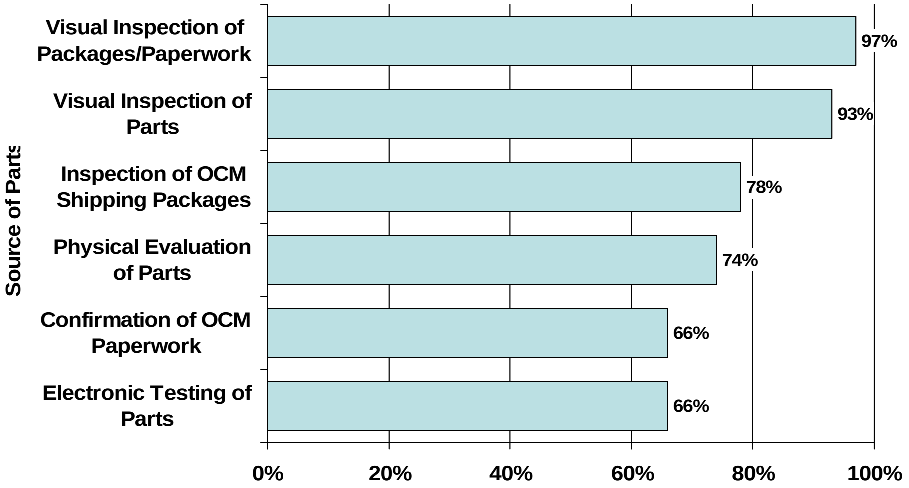
*** Only includes the companies that purchased from each supplier.**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Of those contractors that conduct pre-stock testing, the vast majority perform visual inspections of the parts, packages, and paperwork (see Figure V-14). A lesser percentage of contractors (78 percent) inspect the OCM shipping packages, and still fewer confirm OCM paperwork as genuine. Several contractors commented that the level of pre-stock testing depends on the type of supplier, indicating parts from certain types of suppliers are subject to more scrutiny than parts from others, although survey respondents do not necessarily support these claims.

The high percentage of contractors that said they conduct physical evaluation as compared to electronic testing might be invalid. It is likely that respondents did not understand physical evaluation to be a type of destructive testing, and instead thought it was a type of visual inspection.

Figure V-14: Percent of Prime/Sub Contractors Conducting Each Type of Pre-Stock Testing*



* Percentage is taken out of the companies that do any type of pre-stock testing

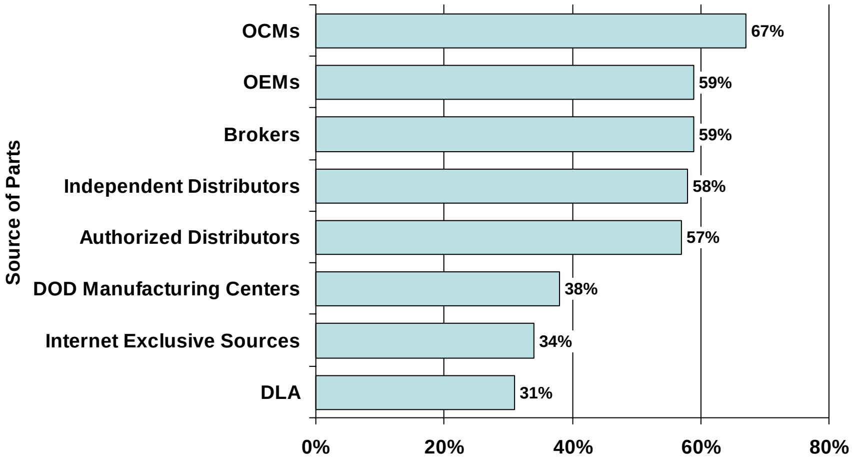
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Contractors can require their suppliers to provide verification of testing and confirmation that parts meet OCM performance specifications. More than half of contractors that purchase parts from OCMs, Original Equipment Manufacturers (OEMs), brokers, authorized distributors, and independent distributors require such verification (see Figure V-15).

The low percentage of contractors that require Internet-exclusive sources to provide testing verification of OCM performance could be problematic, especially considering the small percent that conduct pre-stock testing of parts from this type of supplier. This makes it seem as if contractors that purchase components from Internet-exclusive sources have a high level of trust in the authenticity of the procured parts.

There also seems to be a high level of trust in parts procured from DOD entities, given the low percent of contractors requiring supplier testing verification or conducting pre-stock testing on DOD-sourced parts. Considering DOD entities are generally consumers of supplied products and conduct very little testing on the parts they procure, this high level of trust is cause for concern.[53]

Figure V-15: Percent of Prime/Sub Contractors Requiring Verification of OCM Performance Specifications by Type of Supplier*



*** Only includes the companies that purchased from each supplier.**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

CO-MINGLING OF INVENTORY AND AUDITING PRACTICES

If a counterfeit component makes it past acquisition and pre-stock testing procedures, it can still be discovered if the company conducts periodic inventory audits for counterfeits. However, the effectiveness of these audits depends on whether a contractor co-mingles parts from different suppliers in the same bin. Co-mingling parts can make it difficult, if not impossible, to remove all suspect counterfeit parts for testing and quarantine, or to follow-up with a supplier or law enforcement authorities.

Sixty percent of contractors acknowledged co-mingling identical parts from different suppliers in the same bin. Several contractors specified that while parts are co-mingled, they are given specific markings for internal tracking, lot-controlled, or separated in unique bags within the bin.

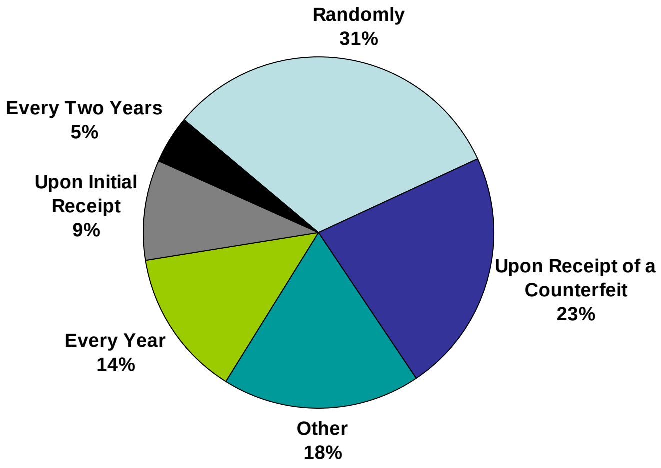
[53] The level of testing conducted by DOD entities is examined in Chapter VI of this assessment.

One contractor added that co-mingling only takes place after testing is conducted. In these instances, co-mingling does not present the same level of risk as it does when untraceable parts are combined and kept together.

Just 19 percent of surveyed companies conduct audits of their inventory for counterfeit parts. Many of the contractors that do not perform counterfeit-specific audits said it was not necessary due to the level of their pre-stock testing. A few others said they conduct larger inventory audits that are not specifically directed at detecting counterfeit parts.

Most contractors that conduct inventory audits for counterfeit parts do not have a set schedule for this activity (see Figure V-16). Instead, these inventory audits are conducted randomly or upon receiving a counterfeit part. Company staff members primarily perform audits for counterfeits, although 43 percent of contractors conducting audits have their procedures reviewed by independent authorities.

Figure V-16: Frequency of Inventory Audits for Counterfeits - Prime/Sub Contractors*

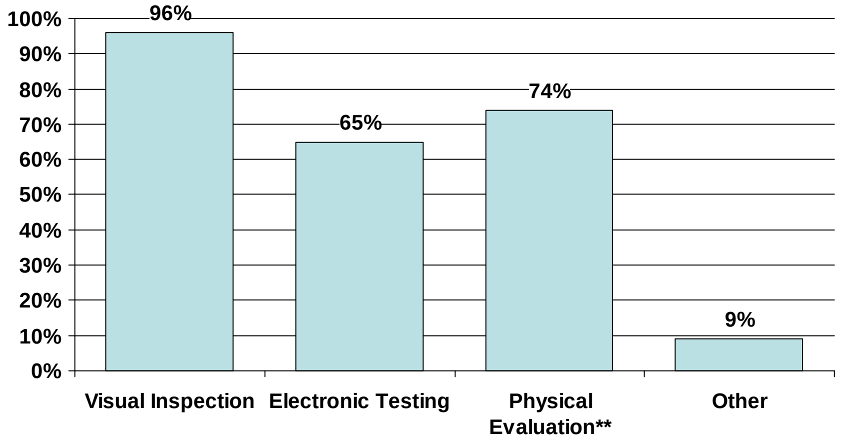


*** Only includes companies who audit their inventory for counterfeits**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Visual inspection is the preferred process used by contractors that conduct counterfeit-specific audits (see Figure V-17). A lesser percentage of contractors use electronic testing and physical evaluation during their counterfeit audits.[54] Only a few contractors check external databases as part of their auditing procedures, and one said the auditing method used would depend on their level of concern.

Figure V-17: Form of Inventory Audits for Counterfeits - Prime/Sub Contractors*



*** Only includes companies who audit their inventory for counterfeits**

**** Physical evaluation may have been misinterpreted to mean a type of visual inspection, rather than destructive testing**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

TESTING AND TESTING FACILITIES

Survey respondents identified the number of product models for which they ordered visual inspections, electronic testing, and physical evaluation. In 2008, half of surveyed contractors ordered visual inspections for at least one product model (see Figure V-18). During that year, contractors conducted more visual inspections than the other two types of testing. Several companies qualified that while inspection and testing procedures are in place, they are not for the express purpose of detecting counterfeit parts.

[54] As stated previously, the higher number of contractors conducting physical evaluation is likely due to respondents mistaking it for a form of visual inspection.

Figure V-18: Percent of Prime/Sub Contractors Testing at Least One Product Model by Test Type

	Visual Inspection	Electronic Testing	Physical Evaluation*
Prime/Sub Contractors	50%	40%	32%

*** Physical evaluation may have been misinterpreted to mean a type of visual inspection, rather than destructive testing**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

The most basic and inexpensive type of testing that can be conducted to identify counterfeit components are non-invasive visual inspections. Contractors look for a wide variety of criteria when conducting this level of testing for counterfeit parts (see Figure V-19). While almost all contractors (99 percent) check part numbers, a lesser number check trademarks, dates of manufacture, serial numbers, marking techniques, places of manufacture, and surface textures. A small number of contractors check radio frequency identification (RFID) and embedded authenticity data.

Figure V-19: Percent of Prime/Sub Contractors Utilizing Visual Testing Criteria*

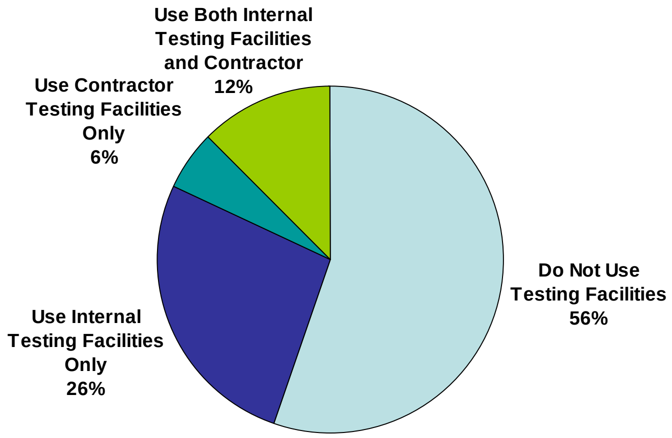
Part Number	99%
Trademarks	77%
Date of Manufacture	69%
Serial Number	64%
Marking Techniques	61%
Place of Manufacture	61%
Surface Texture	53%
Bar Coding	34%
Covert Markings	29%
Holograms	27%
Other	16%
RFID	15%
Embedded Authenticity Data	12%

*** As a percent of companies utilizing at least one of the criteria**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Companies can choose to use internal or contractor facilities to conduct various levels of counterfeit part testing. More than half of contractors do not use any testing facilities for the purpose of detecting counterfeit parts. The remaining 44 percent of contractors use a combination of internal and contractor testing facilities (see Figure V-20). The majority of these testing facilities are located in the United States.

V-20: Percent of Prime/Sub Contractors Utilizing Testing Facilities to Detect Counterfeits

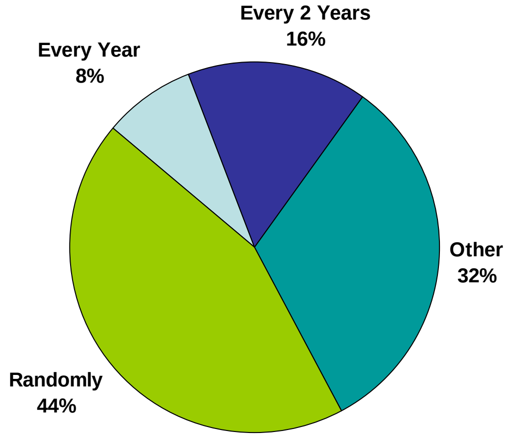


Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

SUPPLIER INVENTORY PRACTICES

Some contractors are not only concerned about the presence of counterfeit components in their own inventories, but also their suppliers' inventories. Twenty-one percent of contractors conduct audits of their suppliers' inventories for counterfeit parts (see Figure V-21). Many do this randomly, but a few contractors base the frequency of their supplier audits on the risk of counterfeits. Some contractors do not audit their suppliers for counterfeit parts, but monitor their suppliers' procurement practices and other procedures.

Figure V-21: Frequency of Inventory Audits of Suppliers' for Counterfeits - Prime/Sub Contractors*



*** Only includes companies who audit their suppliers' inventory for counterfeits**

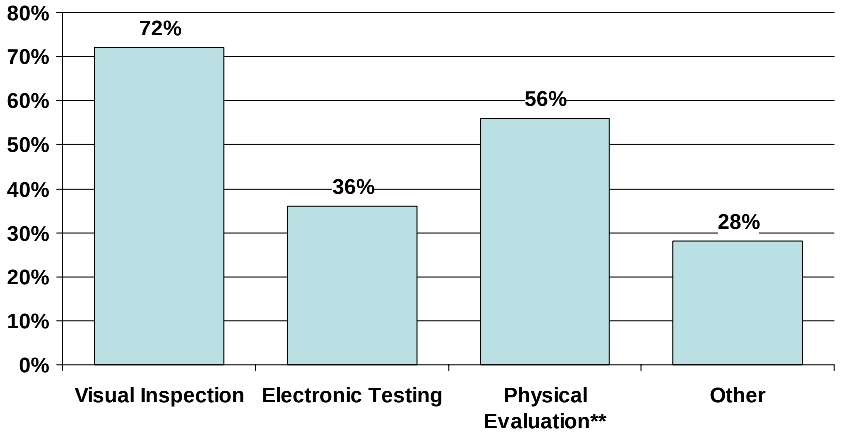
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Like those performed internally, audits of suppliers by contractors for counterfeit parts are primarily conducted by company staff. Only four percent of companies that audit their suppliers for counterfeit parts use independent auditors. Eighty-eight percent, however, have their supplier auditing practices reviewed by independent authorities such as International Aerospace Quality Standard AS9100 assessors.

The most common type of testing used by contractors when auditing their suppliers' inventory for counterfeit parts is visual inspection, with 72 percent of contractors using this method (see Figure V-22). Fewer contractors use electronic testing and physical evaluation during inventory audits of their suppliers.[55] The contractors that reported using a different form of inventory audit said they look at the traceability of parts or audit the procedures and processes used by suppliers.

[55] As stated previously, the higher level of contractors conducting physical evaluation is likely due to respondents mistaking it for a form of visual inspection.

Figure V-22: Form of Inventory Audits of Suppliers for Counterfeits - Prime/Sub Contractors*



*** Only includes companies who audit their suppliers' inventory for counterfeits**

**** Physical evaluation may have been misinterpreted to mean a type of visual inspection, rather than destructive testing**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Survey respondents were also asked if they had a legal agreement with their suppliers concerning counterfeit products. A quarter of contractors have such an agreement in place. Many contractors do not have a separate legal agreement with their suppliers regarding counterfeits, but address the issue within the contract, purchase order, and/or terms and conditions.

Of those contractors that do have such agreements, 60 percent require their suppliers to notify them of suspected counterfeit parts (see Figure V-23). Seven contractors (23 percent) require their suppliers to notify federal authorities of suspected counterfeit parts. Some of the other conditions incorporated by contractors in legal agreements include proof of the traceability of parts and requirements to purchase parts only from OCMs and OEMs.

Figure V-23: Requirements Concerning Counterfeits from Legal Agreements of Contractors*

Requirement	Percent
Notification of Prime/Sub Contractor Concerning Counterfeit Products	60%
Notification of Federal Authorities Concerning Counterfeit Products	23%
Inventory Checks	20%
Other	20%
Logs of Counterfeit Products	20%
Purchasing Requirements	13%
Include Certificates of Conformance	13%

*** Percentage is of the companies with a legal agreement with their suppliers**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

ACTIONS TAKEN REGARDING COUNTERFEITS

There are many steps contractors take or are willing to take regarding counterfeit electronic components. Contractors were asked several questions about these actions: steps taken once they are notified of and possess counterfeits; authorities they contact; related legal actions; and what is being done to mitigate the risk.

STEPS TAKEN AFTER NOTIFICATION AND POSSESSION OF A COUNTERFEIT PART

One area of potential action occurs when a contractor is notified about or becomes aware of a counterfeit part. This notification can come from several different places, including testing houses, customers, government authorities, suppliers, or other contractors. When a contractor is notified of a counterfeit part being shipped, the most common response is for contractors to pull back inventory (see Figure V-24).[56] A minority of contractors notify federal authorities or industry associations, 35 percent and 22 percent, respectively.

[56] Some respondents answered this survey question from the perspective of what they would do if they were notified of counterfeit parts, and not what they have done.

Figure V-24 Steps Taken/Would Be Taken After Notification of a Counterfeit Part Being Shipped – Prime/Sub Contractors

Pull Back Inventory	71%
Notify Internal Company Authorities	68%
Locate Select Inventory	67%
Trace Supply Chain	64%
Inform OCM	56%
Inform Authorized Distributors	50%
Perform Random Testing	45%
Notify Federal Authorities	35%
No Steps Are Taken	26%
Notify Industry Associations	22%
Other	21%
Wait for Additional Complaints	5%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Another area of potential action occurs when a contractor has physical possession of a counterfeit part. Out of the 14 actions provided in the survey, there is no single action taken by a majority of contractors after they gain possession of a counterfeit (see Figure V-25).[57] Approximately half of contractors test the counterfeit part and half enter the incident into a company database. Thirty-two percent of contractors take no action once they have counterfeits in their possession.

Contractors have little communication with federal authorities and industry associations once they gain possession of counterfeit components. Thirty-six percent of respondents check industry or U.S. government databases for information on the counterfeit part, and 24 percent enter information about their incident into those databases. Even fewer contractors turn the suspect parts over to law enforcement.

[57] Some respondents answered this survey question from the perspective of what they would do if they had possession of counterfeit parts, and not what they have done.

Figure V-25: Steps Taken/Would be Taken After Possession of a Counterfeit Part – Primes/Sub Contractors

Test Part	54%
Enter into Company Database	50%
Random Inventory Testing	46%
Retain Samples for Reference	43%
Quarantine Parts	40%
Issue Credit	36%
Check Industry or USG Databases	36%
No Steps are Taken	32%
Return to Distributor or OCM	30%
Enter into Industry or USG Databases	24%
Dispose of Parts Immediately	20%
Turn Over to Law Enforcement Authorities For Analysis	18%
Turn Over to Law Enforcement Authorities After Analysis	18%
Other	16%
Leave Disposal Up to Party Filing Complaint	7%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

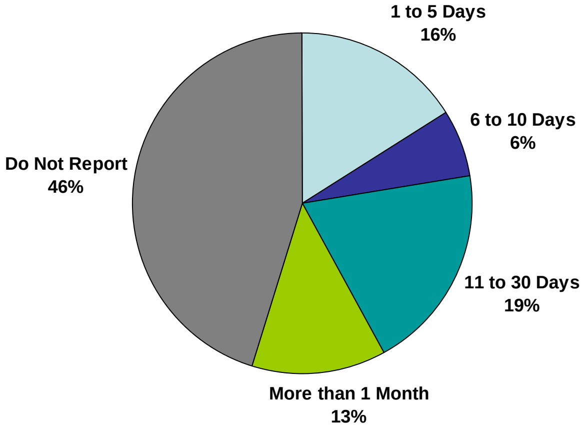
Authorities Contacted After Counterfeit Incidents

Further review of survey data shows only 52 percent of contractors know what authorities to contact when they are notified or have possession of counterfeit parts. In fact, 46 percent of contractors that have encountered counterfeit components do not report these incidents to government authorities (see Figure V-26).[58] There is also little reporting of counterfeit parts to industry associations; 81 percent of contractors that encountered counterfeits do not report incidents to any industry associations.

A few contractors reported to their suppliers, customers, or “any other affected party” instead of the government. Some only notify government authorities of confirmed counterfeit components. One respondent said, “There is a general fear of liability in these situations with ‘suspect parts.’” The majority of those that report or would report incidents to government authorities do so within one to 30 days.

[58] See Figure B-11 in Appendix B for the number of incidents reported over the four-year period.

Figure V-26: How Long it Takes to Report Counterfeits to Government Authorities – Prime/Sub Contractors*



*** Only includes companies who encountered counterfeits**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

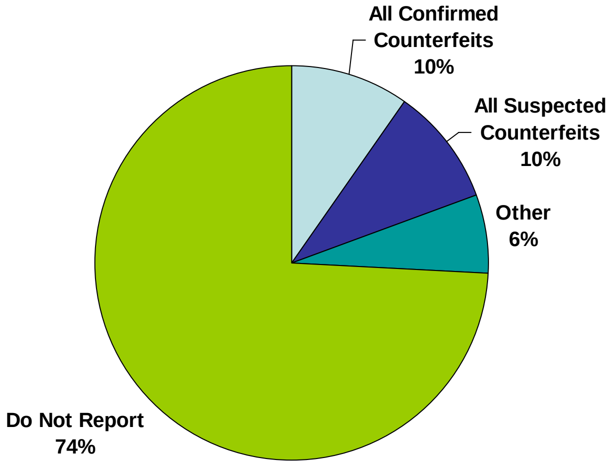
Contractors with counterfeit incidents most often reported to the GIDEP, but only 26 percent do so.[59] Contractors that submit alerts to GIDEP report a mixture of all confirmed counterfeits and all suspected counterfeits (see Figure V-27). One contractor said it reports to GIDEP only when required by a contract.

There were several reasons offered as to why contractors do not report counterfeit components to GIDEP:

- were not aware of GIDEP or that it tracked counterfeit incidents;
- did not believe they had enough incidents to warrant reporting;
- attempted to resolve the issue directly with the supplier or manufacturer;
- used another system to report counterfeit parts, such as ERAI or FAA; or
- believed only OCMs and OEMs report to GIDEP.

[59] See Figure B-8 in Appendix B for a list of other authorities contacted by contractors after a counterfeit incident.

Figure V-27: Level of Reporting to GIDEP for Prime/Sub Contractors Encountering Counterfeits



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Contractors not only have to take action to deal with any counterfeit parts they discover, but also work with their customers to handle counterfeit parts issues. Almost 60 percent of contractors instruct customers to notify their company in the event of a counterfeit incident (see Figure V-28). More than a third of contractors do not provide customers with any notification instructions. Many of these contractors do not tell customers who to contact because they have never encountered counterfeits.

Figure V-28: Authorities Customers are Told To Contact in Case of Counterfeit Incidents

My Company (Survey Respondent)	59%
None	36%
Government-Industry Data Exchange Program (GIDEP)	12%
Federal Aviation Administration (FAA)	10%
Defense Logistics Agency (DLA)	6%
State/Local Authorities	5%
Other	5%
Federal Bureau of Investigation (FBI)	5%
Defense Related Investigative Services (e.g., DCIS, etc.)	5%
NASA	4%
NSA	4%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Legal Guidance and Liabilities

Contractors were asked several questions about their awareness of legal requirements, liabilities, and guidance regarding the handling of counterfeit parts. Fifty-nine percent of respondents are not aware of any legal requirements for the management and/or disposal of counterfeits. One contractor was not aware of specific legal requirements because it had not encountered counterfeit components. Another contractor considers counterfeit parts to fall within the scope of more general legal requirements.

A higher number of contractors (62 percent) are not aware of any written instructions or guidance from federal authorities on reporting counterfeit incidents. One contractor said, "We have sought guidance from federal authorities on what to do with parts suspected or known to be counterfeit. That guidance has not been forthcoming." A couple contractors that indicated awareness of written guidance pointed to documents that do not deal specifically with counterfeit components, such as the Federal Aviation Administration's (FAA's) Suspected Unapproved Parts guidance.[60]

[60] Information on this program can be found at http://www.faa.gov/aircraft/safety/programs/sups/

Fifty-one percent of contractors are not aware of liabilities related to the distribution, storage, and disposal of counterfeit parts and 59 percent were not aware of legal requirements. Despite this, a similar percentage (58 percent) said they do not need guidance from the government with regard to these liabilities because they have not had counterfeits. However, one contractor said, "Our investigation has not indicated the existence of any such civil and criminal liability and penalties. We would welcome any guidance in this area."

DIFFICULTY IDENTIFYING COUNTERFEIT PARTS

Given the increase in the proliferation of counterfeits, contractors were asked whether it is difficult for contractors to detect such parts and if this identification is getting more difficult. Fifty-two percent of contractors find it difficult to identify counterfeit parts. Most of this is because counterfeiters and their methods have become increasingly more sophisticated. For example, many counterfeit components have identical markings and performance comparable to authentic parts. Some contractors said it is not cost-effective to perform the extensive testing required to discover counterfeit parts. Other contractors simply did not know what to look for when trying to identify counterfeits.

On the other hand, 48 percent of contractors said they do not find it difficult to identify counterfeit parts. Many of these contractors use only approved and screened vendors, primarily OCMs and authorized distributors. Some said counterfeit identification is not difficult because they require complete traceability of the parts they procure. Several contractors also believe their testing and inspection procedures are sufficient to identify counterfeit components.

While over half of contractors find it difficult to identify counterfeit parts, 60 percent of contractors believe they are better able to identify counterfeit parts now than they were five years ago. This is mainly due to increased awareness among contractors of the counterfeit part problem. Many contractors also have added more testing and screening infrastructure and implemented additional or expanded quality assurance and procurement processes. Some contractors have inserted stricter language and requirements regarding counterfeit components into contracts and purchase orders with suppliers.

Conversely, 40 percent of contractors do not believe they are better able to identify counterfeit parts today. The majority of these contractors contend not to have a problem with or have never encountered counterfeit components. Other contractors commented that they are not better able to identify counterfeit parts because they are still using the same detection methods and processes as they were five years ago.

Reasons for Counterfeits Entering the U.S. Supply Chain

Survey respondents were asked to provide their opinion on the key reasons counterfeit components enter the U.S. supply chain (see Figure V-29). Approximately half of contractors said counterfeit infiltration was due to less stringent inventory management and greater reliance on gray market parts by brokers, and a smaller percentage pointed to the same actions by independent distributors.[61] More than a third of contractors attributed counterfeits in the supply chain to an insufficient chain of accountability.

Almost a third of respondents pointed to inadequate part production by OCMs and premium prices charged by authorized after-market manufacturers.[62] In fact, several contractors said the short supply of parts due to the issues has contributed significantly to the counterfeiting problem. As one contractor said, "Supplier allocation issues provide [the] market opportunity and inflated aftermarket prices provide the incentive."

Related to the issue of after-market availability is the issue of obsolescence, especially in the defense supply chain. Aerospace, space, and defense systems have life cycles that are generally much longer than regular commercial systems. This means many critical parts, which have short production run times, are not manufactured for the entire time they are needed. Many contractors pointed to this shortage of parts as a reason why counterfeits enter the supply chain.

[61] A gray market is the trade of parts through distribution channels which, while legal, are unofficial, unauthorized, or unintended by OCMs.

[62] An after-market manufacturer is a company engaged in the manufacture of electronic products initially but no longer produced by an OCM.

Figure V-29: Prime/Sub Contractors' Top Ten Reasons For Counterfeits Entering the Supply Chain

Less stringent inventory management by parts brokers	49%
Greater reliance by brokers on gray market parts	45%
Greater reliance by independent distributors on gray market parts	40%
Insufficient chain of accountability	39%
Less stringent inventory management by independent distributors	37%
Insufficient buying procedures	31%
Inadequate parts production by OCMs	30%
Purchase of excess inventory on the open market	30%
Insufficient testing of parts	28%
Premium prices charged by after-market manufacturers	28%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Internal and External Actions Taken to Prevent the Infiltration of Counterfeits

Contractors were asked about the internal and external actions they have taken to prevent and mitigate the risk of counterfeit infiltration. Thirty-seven percent of contractors are performing internal screening and testing on inventory in order to stop the proliferation of counterfeits (see Figure V-30). Approximately the same percentage of contractors are training their staff on the negative impacts of counterfeit products. A small percentage of contractors embed new security measures in existing product lines or add security markings to existing inventory.

A third of contractors have taken no internal actions to prevent the infiltration of counterfeits. A number of these contractors have taken no actions because they have not encountered counterfeit parts and/or do not believe counterfeits are a significant issue. A few have taken no internal actions because they have just begun establishing counterfeit avoidance procedures.

Figure V-30: Internal Actions Taken to Prevent Infiltration of Counterfeits – Prime/Sub Contractors

Performing screening and testing on inventory	37%
Training staff on the negative economic and safety impacts of counterfeit products	36%
No internal actions taken	32%
Revising procurement procedures to more carefully screen/audit/evaluate authorized returns from customers	23%
Revising company procedures for disposal of "seconds," defective parts, and production overruns	17%
Other	11%
Increased inspection rates and traceability	6%
Revising procurement procedures to reduce purchases from independent distributors and brokers	4%
Embedding new security measures in existing product lines	2%
Adding security markings to existing inventory	2%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

The majority of contractors (69 percent) are not taking any external actions to prevent the infiltration of counterfeits into their inventory and supply chains (see Figure V-31). A number of these contractors, like those not taking internal actions, do not take external actions because they have not encountered counterfeit parts or do not see counterfeit parts as a problem.

The most common external action taken by contractors is to tighten contractual obligations of contract manufacturers, although only 12 percent of contractors are doing so. Less than 10 percent of contractors are sharing information about counterfeit components with customers, and only two percent said they are participating in industry groups dedicated to the issue of counterfeit parts.

Figure V-31: External Actions Taken to Prevent Infiltration of Counterfeits – Prime/Sub Contractors

No external actions taken	69%
Tightening contractual obligations of contract manufacturers with regard to disposal of “seconds,” defective parts, and overruns	12%
Educating customers/suppliers on the negative economic and safety impacts of counterfeit products	9%
Educating customers about risks associated with gray market products	8%
Other	7%
Referring customers to companies that could identify suitable substitute products or re-engineer system components	6%
Referring customers to authorized after-market manufacturers	5%
Prohibiting authorized distributors from buying back excess inventory on the gray market	5%
Prohibiting authorized distributors from buying back excess inventory from their customers	3%
Contributing/Participating in Industry Work Groups	2%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Overall, prime contractors and subcontractors have demonstrated a mixed level of awareness of counterfeit parts. Most of the contractors that encountered counterfeit parts have taken measures to reduce their risk through testing, inventory audits, revised procedures, and employee training. The majority of contractors do not take any internal or external actions to prevent counterfeits and do not share information with industry and law enforcement authorities consistently. Many of these companies, however, may not be aware of potential problems due to a lack of scrutiny paid to the parts they procure. In general, contractors need to take a proactive approach to counterfeit incidents, making broad efforts to reduce their risk rather than solving problems after they occur.

VI. Department of Defense

The Department of Defense (DOD) is a major end-user of discrete electronic components, microcircuits, and circuit boards. These items are embedded in weapons, transportation, information, and security systems upon which the warfighter depends. Within DOD, the responsibility for procuring and distributing these electronic components resides mainly with the Defense Logistics Agency (DLA). In 2008, DLA had 25 distribution depots, supported 1,603 weapon systems, and conducted over $42 billion in sales and services worldwide.[63]

Recently, however, counterfeit electronics have been uncovered in DOD systems, threatening to erode military readiness and mission capabilities. In March 2008, an article in *Inside the Air Force* found that "an unknown number of counterfeit aircraft parts are being fastened into U.S. military weapon systems after infiltrating supply depots."[64] One DOD official estimated that "such components are leading to a 5 to 15 percent annual decrease in weapon systems reliability."[65]

Higher-than-anticipated demand for electronic components due to the extended conflicts in Iraq and Afghanistan, combined with longer life cycles for weapon systems, have made it difficult for DOD to maintain inventories and procure adequate volumes of electronic parts. The need for obsolete and out-of-production parts, coupled with regulation requirements to procure parts based on the lowest quoted price, has also made it difficult to locate secure and legitimate sources of supply. To satisfy its requirements, DOD has relied on non-traditional supply sources for electronic parts. This has created opportunities for counterfeits to enter DOD inventories and electronics systems.

[63] "About Our Business, " Defense Logistics Agency, May 2009 <http://www.dla.mil/dlabusiness.aspx>.

[64] John Reed, "Fake Parts are Seeping Into Military Aircraft Maintenance Depots," Inside the Air Force, 19.13 (2008).

[65] Ibid.

To capture the unique position and experiences of DOD, OTE surveyed DLA as well as a variety of depots, maintenance centers, and supply centers maintained by the armed services in order to identify the extent to which counterfeits have infiltrated the supply chain.

DOD organizations were asked to classify themselves as arsenals, maintenance depots, fleet readiness centers, fleet industrial supply centers, or DLA depots or supply centers. For ease of analysis, organizations were then classified as either DLA or non-DLA. In total, OTE received 53 completed surveys from DOD – 19 from DLA and 34 from non-DLA organizations (see Figure VI-1). A total of three DLA and 11 non-DLA organizations reported encountering counterfeit parts in some form, a quarter of all DOD respondents.[66]

Figure VI-1: Companies Encountering Counterfeit Electronics

Type of DOD Organization	Encountered Counterfeits	Did Not Encounter Counterfeits	Total
DLA	3	16	**19**
Non-DLA	11	23	**34**
Total	**14**	**39**	**53**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Source of Parts

Most organizations reported that electronic parts are ordered through the FEDLOG, the DOD supply system that “determines the Source of Supply (SoS)” and sends out product requests. Most of the time non-DLA organizations simply request the parts, leaving supplier selection and negotiation to DLA supply centers. This is not always the case, however. Organizations sometimes go outside the DLA system and purchase parts unique to specific armed services from all types of suppliers, including OCMs, contract manufacturers, distributors, or other vendors.

[66] For the purposes of this assessment, the term “counterfeit part” and any variation of it, is used to mean a suspected or confirmed counterfeit part or component.

The 53 DOD organizations surveyed rarely track their procurement in detail. Of these, the highest percentage of parts is purchased from DLA (see Figure VI-2). DLA organizations acquire 48 percent of their parts from other entities within their organization. The data provided by DLA indicates they do not receive a significant percentage of parts from independent distributors, brokers, virtual vendors, or Internet-exclusive sources, although anecdotal evidence provided in the survey and elsewhere suggests otherwise.

Non-DLA organizations claim that 33 percent of the parts they acquire are from DLA organizations. Anecdotal evidence provided in the survey and elsewhere suggests that this percentage is very low. The rest of the parts purchased by non-DLA organizations were reported to come from a variety of other sources.

Figure VI-2: Percent of Parts Purchased by Supplier

Supplier	DLA (15 Organizations)	Non-DLA (19 Organizations)
DLA	48%	33%
DOD Maintenance Depots	17%	9%
Other U.S. Government Sources	10%	8%
Other	7%	11%
Authorized Distributors	3%	12%
OEMs	6%	8%
General Services Administration (GSA)	6%	4%
OCMs	1%	5%
Fleet Readiness Centers	1%	4%
Virtual Vendors	0%	2%
Independent Distributors	0%	2%
DOD Manufacturing Centers	0%	1%
Parts Brokers	0%	1%
DOD Arsenals	0%	0%
Internet-Exclusive Sources	0%	0%
Electronic Salvage Dealers	0%	0%

Source: U.S. Department of Commerce, Office of Technology Evaluation *Counterfeit Electronics Survey*, November 2009.

Nineteen DOD organizations did not respond to the question, explaining they either did not know or did not track how often they use different types of suppliers. One DLA organization stated that “due to the large volume of items we procure and the large number of sources we use, we do not have a breakdown of this volume by type of source.”

INVENTORY ACCESS AND TRADING

Access to the inventory information of other organizations could provide DOD with another avenue to acquire hard to find parts. DOD organizations have varying degrees of access to information on the inventories of the Army, Navy, Air Force, Marines, and other government agencies (see Figure VI-3). Generally, both DLA and non-DLA organizations do not have access to the inventory information of agencies outside DOD. DLA organizations stated that they have no access to National Aeronautics and Space Administration (NASA), Department of Energy (DOE), or Department of Transportation (DOT), including the Federal Aviation Administration (FAA), inventory information.[67] Non-DLA organizations are similar, with only one or two having access to these government agencies.

Figure VI-3: Access to Inventory Information

	DLA Organizations		Non-DLA Organizations	
	Full/Partial Access	No Access	Full/Partial Access	No Access
DLA	72%	28%	72%	28%
Air Force	25%	75%	37%	63%
Navy	37%	63%	47%	53%
Army	25%	75%	31%	69%
Marines	25%	75%	41%	59%
Coast Guard	19%	81%	25%	75%
NASA	0%	100%	13%	87%
Department of Energy	0%	100%	13%	87%
FAA	0%	100%	6%	94%
Department of Transportation	0%	100%	3%	97%
GSA	17%	83%	52%	48%
Sandia National Laboratories	0%	100%	6%	94%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Fifty percent of non-DLA organizations reported having full access and 22 percent reported having partial access to DLA inventory information. Twenty-eight percent of non-DLA organizations say they have no access to this information. It is unclear why different non-DLA organizations have varying degrees of access to the DLA inventory. There are even significant limits to information sharing within DLA; 33 percent of organizations said they have full access,

[67] Many of the electronic parts kept by NASA, the Department of Energy, and other government agencies can often be used for defense applications.

39 percent said they have partial access, and 28 percent said they have no access. It is possible, however, that DLA and non-DLA organizations either do not know that they have access or do not know how to gain access to this information.

ACQUISITION CRITERIA AND BUYING PROCEDURES

DOD organizations were asked to describe their acquisition procedures. DLA makes procurement decisions based upon a variety of regulations, including the Federal Acquisition Regulation (FAR), Defense Federal Acquisition Regulation (DFAR), and other military standards. One major DLA purchaser indicated the means by which it purchases parts differs depending upon the customer. When a request comes in, the respondent DLA attempts to "purchase the item our customer asks us to purchase using the documentation they provide." This documentation can range from part numbers and CAGE codes to technical drawings.[68]

As stated previously, non-DLA organizations usually purchase parts from DLA through the FEDLOG system. If unable to find parts through this system, however, organizations will attempt to "research known and reputable parts sources and procure through them." Should parts still be difficult to find, non-DLA survey respondents said they will seek out nearly any supplier that can fulfill their requirements.

DOD organizations also ranked the top three factors that influenced their part acquisition decisions. Quality, cost, and part availability were the top factors for DLA organizations (see Figure VI-4). One such organization stated its "first priority is to provide the right item (quality) at the right time (speed) and place…cost is an important consideration as well." Although this statement reflected the sentiments expressed by DLA, it is not necessarily in line with other evidence provided by non-DLA organizations regarding DLA purchasing procedures. For their own purchases, many non-DLA organizations complained that interpretations of the DFAR restrict their purchasing decisions, forcing them to buy from the lowest bidder, in most cases.

[68] A CAGE code is a five position code that identifies companies doing or wishing to do business with the U.S. Government.

There was a significant difference between DLA and non-DLA organizations when asked if they could purchase parts for reasons other than "low bid."[69] Only 21 percent of DLA organizations reported being able to purchase parts for reasons other than low bid, while 52 percent of non-DLA organizations can do the same. Three non-DLA organizations provided reasons for not being able to circumvent low bid requirements, which included adherence to the DFAR, specific Navy regulations, and Small Business Administration (SBA) rules.

Figure VI-4: Top Factors Influencing Part Acquisitions*

DLA Factors	Non-DLA Factors
Quality	Part Availability
Cost	Quality
Part Availability	Cost
Delivery Speed	Trustworthiness of Supplier
	GSA Listing
	Delivery Speed
	Distributor Status
	Previous Supplier Performance

*** Only includes those factors that received a response. Factors are ranked from most influential to least.**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey,* November 2009.

Problems with Inventory Levels

With extended life cycles for weapon systems and a larger than anticipated demand for parts (due in part to ongoing conflicts in Iraq and Afghanistan), DOD has at times had problems maintaining adequate inventory levels for electronic parts. DLA and non-DLA organizations identified a range of factors contributing most to inadequate parts supplies. Insufficient spares in inventory was the most commonly cited cause, while high demand for replacement parts and higher than anticipated utilization of parts were also top explanations (see Figure VI-5).

[69] Other procurement strategies, such as "best value," involve paying higher prices for higher quality parts rather than entirely cost-based purchasing.

DOD organizations also cited failure to plan for redesigns as parts go out-of-production. Although redesigns are an expensive and time-consuming solution to obsolescence, they can eliminate the problem of finding an adequate, secure part substitute. Lastly, survey respondents cited structural changes in DOD-wide parts inventories. There is evidence that the closing of storage and maintenance facilities has caused excess inventories of parts to be surplused.

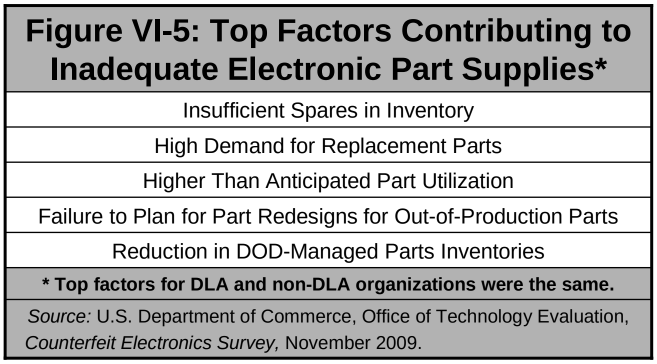


Figure VI-5: Top Factors Contributing to Inadequate Electronic Part Supplies*
Insufficient Spares in Inventory
High Demand for Replacement Parts
Higher Than Anticipated Part Utilization
Failure to Plan for Part Redesigns for Out-of-Production Parts
Reduction in DOD-Managed Parts Inventories
*** Top factors for DLA and non-DLA organizations were the same.**
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey,* November 2009.

OTHER PROCUREMENT CRITERIA

DOD organizations identified other criteria used to choose their parts suppliers and the parts they receive. Most DOD organizations do not require suppliers to disclose the country of origin for parts procured in advance of contract approval. Only 11 percent of DLA organizations and 24 percent of non-DLA organizations require country of origin information in advance of purchase. If parts from other countries are purchased, only 21 percent of DLA organizations and three percent of non-DLA organizations have special policies in place to handle them. Overall, these policies regarding parts from other countries are inconsistent between organizations and do not necessarily involve additional scrutiny or testing.

Most DOD organizations do not fully evaluate their commercial electronic suppliers before they commence business with them (see Figure VI-6). In fact, 74 percent of DLA and 58 percent of non-DLA organizations do not evaluate business practices, past performance, locations, or facilities before placing orders with a commercial supplier. Those DLA organizations that evaluate their suppliers rely heavily upon Qualified Manufacturer List (QML) and Qualified Product List (QPL) inspections and audits to ensure the quality of a commercial vendor.[70]

Figure VI-6: Factors Evaluated Before Commencing Business With Commercial Suppliers

Factor	DLA Organizations	Non-DLA Organizations
Business Practices	21%	30%
Experience & Past Performance	11%	39%
Supplier Location	16%	27%
Warehouse Facilities	5%	9%
Other	5%	0%
Do Not Evaluate Any Factors	74%	58%

Source: U.S. Department of Commerce, Office of Technology Evaluation *Counterfeit Electronics Survey*, November 2009.

Non-DLA organizations largely rely upon others in the procurement supply chain to evaluate the capabilities and performance of potential suppliers. Many of these organizations assume that those that negotiate purchasing contracts (DLA and non-DLA purchasing agents) evaluate suppliers beforehand.

Survey results show non-DLA organizations are primarily concerned with receiving the parts that they request, not how they are acquired. When parts are not available through standard methods, their main priority is to find any possible supplier. One non-DLA organization noted "when the information is available it is checked. There are times when a source is the only means of purchasing a component and [these] factors cannot be verified."

In addition, most DOD organizations do not require their commercial suppliers to adhere to any particular industry quality standards concerning electronic parts (see Figure VI-7). For example, only 34 percent of DLA and 11 percent of non-DLA organizations require suppliers to be ISO 9000 certified.[71] Organizations offered two main reasons why they do not require any or limited

[70] According to the Federal Acquisition Regulations (FAR), the QML is "a list of manufacturers who have had their products examined and tested and who have satisfied all applicable qualification requirements for that part. The QPL "is a list of products that have been examined, tested, and have satisfied all applicable qualification requirements."

[71] ISO 9000 is a standard created by the International Standards Organization on creating quality management systems.

standards. First, many organizations do not have purchasing authority for electronic parts and rely upon DLA supply centers to set requirements. Second, if a part is not readily available, non-DLA organizations will attempt to acquire it through their next best option. Therefore, when in need, parts are purchased based upon availability, not upon a supplier's business practices or qualifications.

Figure VI-7: Percent of DOD Organizations That Require Commercial Suppliers to Conform to Industry Standards

Factor	DLA Organizations	Non-DLA Organizations
ISO 9000	11%	34%
IDEA 1010	5%	3%
JEDEC 31C	0%	6%
EIA/G-12 Engineering Bulletin	0%	3%
Other	0%	3%
Do Not Require Any Industry Standards	89%	69%

Source: U.S. Department of Commerce, Office of Technology Evaluation *Counterfeit Electronics Survey*, November 2009.

Few DOD organizations said they allow their suppliers to ship electronic parts directly to domestic and foreign depots and field centers. On this topic, one DLA organization stated that:

> "Parts are never delivered to a DLA supply center so any shipment to any location as required by contract is not 'bypassing' the supply center. DLA does have parts shipped to our depots as well as directly to our customers and/or their depots."

Sixteen percent of DLA and 10 percent of non-DLA organizations allow parts to bypass DLA supply centers and go straight to domestic depots and centers. In addition, two organizations, one DLA and one non-DLA, permit this practice for foreign field centers.

In cases such as this, parts are going directly to the end-user without any form of testing performed by DLA. This practice can add risk, considering that many non-DLA organizations assume incoming parts have been inspected by DLA prior to shipment.

Procurement Risk Models

Two of the 53 DOD organizations surveyed, one DLA and one non-DLA, employ risk models when purchasing electronic parts. Many organizations explained that they do not have a risk model because they rely upon DLA supply centers to make purchasing decisions. The sole DLA organization that does employ a risk model assesses the past performance of the supplier, making purchasing decisions based on a "history of quality and performance issues." The non-DLA risk model involves conditional approval for sources and "first article testing" to verify the conformance of the supplier.[72]

Many DOD organizations rely upon another organization in the supply chain to perform cost-benefit analysis when purchasing electronic parts. Forty-seven percent of DLA and 45 percent of non-DLA organizations rely upon, for the most part, DLA supply centers to perform a cost-benefit analysis during purchasing. As seen above, however, only one such DLA organization regularly employs a risk model when purchasing electronic parts.

Counterfeit Incidents

DOD organizations were asked to quantify their encounters with counterfeit electronics by type of defect, method uncovered, and platforms that were affected.[73] Of the 53 DOD organizations surveyed, three DLA and 11 non-DLA organizations indicated they encountered counterfeits between 2005 and 2008. Only three of these 14 organizations were able to provide details about these incidents beyond the type of parts involved.

[72] "First article testing" is a series of inspections and tests designed to ensure parts conform to drawings or part specifications.

[73] For the purposes of this study, an incident is a single encounter of a suspected/confirmed counterfeit part. An incident could involve one part or a thousand parts of a component.

Tracking Database for Counterfeits

Very few DOD organizations maintain an internal tracking database for counterfeit electronics. Only two of the 14 organizations that encountered counterfeits maintain such a database, both of which are non-DLA. In some cases, DOD organizations create incident reports for non-conforming parts, but almost none specifically record incidents of counterfeit parts.

DOD is largely reactive, only identifying counterfeit parts and fraud after it occurs. Many DOD organizations assess parts by making sure the part numbers match the items listed on the purchase order, not by evaluating part performance. If parts make it past this verification step, explained one respondent, most organizations will "only be aware of a counterfeit issue if [the part] failed, in which case we would issue a [Product] Quality Deficiency Report."[74]

Type of Counterfeit Parts

DOD organizations encountered counterfeit versions of every type of discrete electronic component, microcircuit, bare circuit board, and assembled circuit board listed in the OTE survey (see Figures F-1 through F-4 in Appendix F). As noted earlier, most DOD organizations did not track how many total counterfeit incidents they encountered over the 2005-2008 period. It is therefore not possible to identify which type of parts, if any, are more at risk of being counterfeits.

Type of Problems and Method of Discovery

The 53 DOD organizations were largely unable to identify what type of counterfeit parts they were receiving. [75] To verify these responses, OTE staff conducted follow-up phone calls with

[74] A Product Quality Deficiency Report (PQDR) is a form used by the military services and the General Service Administration to record and transmit data on defects or nonconforming conditions detected on new or newly reworked Government-owned products, premature equipment failures, and products in use that do not fulfill their expected purpose, operation or service.
[75] The definition of counterfeit parts used in the OTE study is specific to this assessment, and is broader than definitions typically used by industry.

several DOD entities. Only one non-DLA organization kept track of counterfeit incidents by type of counterfeit, identifying 32 incidents of “fake [non-working] OCM product” in 2007 and 2008.

DOD organizations were also unable to categorize how counterfeits were uncovered; only three maintained records of how these parts were identified. These organizations primarily discovered counterfeit parts when defective or through testing. Some DOD organizations said they did not know how counterfeits were being uncovered because they have never encountered counterfeit parts. Other respondents stated they handled too many parts to know how counterfeits were uncovered or had no method in place to track this information.

TYPE OF PLATFORMS AFFECTED BY COUNTERFEITS

DOD organizations were asked how their exposure to counterfeit electronics has affected the military platforms they are responsible for maintaining. Specifically, organizations were asked to identify the sub-systems affected, number of units affected, and average out-of-service time for each platform that experienced counterfeit issues. Only one of the 14 organizations experiencing counterfeits identified a problem with a platform – a counterfeit discovered during repairs of a communications system for an aircraft. The remainder of the survey respondents provided no information on how systems have been affected by counterfeit components.

DOD organizations provided no evidence that they trace counterfeit parts to the platforms they affect. This is consistent with the fact that few organizations keep detailed records of counterfeit incidents. With no way to identify trends or patterns in counterfeit parts penetrating its supply chain, there is no reliable method within DOD for identifying which platforms or systems may be at risk when an incident occurs.

INVENTORY CONTROL AND TESTING

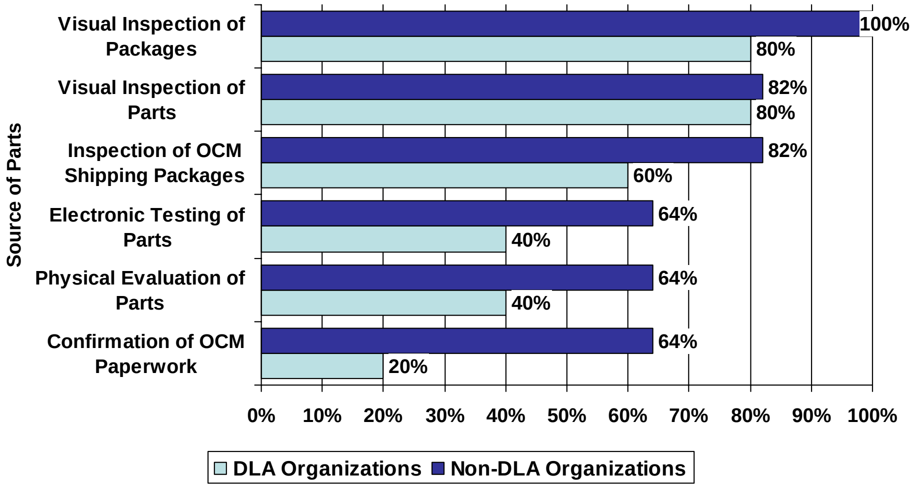
Inventory control is an important element of any effort to prevent counterfeit parts from entering systems. Testing and quality control is primarily a DLA function because of its central procurement role, although depots also have a responsibility for maintaining parts inventories. Overall, survey data showed that testing levels are low, inspection standards are inconsistent, and communication between DLA and non-DLA organizations is uneven.

PRE-STOCK TESTING

DOD organizations were asked to identify the methods of pre-stock testing they use to verify parts before they are placed in inventory. Only 26 percent of DLA and 32 percent of non-DLA organizations undertake any type of pre-stock testing. This testing could include visual inspection of packages and paperwork, confirmation of OCM pedigree paperwork, visual inspection of parts, electronic testing, or physical evaluation.

Based on DLA comments, the limited amount of testing consists primarily of visual inspection techniques (see Figure VI-8). This visual inspection is not necessarily designed to identify counterfeit parts but to “verify part number(s) with stock number(s) to ensure [the] item received matches shipping documentation.” Beyond this initial documentation check, there is no consistent practice of pre-stock testing across organizations. Some DLA organizations said they perform “first article testing” when they use a new vendor, some perform more in-depth visual inspections depending on the source, and some perform no additional verification.

Figure VI-8: Percent of DOD Organizations Conducting Each Type of Pre-Stock Testing*



*** Percentage is taken out of the companies that do any type of pre-stock testing**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

When non-DLA organizations test incoming parts, they primarily visually inspect part documentation before placing parts in inventory. Although survey responses indicate these organizations are more likely to conduct electronic or physical testing than DLA entities, many simply catalog the parts they receive and place them in a bin. Some of this behavior may be explained by the fact that 38 percent of non-DLA organizations say they rely upon DLA to assure the quality of delivered parts.

DOD organizations were also asked whether they require parts suppliers to provide verification from internal or independent testing facilities that the parts they ship are genuine and meet OCM performance specifications. This type of verification is not very common for DOD organizations, only 24 percent of DLA and 48 percent of non-DLA organizations requiring it. For the most part, organizations believe this verification is either implicitly required in purchasing contracts or is the responsibility of the DLA inventory control point (ICP), such as Defense Supply Center Columbus (DSCC). Although some DOD organizations evaluate suppliers before they purchase parts, they only require verification that the parts ordered meet the purchase order, not that they are genuine and meet performance specifications.

Co-Mingling of Inventory and Auditing Practices

If a counterfeit component makes it past acquisition and pre-stock testing procedures, there are additional opportunities to uncover the part if a DOD organization conducts periodic inventory audits. However, organizations that co-mingle identical parts from multiple suppliers in the same storage bin without accompanying documentation can significantly diminish or eliminate part traceability. Eighty-seven percent of DLA and 55 percent of non-DLA organizations co-mingle electronic parts in the same bin. Given the low levels of counterfeit tracking, pre-stock testing, and part verification, co-mingling within DOD organizations exacerbates potential counterfeit problems.

Only 16 percent of DLA and 17 percent of non-DLA organizations conduct inventory audits for counterfeits. For the most part, these audits are conducted on a "random" basis and are usually triggered by allegations of problematic parts or supplies. This indicates that even if inventory audits are performed, they are not necessarily undertaken as a method to proactively identify and protect against counterfeit parts.

This lack of auditing for counterfeits becomes more evident considering how few DOD organizations ordered product models to be visually inspected, electronically tested, or physically evaluated. Only 11 percent of DLA organizations ordered at least one product model to be tested, although many did not keep track of this information (see Figure VI-9).

Figure VI-9: Percent of DOD Organizations Testing at Least One Product Model by Test Type in 2008

	Visual Inspection	Electronic Testing	Physical Evaluation*
DLA Organizations	5%	11%	5%
Non-DLA Organizations	3%	0%	3%

*** Physical evaluation may have been misinterpreted to mean a type of visual inspection, rather than destructive testing**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

DLA organizations generally conduct visual inspection to assess "kind, count and condition [of parts] at time of receipt," not to specifically detect counterfeit parts. One of the few DLA organizations that does test said, "We perform numerous tests on parts received and in inventory due to a variety of reasons, but they are targeted to suspected concerns." Even those few DLA organizations that test parts do so reactively, after problems have surfaced.

Testing is less common among non-DLA organizations. For the most part, non-DLA organizations are concerned with stocking and installing parts received from DLA and other sources, not with whether or not the part is counterfeit. Non-DLA organizations usually do "not have a counterfeit parts screening process, [these] issues are discovered incidentally." One non-DLA organization that visually inspects parts at the time of installation stated that "it is not practical to believe the part would or could be determined to be counterfeit."

Visual Inspection Criteria

As stated previously, the vast majority of testing performed by DOD organizations is visual rather than electronic or physical. There are a wide range of visual inspection criteria that organizations can utilize to try to confirm part authenticity, but only 47 percent of DLA and 46 percent of non-DLA organizations said they examined parts for any visual criteria. As with auditing, DOD organizations indicated that visual inspections are "intended to ensure the accuracy [and] completeness of all received/shipped parts," not to discover counterfeits.

Those that conduct visual inspections almost always confirm the part number of electronic components (see Figure VI-10). Beyond this, most DOD organizations examine serial numbers, dates and places of manufacture, and marking techniques, but not many examine more in-depth visual criteria, such as surface texture, holograms, or covert markings.

Figure VI-10: Percent of DOD Organizations Utilizing Visual Inspection Criteria*

Criteria	DLA Organizations	Non-DLA Organizations
Part Number	100%	92%
Serial Number	75%	77%
Date of Manufacture	63%	69%
Place of Manufacture	63%	69%
Marking Techniques	50%	69%
Bar Coding	63%	54%
Surface Texture	38%	46%
Trademarks	25%	54%
Embedded Authenticity Data	38%	38%
RFID	50%	31%
Covert Markings	25%	38%
Holograms	25%	8%
Other	25%	0%

*** As a percent of companies utilizing at least one of the criteria**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Some DLA and non-DLA organizations said they cannot perform counterfeits testing because they have inadequate training, personnel, and facilities. In fact, 89 percent of DLA and 82 percent of non-DLA organizations do not use any internal or contractor-operated facilities to test or inspect parts for counterfeits.

PERSONNEL TRAINING

While DOD conducts a wide-variety of training programs for its personnel, only 17 percent of DLA and 31 percent of non-DLA organizations actively train personnel on how to perform visual screenings for electronic components.[76] Compounding the lack of training, even fewer DOD entities – 22 percent of DLA and 17 percent of non-DLA organizations – have a designated person for handling suspected or confirmed counterfeit electronics. Almost all DOD organizations identified an interest in training on screening for counterfeits, given the necessary and available resources.

[76] The DLA and non-DLA visual screening training programs were implemented between 1978 and 2008.

THE DFAR AND PROCUREMENT

The DFAR set the basic legal guidelines and rules by which defense procurement takes place. To understand how the DFAR affects defense procurement, DOD organizations were asked a series of questions about the regulation, other procurement protocols, and what changes should be made to prevent counterfeit infiltration. Based on survey responses, the DFAR as currently structured seems to promote a procurement system that favors the lowest priced items rather than the best overall value. While such a system can be very cost effective, it can also allow price to dictate suppliers and increase the risk of counterfeit incidents.

Only 28 percent of DOD organizations said that the DFAR contains sufficient provisions to prevent counterfeit parts from infiltrating the defense supply chain. One DLA organization stated that "there is no doubt that counterfeit components are in our supply system, yet we still have no method of identifying it or controlling those suppliers that sell counterfeit components. [This] indicates that we have inadequate procuring procedures to address this issue."

Most of the DOD organizations that provided reasons why the DFAR is inadequate stated that the DFAR does not specifically discuss counterfeit electronics. As has been shown, without specific policies in place that identify and address the problem, the risk of counterfeits penetrating the defense supply chain will remain.

Most of these organizations also said that the DFAR should be modified to help prevent counterfeit parts from entering the supply chain. The proposal suggested most often was to edit the DFAR to reduce the emphasis placed on small business considerations and lowest bidder, and to allow organizations to select suppliers based on "best value." Many DOD organizations said they feel the DFAR "forces those who are responsible for procuring piece parts to buy from unauthorized distributors or independent sources."

DOD organizations also were asked if they have written procurement protocols in place, not including the DFAR, to minimize the risk of receiving counterfeit electronic components. Only 11 percent of DLA and nine percent of non-DLA organizations have such policies. All of these procurement protocols were created at the organizational level, rather than through a DOD-wide directive.

Only one DLA and two non-DLA organizations include obligations regarding counterfeit parts in their procurement contracts with commercial suppliers. The two non-DLA organizations require their suppliers to perform inventory checks, keep logs of counterfeit products, and notify federal authorities and their organization if counterfeits are encountered. The DLA organization that added obligations regarding counterfeit parts in its procurement contracts did not specify what type of requirements it imposes on its suppliers.

ACTIONS TAKEN REGARDING COUNTERFEITS

In addition to having few preventative policies to protect against counterfeits, DOD organizations generally do not take strong measures once a counterfeit incident occurs. Only five of 53 DOD organizations, and one of the 14 that encountered counterfeits, stated that they have written procedures directing staff on what to do if they encounter suspected or confirmed counterfeit parts. Guidance provided by the written procedures to staff is similar between the five DOD organizations and focused on non-conforming parts. According to two of the five organizations, any suspicion of fraudulent activity would be reported and would prompt an investigation into the supplier and the parts.

Only two of the 14 DOD organizations that encountered counterfeits require their staff to report incidents of suspected or confirmed counterfeit parts. Of these, only one DOD organization filed an incident report for a counterfeit part in the 2005-2008 period. The other 13 DOD organizations that encountered counterfeits did not file any incident reports during the reporting period. This minimal reporting makes it nearly impossible for DOD organizations to identify patterns of misconduct or areas where procurement procedures need to be modified.

In addition to not having written policies in place, the majority of DOD organizations do not take any actions once they have possession of a suspected or confirmed counterfeit part (see Figure

VI-11).[77] If an organization does act, they most likely notify management and write up an incident report on the incident.

Figure VI-11: Steps Taken After Possession of Counterfeit Parts – Department of Defense Organizations

Step	DLA Organizations	Non-DLA Organizations
None at All	68%	62%
Notify Management	16%	21%
Hold the part, OCM data sheet, procurement paperwork, and packaging and write up a report	21%	15%
Quarantine Parts	11%	15%
Conduct Random Inventory Testing	11%	9%
Enter Into an Electronic Database	11%	9%
Request Credit	11%	9%
Test Part	5%	12%
Other	11%	6%
Issue Credit	11%	6%
Turn Over to Law Enforcement Authorities for Analysis	5%	9%
Leave Disposal Up to Party Filing Complaint	5%	6%
Retain Samples for Future Reference	5%	6%
Check industry/USG databases for similar problems	5%	3%
Return Parts	0%	6%
Dispose of Parts Almost Immediately	0%	3%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

The majority of DLA and non-DLA organizations also do not contact any government authorities if a counterfeit incident occurs (see Figure VI-12). If authorities are notified, they tend to be within DLA rather than defense-related investigative services or other law enforcement agencies.

[77] Some respondents answered this survey question from the perspective of what they would do if they had possession of counterfeit parts, and not what they have done.

Figure VI-12: Authorities Notified After Counterfeit Incidents – Department of Defense Organizations

Authority	DLA Organizations	Non-DLA Organizations
None at All	68%	62%
Defense Logistics Agency (DLA)	32%	26%
Parts Suppliers	5%	21%
DCMA	16%	6%
Other	5%	12%
Defense Related Investigative Services	11%	3%
Government-Industry Data Exchange Program (GIDEP)	5%	3%
Non-Defense Related Investigative Services	5%	0%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

There is also very little information sharing through databases, which law enforcement authorities, industry, and other DOD entities use for information on counterfeits. Very few DOD organizations check industry or government databases for information on counterfeit electronics that could impact them. Eleven percent of DLA and 20 percent of non-DLA organizations check at least one database, usually the GIDEP database.

DIFFICULTY IDENTIFYING COUNTERFEITS

DOD organizations were asked whether or not they have difficulty identifying counterfeit components. The vast majority of DLA organizations (82 percent) said they have difficulty identifying counterfeit parts. Six of these organizations attributed their difficulty to a lack of training concerning counterfeit electronics or inadequate staffing levels.

Their difficulty also stems from the fact that, for the most part, DLA counterfeit detection is reactive, uncovering parts only after they are put into systems and subsequently fail. One organization said that “the only way we would identify a counterfeit part is if we noticed an unexplained rise in failures or Quality Deficiency Reports for a particular item.” The few DLA organizations that had no difficulty identifying counterfeits either have access to or utilize advanced testing equipment, such as decapping or x-ray machines, to make counterfeit identification easier and more accurate.[78]

Approximately half of non-DLA organizations find it difficult to identify counterfeit parts. Although this number is lower than DLA organizations, five non-DLA organizations said they have not had difficulty because they have not found any counterfeit parts. Overall, the non-DLA organizations that have difficulty pointed to the complex nature of the defense supply chain. As with DLA organizations, non-DLA respondents said lack of training and resources prevent many organizations from taking a comprehensive approach to counterfeits.

DLA and non-DLA organizations generally agreed that they were not able to better control the infiltration of counterfeits today than they were five years ago. Survey respondents stated there have been no DOD-wide policies put in place to prevent counterfeit electronics from infiltrating the supply chain. One DLA organization said it "did not have any methods of identifying counterfeit components five years ago [and] we still do not have any today."

Even DOD organizations reporting that they are better able to handle counterfeits said they were able to do so as a result of their individual efforts, not through a DOD-mandated policy. A non-DLA organization stated that they have "educated some of [their] senior technicians on what to look for, but without a formal process [counterfeit identification it] is hit or miss."

REASONS FOR COUNTERFEITS ENTERING THE U.S. SUPPLY CHAIN

Few DOD organizations provided reasons for counterfeit products entering the U.S. supply chain. The majority of DOD organizations that did not respond claimed that this type of conjecture was beyond their expertise.

For those that responded, the most common reasons for counterfeit infiltration cited were an insufficient chain of accountability, insufficient buying procedures, and insufficient testing (see

[78] Decapsulation, or decapping, is when the packing of a component is opened in hermetic conditions to allow for the examination of the die and internal features of the package.

Figure VI-13). A smaller but significant number of question respondents cited inadequate parts purchase planning by contract manufacturers and OCMs and insufficient notice of part production termination.

Organizations also provided many additional explanations not pre-identified in the OTE survey, including:

- parts purchased from the lowest bidder due to the DFAR;
- high reliance upon obsolete parts for aging weapon systems;
- lack of additional screening procedures for parts purchased from independent distributors or brokers as opposed to OCMs;
- use of contractors to buy spare parts, many of which do not test for counterfeits; and
- depot technicians have not been trained in how to identify counterfeit parts.

Figure VI-13: DOD Organizations' Top Ten Reason For Counterfeits Entering the Supply Chain*

Insufficient chain of accountability	83%
Insufficient buying procedures	78%
Insufficient testing	78%
Less stringent inventory management by independent distributors	72%
Less stringent inventory management by parts brokers	72%
Greater reliance on contract manufacturers for procurement	67%
Less stringent inventory management by authorized distributors	67%
Inadequate parts purchase planning by contract manufacturers	61%
Inadequate parts purchase planning by OEMs	61%
Insufficient notice to customers of part production termination	61%

*** Percentage is out of 18 DLA and non-DLA organizations who responded.**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

INTERNAL ACTIONS TAKEN TO PREVENT INFILTRATION OF COUNTERFEITS

DOD organizations were asked what actions they are taking internally to prevent the infiltration of counterfeit electronics. Despite the fact that many organizations recognized counterfeits as a potential problem, 83 percent of DLA and 59 percent of non-DLA organizations have not taken any internal actions to protect themselves against counterfeits (see Figure VI-14). Many organizations stated, however, that they cannot make progress toward minimizing the risk of counterfeits without the support of a Department of Defense-wide policy. In separate conversations, DLA said it was taking steps at Defense Supply Center Columbus, its main parts distribution center, to establish counterfeit avoidance measures.[79]

Figure VI-14: Internal Actions Taken to Prevent Infiltration of Counterfeits – DOD Organizations

Action	DLA Organizations	Non-DLA Organizations
No internal actions taken	83%	59%
Performing screening and testing on inventory	17%	24%
Training staff on the negative economic and safety impact of counterfeit products	11%	21%
Revising organization procedures for disposal of "seconds," defective parts, and production overruns	11%	14%
Revising procurement to more carefully screen/audit/evaluate authorized returns from customers	11%	14%
Adding security markings to existing inventory	6%	10%
Embedding new security measures in existing product lines	6%	0%
Embedding new security measures in product lines	0%	0%
Other	0%	0%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Overall, there is no consistent policy or procedures within DOD organizations specifically designed to identify and screen for counterfeit electronics. Due to inadequate training, awareness, and resources, organizations are unable to detect counterfeit electronic parts before they are incorporated into fielded systems. Moreover, many DOD organizations said they are not certain how pervasive counterfeits are within their current inventories because they do not inspect at many of the critical entry points into their supply chain. As an end-user, DOD organizations seem to rely on other entities in the supply chain to verify the authenticity of electronic parts.   The issue is further compounded by limited reporting, minimal record keeping, and a lack of information sharing within DOD, as well as between DOD and other organizations. To address the problem of counterfeit parts, DOD needs to implement effective and comprehensive counterfeit identification and avoidance practices and protocols throughout the military services and DLA.

[79] Appendix G contains information on the steps Defense Supply Center Columbus is taking to establish counterfeit avoidance measures.

VII. CROSS-SECTOR ANALYSIS

The proliferation of counterfeit parts is not limited to occasional, isolated incidents, but is increasingly present at every level of the supply chain. Nor are incidents of counterfeit components restricted to one class of suppliers, specific discrete electronic component or microcircuit product lines, or older "legacy" components. The five sectors examined in this report – original component manufacturers (OCMs), authorized and unauthorized parts distributors, circuit board assemblers, prime contractors and subcontractors, and the Department of Defense (DOD) – provided unique and in-depth insights on the proliferation of counterfeits at various stages of the supply chain. While the behavior of each sector is important, none of them operate independently of each other. Data collected by the Office of Technology Evaluation (OTE) demonstrates that counterfeit electronic components are infiltrating commercial, industrial, and defense product manufacturing supply chains across the five sectors.

Of the 387 organizations responding to the survey, 152 organizations from all five sectors (39 percent) encountered counterfeits at least once during the 2005-2008 period (see Figure VII-1). [80]

[80] For the purposes of this assessment, the term "counterfeit part," and any variation of it, is used to mean a suspected or confirmed counterfeit part.

Figure VII-1: Organizations Encountering Counterfeit Electronics

Type of Company/Organization		Encountered Counterfeits	No Counterfeit Incidents	Total
Original Component Manufacturers	Discrete Electronic Components	18	21	**39**
	Microcircuits	24	20	**44**
Distributors	Authorized Distributors	10	35	**45**
	Unauthorized Distributors	44	9	**53**
Board Assemblers		11	21	**32**
Prime/Sub Contractors		31	90	**121**
Department of Defense	DLA Organizations	3	16	**19**
	Non-DLA Organizations	11	23	**34**
Total		**152**	**235**	**387**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey,* November 2009.

SOURCES OF PARTS

Distributors, circuit board assemblers, and prime contractors and subcontractors were asked to identify the types of parts they purchase – discrete electronic components, microcircuits, bare circuit boards, and assembled circuit boards – as well as the entities that supply the parts.[81] The majority of these companies purchase parts from OCMs, authorized distributors, and independent distributors (see Figure VII-2). It should be noted, however, that respondents in all three sectors purchase electronic parts from a variety of sources, including Internet-exclusive sources, contract manufacturers, and the Defense Logistics Agency (DLA).

[81] OCMs were not asked this question, as they manufacture the electronic parts in question and do not purchase them. DOD was asked this question, but the data provided was inconsistent and not useable for comparison.

Figure VII-2: Percent of Companies Purchasing Parts From Different Suppliers

Type of Supplier	Distributors	Circuit Board Assemblers	Prime/Sub Contractors
OCMs	88%	91%	89%
Authorized Distributors	85%	97%	89%
Independent Distributors	72%	88%	77%
Brokers	63%	9%	56%
OEMs	57%	66%	22%
Internet-Exclusive Sources	44%	28%	26%
Contract Manufacturers	39%	9%	17%
DOD Depots	7%	0%	11%
DOD Manufacturing Centers	6%	0%	7%
DOD Surplus	4%	0%	7%
DLA	2%	3%	11%

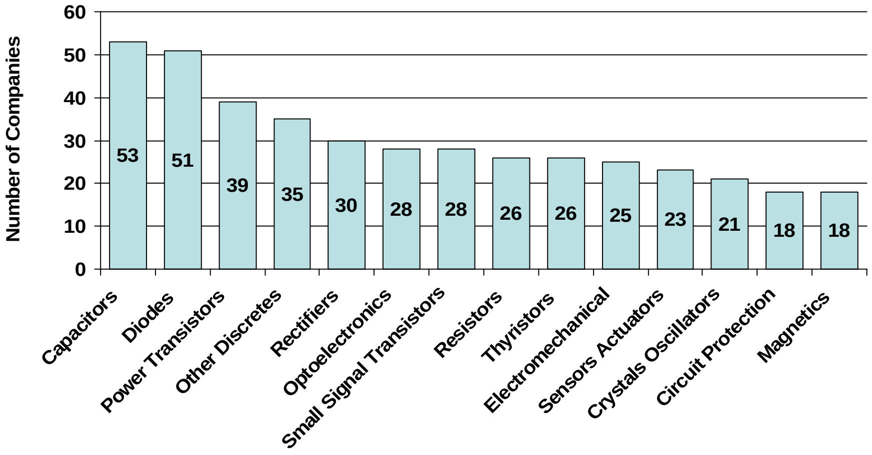
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey,* November 2009.

COUNTERFEIT INCIDENTS

Not all electronic components are counterfeited with the same frequency or in the same volume. For discrete electronic components, counterfeit parts were reported by survey respondents across 14 component categories for the 2005-2008 period. Organizations reported encountering counterfeit parts in all component categories, with capacitors and diodes being the most prevalent (see Figure VII-3).

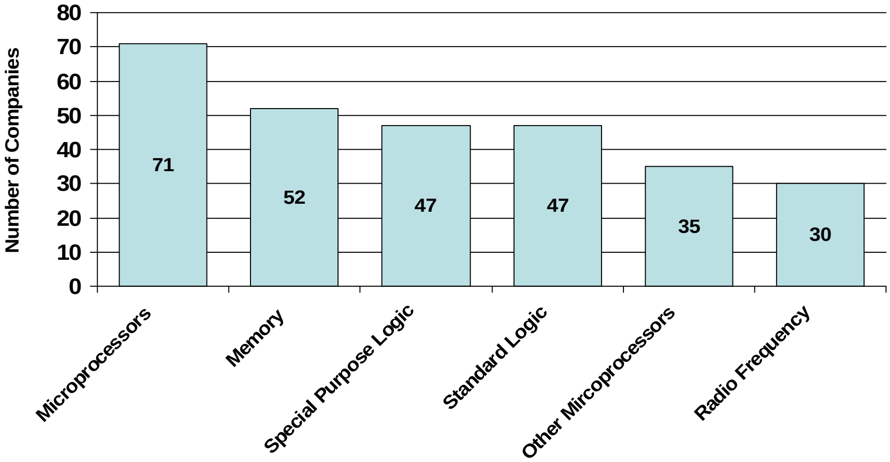
Many organizations encountered counterfeit microcircuit products across six product categories. The largest product area for counterfeit microcircuits is microprocessors, with 71 organizations having encountered counterfeit versions (see Figure VII-4). Another 52 organizations reported problems with counterfeit memory devices.

Figure VII-3: Types of Parts Suspected/Confirmed to be Counterfeit - Discretes



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

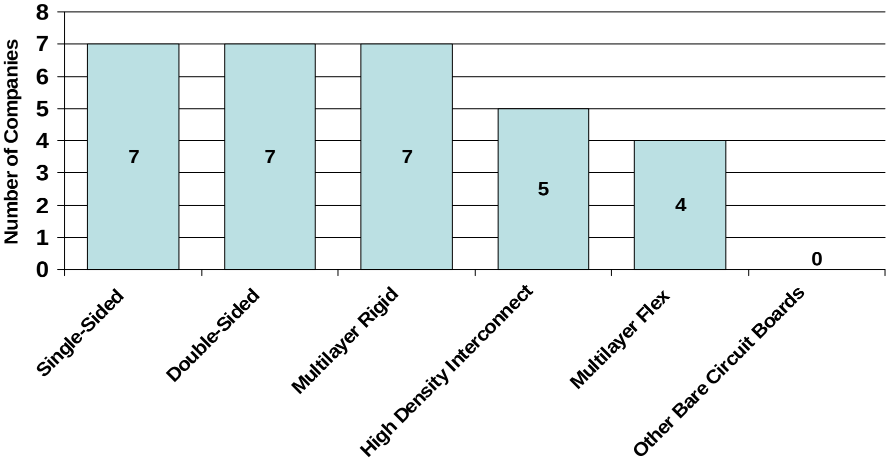
Figure VII-4: Types of Parts Suspected/Confirmed to be Counterfeit - Microcircuits



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Survey respondents were also asked to identify the counterfeit bare circuit boards they encountered across six product categories between 2005 and 2008. The types of bare circuit boards with the highest numbers of counterfeits were single-sided, double-sided, and multilayer rigid circuit boards (see Figure VII-5).

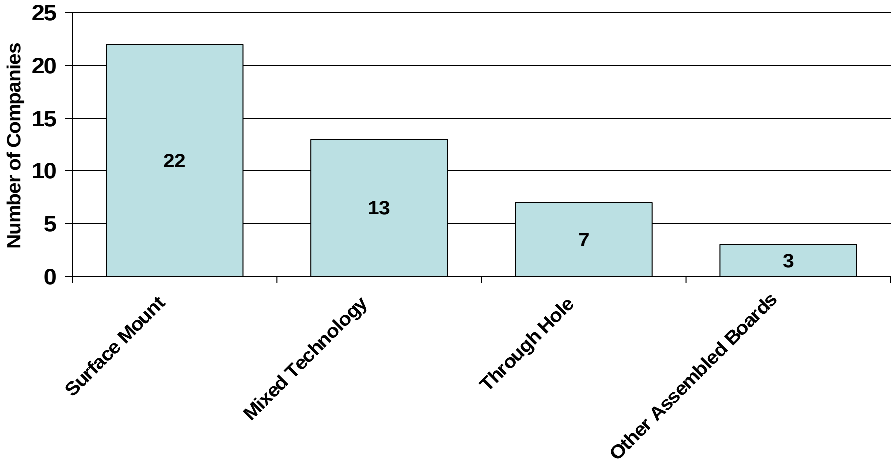
Figure VII-5: Types of Parts Suspected/Confirmed to be Counterfeit – Bare Circuit Boards



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

With respect to assembled circuit boards, organizations reported counterfeit parts in four product categories across the survey time period. The largest number of respondents reported encountering counterfeit surface mount assembled circuit boards (see Figure VII-6).

Figure VII-6: Types of Parts Suspected/Confirmed to be Counterfeit – Assembled Circuit Boards

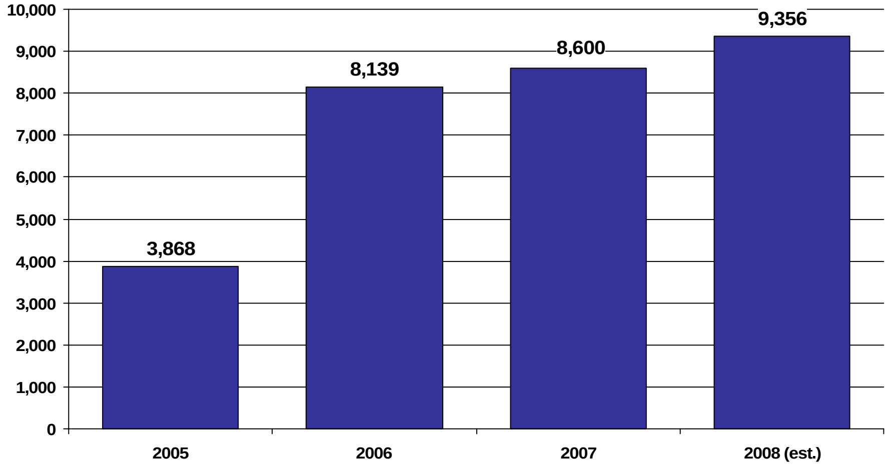


Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

For the five survey sectors, the number of counterfeit incidents for all electronic part types climbed dramatically from 3,868 cases in 2005 to 9,356 cases in 2008 (see Figure VII-7).[82] This substantial increase could be due to growth in the number of counterfeits in the supply chain, better record-keeping, improved testing methods, and/or heightened organizational and governmental awareness, to name a few possibilities. OCMs encountered more counterfeit incidents then any other sector in the supply chain (see Figure VII-8).

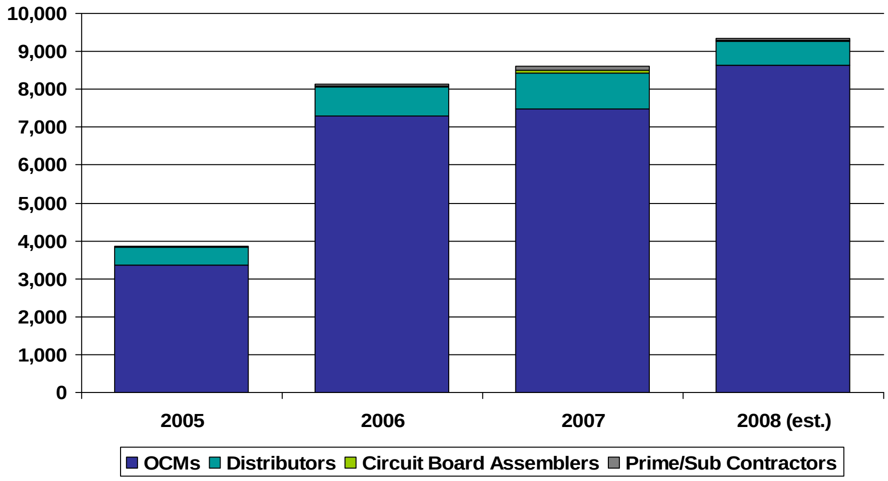
[82] For the purposes of this study, an incident is a single encounter of a suspected/confirmed counterfeit part. An incident could involve one part or a thousand parts of a component.

Figure VII-7: Total Counterfeit Incidents: OCMs, Distributors, Board Assemblers, Prime/Sub Contractors 2005 - 2008



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

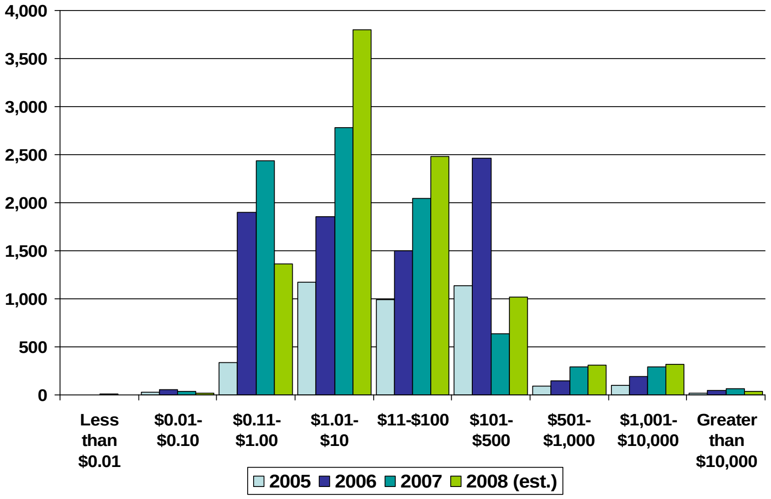
Figure VII-8: Total Counterfeit Incidents: OCMs, Distributors, Board Assemblers, Prime/Sub Contractors 2005 - 2008



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

A further examination of counterfeit incidents from 2005 to 2008 by product resale value shows the supply chain primarily encountered counterfeit parts in the $1.01 to $100 range (see Figure VII-9). There was a relatively steady increase in the number of counterfeit incidents in this resale value range. A significant number of counterfeit incidents also occurred in the $0.11 to $1.00 range and $101 to $500 range.

Figure VII-9: Counterfeit Incidents by Product Resale Value: (2005 - 2008)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

TYPES OF PARTS COUNTERFEITED

As stated in previous chapters, the electronic components counterfeited have a wide variety of defense and commercial purposes. Survey respondents were asked to identify the number of counterfeit product models encountered by product category to determine the categories most affected.

Based on the survey data, counterfeit incidents in all 11 product categories have increased from 2005 to 2008 (see Figure VII-10). The industrial/commercial and consumer product categories have experienced the highest numbers of counterfeit incidents. There have also been substantial increases in the High Reliability – Industrial, Qualified Manufacturers List (QML), Critical Safety, Qualified Products List (QPL), and High Reliability – Medical product categories.[83]

Figure VII-10: Types of Counterfeit Incidents (2005-2008)

Type of Product	2005	2006	2007	2008 (est.)
Industrial/Commercial	1739	4860	3841	2839
Consumer	154	345	398	531
High Reliability – Industrial	49	81	164	488
Qualified Manufacturers List (QML)	49	77	161	261
Critical Safety	42	63	93	277
Qualified Products List (QPL)	16	39	111	144
High Reliability – Medical	1	24	58	105
ITAR Controlled	15	10	67	19
Commercial Aviation	9	15	17	27
High Reliability – Automotive	2	6	8	25
Generalized Emulation Microcircuits (GEM)	0	0	0	2

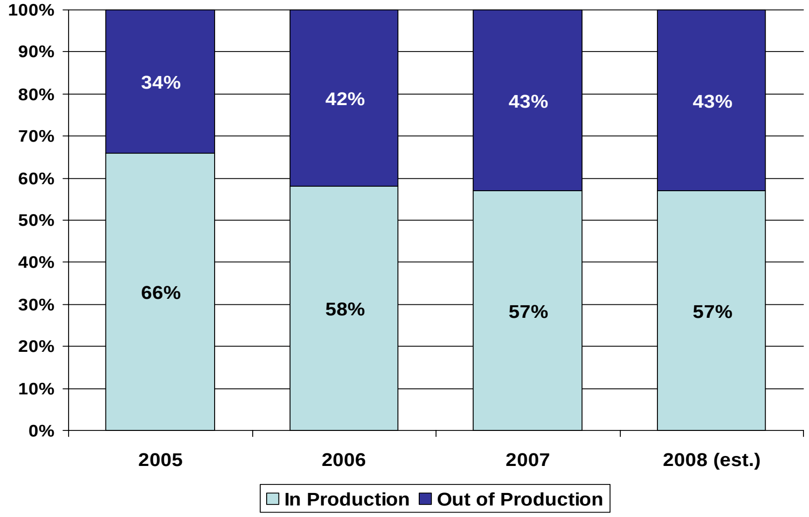
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Although replacement components for aging commercial, industrial, and defense products are often perceived as the prime market for counterfeiters, data shows otherwise. While survey respondents reported an increase in the amount of "out of production" counterfeit parts over the 2005-2008 period, from 34 to 43 percent, they encountered a larger amount of counterfeit "in production" parts, although this varied by sector (see Figure VII-11).[84]

[83] According to the Federal Acquisition Regulations (FAR), the QML is "a list of manufacturers who have had their products examined and tested and who have satisfied all applicable qualification requirements for that product." 48 C.F.R. § 9.201 The QPL is "a list of products that have been examined, tested, and have satisfied all applicable qualification requirements." 48 C.F.R. § 2.101

[84] For this assessment, parts produced by an after-market manufacturer are considered "out of production."

Figure VII-11: Percent of Counterfeit Incidents Involving In/Out of Production Products 2005 - 2008



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

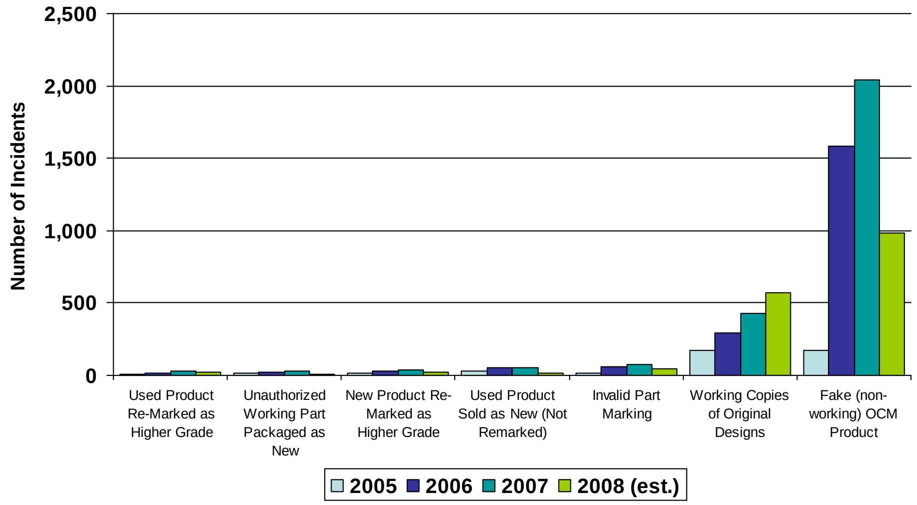
TYPES OF COUNTERFEITS AND METHODS OF DISCOVERY

There are many different types of counterfeit electronic parts, which can make detection especially difficult. Respondents in all five sectors were asked to identify the number of counterfeit incidents they encountered during the 2005-2008 period by type of counterfeit. Overall, organizations encountered all nine types of counterfeits listed on the survey.[85]

For those organizations that encountered counterfeit discrete electronic components, the majority reported "fake (non-working) OCM product" counterfeits (see Figure VII-12). A notable number of organizations have also encountered "working copies of original designs."

[85] One of the types of counterfeits listed on the survey, "unauthorized overrun of OCM product," was reported by only a few respondents and was too infrequent to be captured by the figures in this section.

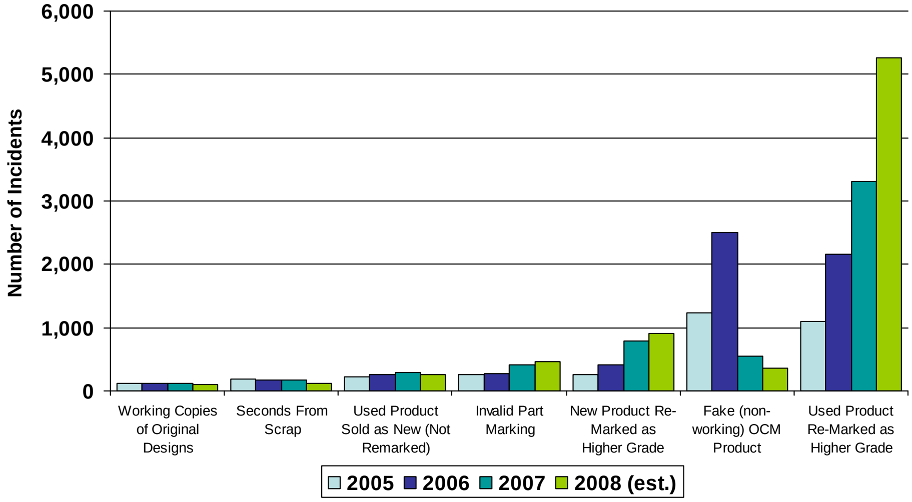
Figure VII-12: Counterfeit Incidents by Type of Problem – Discretes (2005-2008)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

A large number of respondents in all five sectors reported encountering “used product re-marked as higher grade” counterfeit microcircuits, but there were a significant number of counterfeit incidents that were “fake (non-working) OCM product” (see Figure VII-13). There were also a significant number of counterfeits that were “new product re-marked as higher grade.” This disparity between the types of counterfeit discrete components and microcircuits indicates there are different levels of opportunity for counterfeits to enter the supply chain based on price and the technical complexity of the parts.

Figure VII-13: Counterfeit Incidents by Type of Problem – Microcircuits (2005-2008)

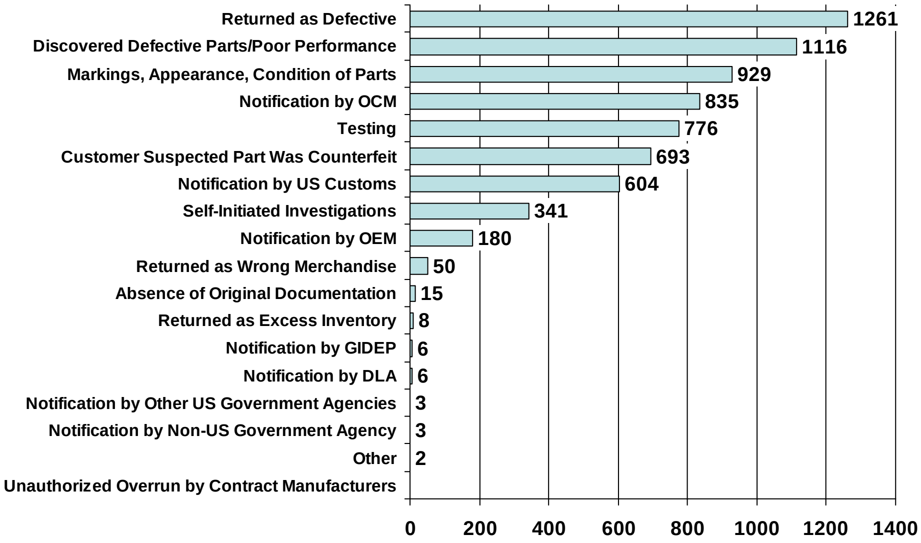


Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

All five sectors also identified the method by which they discovered counterfeit components. The most common methods of uncovering counterfeits were parts returned by customers as defective and the discovery of parts with poor performance, which accounted for 2,377 of all counterfeit incidents (see Figure VII-14). Organizations also discovered significant numbers of counterfeit parts by their markings, appearance, condition, and through notification by OCMs.

Survey respondents uncovered almost no counterfeit incidents through notification by various U.S. Government agencies. The exception was notifications by U.S. Customs and Border Protection (CBP), which accounted for 604 incidents. Organizations reported there were little to no incidents uncovered as a result of notifications issued by the Government-Industry Data Exchange Program (GIDEP), DLA, or other government agencies.

Figure VII-14: How Companies Are Uncovering Counterfeits (2008 est.)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

SOURCES OF COUNTERFEITS

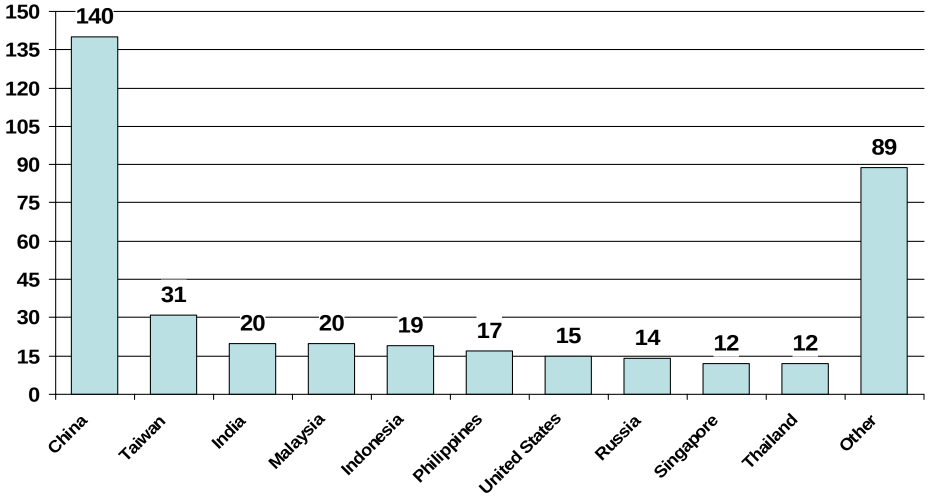
OTE asked survey participants to identify the top five countries suspected or confirmed to be sources of counterfeit electronic components. China was the country most frequently cited as a source of counterfeit components, with 140 citations (See Figure VII-15). Semiconductor Industry Association (SIA) members have documented Chinese entities removing discrete electronic components and microcircuits from electronic scrap and selling the recycled parts.[86]

The next nation most frequently identified as a source of counterfeit electronic components was Taiwan, with 31 citations, followed by India and Malaysia with 20 mentions each. Asia was overwhelmingly the largest regional source of counterfeits, though it is important to note that not

[86] Semiconductor Industry Association, "Combating Counterfeit Semiconductors and Developing a Secure Supply Chain," Diminishing Manufacturing Supplies and Material Shortages (DMSMS) Conference, Palm Springs, CA, 23 Sep 2008.

all counterfeit parts originate from that region. The United States and Russia were also cited as sources of counterfeit parts.[87]

Figure VII-15: Top Countries Suspected/Confirmed to be Sources of Counterfeits*



*** Each company was asked to provide their top five suspected countries**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

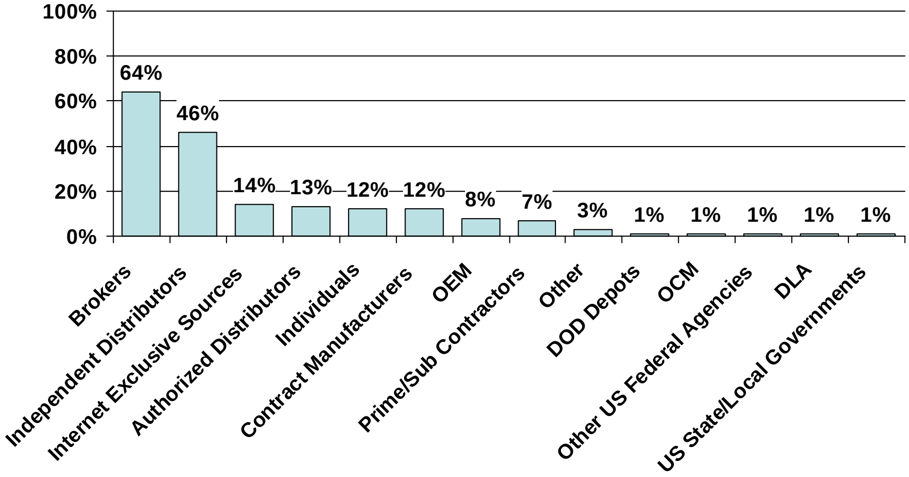
Another sourcing concern is how the counterfeit parts are infiltrating the U.S. supply chain. Survey respondents were asked to identify companies they had documented as selling counterfeits, whether inadvertently or purposely. The majority of organizations that encountered counterfeit components (64 percent) reported parts brokers as a source of counterfeits. Forty-six percent of organizations identified independent distributors as a source of counterfeits (see Figure VII-16).

Brokers and independent distributors were not the only suppliers cited as selling counterfeit components, however. Survey respondents encountered counterfeit parts being sold by twelve

[87] The “Other” column of Figure VII-14 is comprised of the following countries: Japan, Vietnam, Hong Kong, Brazil, Mexico, Israel, North Korea, South Korea, United Arab Emirates, Canada, Paraguay, Pakistan, Argentina, Cambodia, Costa Rica, Iran, Georgia, Hungary, Chile, Germany, Romania, Uruguay, Czech Republic, South Africa, Ukraine, and Haiti.

other types of suppliers, including OCMs, authorized distributors, and DOD. This data indicates that all purchasers and suppliers need to address the issue of counterfeits.

Figure VII-16: Percent of Organizations with Cases of Counterfeit Incidents Sold by Type of Entity*



*** Only includes companies that encountered counterfeits**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

INTERNAL DATABASE TO TRACK COUNTERFEITS

Data suggests that the incident rates reported by survey participants do not fully reflect the size and scope of the counterfeit parts problem. Survey responses reveal that monitoring practices often are not robust, and therefore the level of counterfeit electronic components in supply chains is likely understated. Without a method of tracking the type of counterfeit incidents encountered, a company or organization cannot identify trends or points of vulnerability within their supply chain. When internal records are not kept, problems can reoccur and repeat offenders may not be readily identified.

No DLA organizations reported maintaining a database to track counterfeit incidents (see Figure VII-17). Non-DLA organizations and circuit board assemblers were only slightly better, with 18 percent maintaining such databases. More distributors maintain a database to track counterfeits than any other sector in the supply chain, with 59 percent of distributors doing so.

Figure VII-17: Percent of Companies/Organizations Who Encountered Counterfeits and Maintained a Tracking Database	
OCMs	52%
Authorized Distributors	30%
Unauthorized Distributors	66%
Circuit Board Assemblers	18%
Prime/Sub Contractors	32%
Department of Defense	21%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

INVENTORY CONTROL AND TESTING

Survey respondents were asked a series of questions about their return and re-circulation policies, pre-stock testing procedures, and inventory audits for counterfeit parts. If properly conducted, each of these activities can reduce the proliferation of counterfeit components in the supply chain.

RETURNS, EXCESS INVENTORY, AND RE-CIRCULATION OF PARTS

One way counterfeit parts enter the supply chain is when organizations accept returns or buy excess inventory from their customers. According to the survey data, OCMs and distributors are more likely to accept returns and buy back excess inventory from customers than circuit board assemblers and contractors (see Figure VII-18). OCMs and distributors are also more likely to restock or re-circulate the product they accept back from their customers than the rest of the supply chain. These practices make them more susceptible to counterfeits via their customers.

Figure VII-18: Inventory Control and Return Policies

	OCMs	Distributors	Circuit Board Assemblers	Prime/Sub Contractors
Accept Returns From Customers	96%	100%	84%	81%
Buy Back Excess Inventory From Customers	25%	46%	16%	7%
Restock/Re-circulate Returns or Excess Inventory From Customers	61%	54%	13%	21%
Have Cases of Individual Customers Returning Counterfeits	17%	31%	3%	2%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

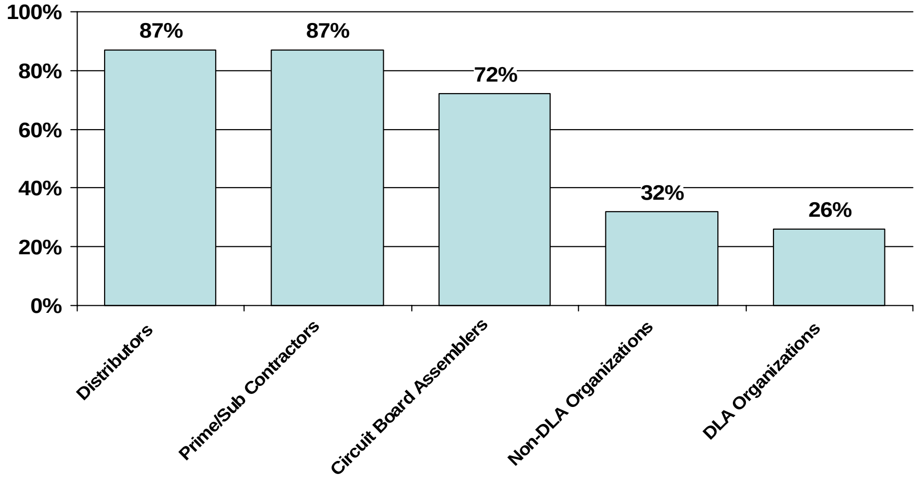
PRE-STOCK TESTING

Testing purchased parts before placing them in inventory, or pre-stock testing, is an effective way to locate counterfeits and remove them from the supply chain. This testing can include visual inspection of parts and packaging, electrical testing to ensure functionality, and/or physical or destructive evaluation to ensure authenticity. The level and thoroughness of pre-stock testing can vary depending on the supplier, the type of part, and type of transaction, as can the amount of parts tested.

There is a disparity in the level of testing throughout the different sectors of the supply chain.[88] Distributors, prime contractors, and subcontractors have the largest percentages of companies (87 percent) that conduct at least one type of pre-stock testing (see Figure VII-19). In contrast, 26 percent of DLA organizations and 32 percent of non-DLA organizations conduct some form of pre-stock testing.

[88] For the purposes of this assessment it was assumed that OCMs do not purchase electronic components, and therefore do not conduct any pre-stock testing.

Figure VII-19:Percent of Companies/Organizations Conducting Any Type of Pre-Stock Testing on Parts

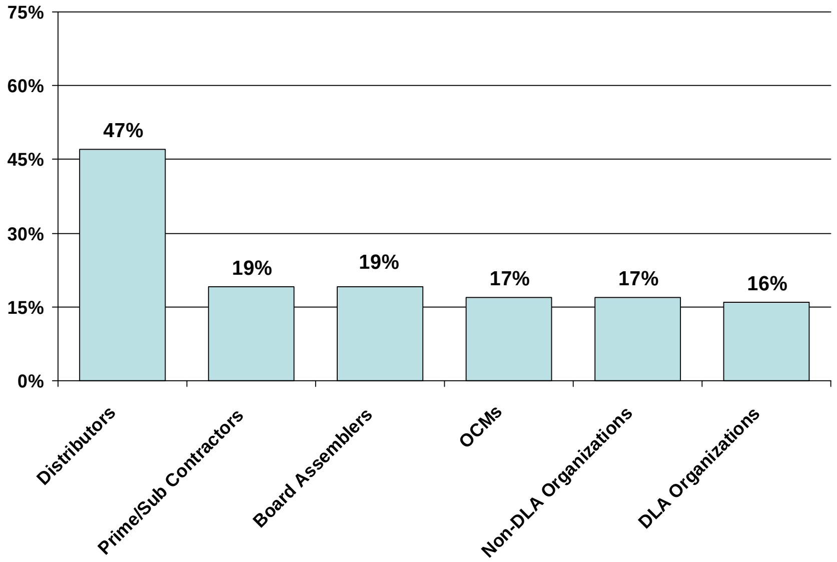


Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

AUDITING PRACTICES

Once electronic parts are placed into an organization’s inventory, firms may uncover counterfeit components by conducting inventory audits. Less than 20 percent of OCMs, circuit board assemblers, prime contractors and subcontractors, and DOD organizations audit their inventory to detect counterfeit parts (see Figure VII-20). A higher percentage of distributors conduct inventory audits to uncover counterfeit components, although that number is still less than half of surveyed companies.

Figure VII-20: Percent of Companies Performing Inventory Audits for Counterfeits



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

One reason for low levels of inventory auditing is that organizations trust the integrity of the supply chain and the products that flow through it, particularly parts from OCMs and authorized distributors. Other respondents stated that there audits are not necessary because components are tested before placed them in inventory. Others conduct more general inventory audits that are not specifically aimed at discovering counterfeit parts.

ACTIONS TAKEN REGARDING COUNTERFEITS

Upon discovering counterfeit parts, organizations can take many internal and external actions to address the situation. Survey respondents were asked several questions about these actions: steps taken once they are notified of and possess counterfeits; authorities contacted; knowledge of legal responsibilities and liabilities; how counterfeits are entering the supply chain; and what is being done to mitigate the risk.

Steps Taken After Notification and Possession of a Counterfeit Part

One of the opportunities an organization has to take action against counterfeits is when it is notified of the existence of a counterfeit part by suppliers, customers, or other entities. Most of the actions survey respondents involve internal steps, such as notifying internal company authorities, pulling back inventory, tracing the supply chain, and locating select inventory (see Figure VII-21).[89]

Communication within and between industry segments is inconsistent. Based on survey data, distributors are the most likely to notify industry associations when they encounter counterfeits. In addition, despite the fact that OCMs have contractual relationships with their authorized distributors, only 35 percent would inform suppliers if they encountered a counterfeit. Exceedingly few companies across all sectors notify federal authorities, making law enforcement action less likely.

Figure VII-21: Steps Taken/Would Be Taken After Notification of a Counterfeit Part

Action Taken	OCMs	Distributors	Circuit Board Assemblers	Prime/Sub Contractors
Notify Internal Company Authorities	69%	62%	66%	68%
Pull Back Inventory	25%	67%	69%	71%
Trace Supply Chain	66%	53%	57%	64%
Locate Select Inventory	37%	58%	66%	67%
Inform Authorized Distributors	35%	32%	50%	50%
Inform OCM	-	37%	47%	56%
Perform Random Testing	22%	38%	41%	45%
Notify Federal Authorities	18%	15%	9%	35%
No Steps are Taken	18%	17%	19%	26%
Wait for Additional Complaints	18%	5%	3%	5%
Other	16%	12%	9%	21%
Notify Industry Associations	13%	51%	13%	22%

Source: U.S. Department of Commerce, Office of Technology Evaluation
Counterfeit Electronics Survey, November 2009.

[89] Some respondents answered this survey question from the perspective of what they would do if they were notified of counterfeit parts, not what they have done.

Organizations can also take action against counterfeits when they physically possess a counterfeit part. Responses varied widely between company types (see Figure VII-22).[90] For the most part, distributors take more external actions than other organizations with regard to information sharing and participation in counterfeits databases. All four industry sectors reported low percentages of turning over counterfeit parts to law enforcement.

Figure VII-22: Steps Taken/Would Be Taken After Possession of a Counterfeit Part

Action Taken	OCMs	Distributors	Circuit Board Assemblers	Prime/Sub Contractors
Enter into USG or Industry Database	7%	41%	9%	24%
Retain Samples for Reference	57%	41%	22%	43%
Test Part	57%	52%	44%	54%
Enter into Company Database	49%	62%	50%	50%
Quarantine Parts	22%	42%	22%	40%
Leave Disposal to Party Filing Complaint	23%	11%	6%	7%
Random Inventory Testing	18%	38%	44%	46%
Dispose of Parts Immediately	19%	32%	16%	20%
Issue Credit	17%	66%	63%	36%
Turn Over to Law Enforcement Authorities for Analysis	10%	15%	13%	18%
Check USG or Industry Database	8%	48%	16%	36%
Other	10%	19%	9%	16%
Turn Over to Law Enforcement Authorities After Analysis	14%	11%	13%	18%
Return to OCM or Distributor	-	-	56%	30%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

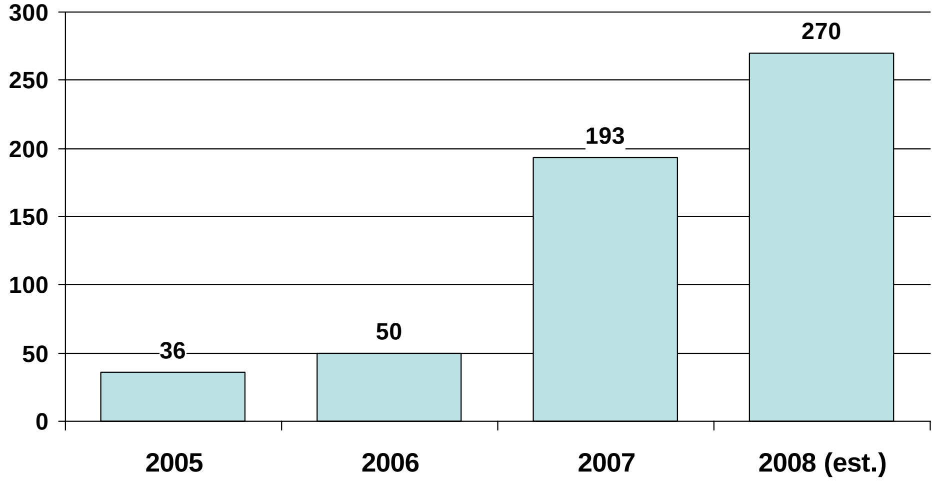
AUTHORITIES CONTACTED AFTER COUNTERFEIT INCIDENTS

Survey respondents stated how many counterfeit incidents they reported to government authorities over the 2005-2008 period (see Figure VII-23). Although the numbers have been increasing, those reported to authorities is only a small fraction of the total counterfeit incidents encountered each year.[91] Although industry reporting to government authorities was at its highest level in 2008, these incidents comprised only three percent of the total counterfeits reported for that year.

[90] Some respondents answered this survey question from the perspective of what they would do if they had possession of counterfeit parts, and not what they have done.

[91] See Figure VII-7 for total counterfeit incidents encountered each year.

Figure VII-23: Number of Incidents Reported to Government Authorities



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Organizations reported incidents to a range of government organizations (see Figure VII-24). The largest percentage of survey respondents (14 percent) reported incidents of counterfeit electronic components to the Government-Industry Data Exchange Program (GIDEP).[92] The percentages of organizations reporting to other government authorities, such as U.S. Customs and Border Protection (CBP) and the Federal Bureau of Investigation (FBI), are even smaller.

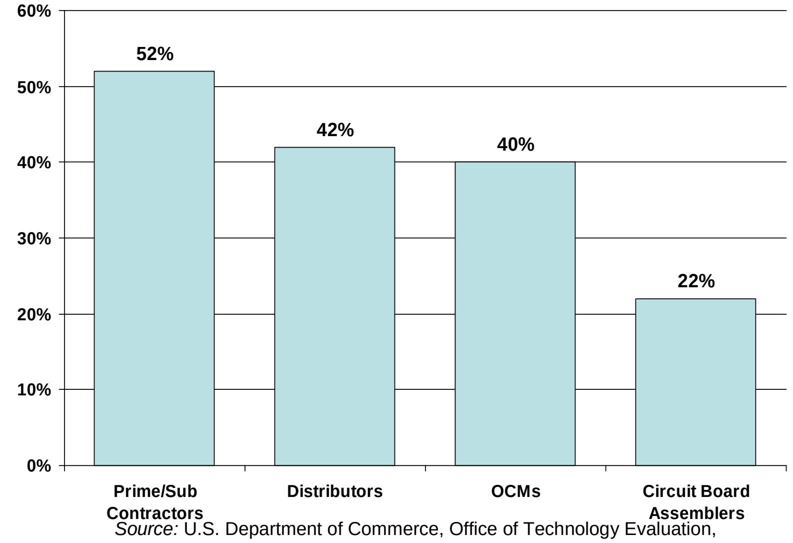
[92] Operated under Department of Defense sponsorship, GIDEP was created to enable industry and government agencies to locate parts for legacy electronic systems and to provide warnings on supply chain problems.

Figure VII-24: Top Authorities Notified After Counterfeit Incidents	
None at All	51%
Government-Industry Data Exchange Program (GIDEP)	14%
Defense Logistics Agency (DLA)	11%
State/Local Authorities	8%
Customs & Border Protection	7%
Federal Bureau of Investigation (FBI)	6%
Defense-Related Investigative Services (e.g., DCIS, NCIS, etc.)	5%
Federal Aviation Administration (FAA)	5%
*** Only includes those companies with counterfeit incidents**	

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

One explanation for low notification levels is that organizations do not know which authorities to notify. At best, half of the survey respondents stated that they know what authorities to contact regarding counterfeit products (see Figure VII-25). Interestingly, 37 companies that encountered counterfeits indicated that they knew what authorities to contact, but did not notify any. These companies were from all four industry segments surveyed. These figures indicate a lack of effective communication between industry and the U.S. Government.

Figure VII-25: Percent of Companies That Know What Authorities to Contact When They Encounter Counterfeit Products



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Legal Guidance and Liabilities

All survey respondents were asked several questions about their awareness of legal requirements, liabilities, and guidance regarding the handling of counterfeit components. The supply chain as a whole is generally unaware of the legal requirements and liabilities related to counterfeits (see Figure VII-26). Only a third of industry and government organizations are aware of legal requirements for the management and disposal of counterfeit products, while just under half are aware of liabilities related to the distribution, storage, and disposal of counterfeits. Only a third of organizations are aware of written instructions and guidance from federal authorities related to counterfeits, yet only 27 percent of respondents said they need such guidance from federal authorities.

Figure VII-26: Legal Liabilities

Percent of Companies Aware of Legal Requirements for Management/Disposal of Counterfeit Products	31%
Percent of Companies Aware of Written Instructions/Guidance From Federal Authorities Related to Counterfeits	31%
Percent of Companies Aware of Liabilities Related to Distribution, Storage, and Disposal of Counterfeits	47%
Percent of Companies That Need Guidance From the Federal Government Concerning Civil/Criminal Liabilities and Penalties Related to Counterfeits	27%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Difficulty Identifying Counterfeit Parts

The five sectors were asked if they find it difficult to identify counterfeit parts and if they are better able to identify counterfeits today than they were five years ago. Slightly more than half of the organizations do not find it difficult to identify counterfeit parts (see Figure VII-27). The reasons for this lack of difficulty vary across sectors, but there are many common explanations, such as:

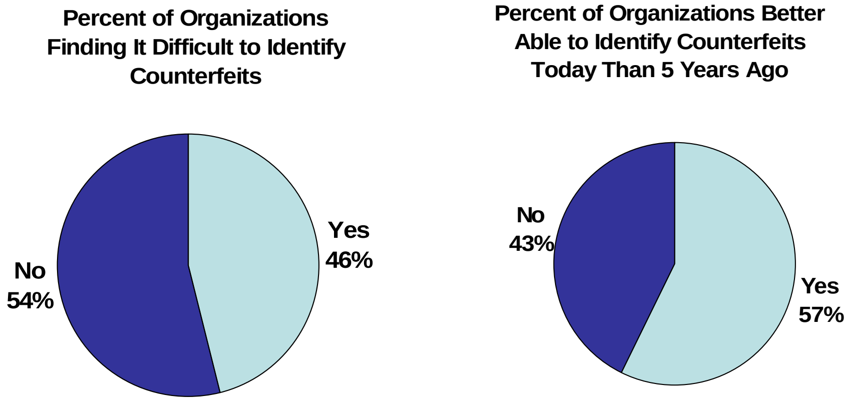
- the use of only approved vendors/trusted suppliers;
- a belief that the risk of counterfeits in certain industry segments is low;
- the use of advanced testing equipment to detect counterfeits;
- adherence to industry standards for quality control; and
- a lack of encounters with counterfeits.

For the 46 percent of organizations that find it difficult to identify counterfeits, respondents primarily pointed to the fact that counterfeiters are continually using more advanced techniques to evade detection. Other explanations were provided, including:

- the high cost of advanced testing equipment;
- a lack of cooperation between industry segments;
- the difficulty in testing large volumes of parts;
- the reliance upon exclusively visual inspection; and
- a lack of training and resources for counterfeit detection.

Moreover, 57 percent said they are better able to identify counterfeit components today than they were five years ago. A large portion of these organizations are in a better position today because of increased awareness and higher levels of testing. The majority of the respondents that said they are not better able to identify counterfeits today than five years ago explained that their processes have not changed over that time or have not encountered any counterfeits.

Figure VII-27: Difficulty Identifying Counterfeits



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Reasons for Counterfeits Entering the Supply Chain

The steady increase in the presence of counterfeit products in supply chains can be attributed to many causes. Survey respondents from the five sectors identified the main reasons they believe are causing counterfeit parts to enter the supply chain.

Three factors were most commonly cited by survey participants as the primary contributors to supply chain contamination: less stringent inventory management by parts brokers; greater reliance on gray market parts by brokers; and greater reliance on gray markets parts by independent distributors (see Figure 28).[93] These three top answers were consistent throughout the individual sector responses to this question. Organizations also pointed to other portions of the supply chain as being deficient in terms of chains of accountability and buying procedures. Original equipment manufacturers (OEMs), contract manufacturers, and OCMs were also identified as having practices that contribute to counterfeit part proliferation.

Figure VII-28: Top Ten Reasons For Counterfeits Entering the Supply Chain

Less Stringent Inventory Management by Parts Brokers	179
Greater Reliance on Gray Market Parts by Brokers	168
Greater Reliance on Gray Market Parts by Independent Distributors	152
Insufficient Chain of Accountability	141
Less Stringent Inventory Management by Independent Distributors	139
Insufficient Buying Procedures	124
Inadequate Purchase Planning by OEMs	117
Purchase of Excess Inventory on Open Market	113
Greater Reliance on Gray Market by Contract Manufacturers	107
Inadequate Production by OCM	105

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, May 2009.

[93] A gray market is the trade of parts through distribution channels which, while legal, are unofficial, unauthorized, or unintended by OCMs.

Internal and External Actions Taken to Prevent the Infiltration of Counterfeits

In light of the growing proliferation of counterfeit parts in the overall supply chain, there are internal and external actions that organizations are taking to protect their inventories and supply chains. Based on survey responses, there is not a great deal of uniformity among the actions organizations take internally across the supply chain (see Figure VII-29). Higher percentages of distributors are revising procurement procedures and training staff than the other sections. Meanwhile, DOD has the highest percentage of entities taking no internal action whatsoever.

Figure VII-29: Internal Actions Taken to Prevent Infiltration of Counterfeits

Action	OCMs	Distributors	Circuit Board Assemblers	Prime/Sub Contractors	DOD
Performing screening and testing on inventory	27%	8%	41%	37%	21%
Training staff on the negative economic and safety impacts of counterfeit products	31%	65%	28%	36%	15%
No internal actions taken	35%	19%	34%	32%	72%
Revising procurement procedures to more carefully screen/audit/evaluate authorized returns from customers	35%	76%	25%	23%	11%
Revising company procedures for disposal of "seconds," defective parts, and production overruns	34%	44%	22%	17%	11%
Other	8%	12%	9%	17%	0%
Revising procurement procedures to reduce purchases from independent distributors and brokers	-	-	13%	4%	11%
Embedding new security measures in existing product lines	12%	4%	3%	2%	2%
Adding security markings to existing inventory	12%	0%	0%	2%	8%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

With respect to external actions, no uniform set of actions is being taken by four of the five surveyed sectors (see Figure VII-30).[94] A significant portion of organizations in the supply chain are taking no external steps to prevent the infiltration of counterfeits. Those that do take external actions seem to focus on different types of activities based on their sectors. For example, more OCMs have tightened contract requirements with contract manufacturers than organizations in other sectors. In addition, more distributors have focused on educating their customers on the impacts of counterfeit products.

[94] DOD respondents were not asked about external actions taken to prevent the infiltration of counterfeits.

Figure VII-30: External Actions Taken to Prevent Infiltration of Counterfeits

Action	OCMs	Distributors	Circuit Board Assemblers	Prime/Sub Contractors
No external actions taken	35%	29%	59%	69%
Tightening contractual obligations of contract manufacturers with regard to disposal of “seconds,” defective parts, and overruns	29%	11%	3%	12%
Educating customers/suppliers on the negative economic and safety impacts of counterfeit products	31%	52%	16%	9%
Educating customers about risks associated with grey market products	40%	57%	28%	8%
Other	8%	5%	3%	9%
Referring customers to companies that could identify suitable substitute products or re-engineer system components	19%	30%	25%	6%
Referring customers to authorized after-market manufacturers	27%	21%	9%	5%
Prohibiting authorized distributors from buying back excess inventory on the grey market	31%	10%	6%	5%
Prohibiting authorized distributors from buying back excess inventory from their customers	6%	5%	0%	3%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

VIII. BEST PRACTICES

As made evident in the previous chapters, counterfeit components impact each sector of the U.S. electronics supply chain – original component manufacturers (OCMs), authorized and unauthorized distributors, circuit board assemblers, prime contractors and subcontractors, and Department of Defense (DOD) entities.[95] Counterfeit discrete electronic components, microcircuits, bare circuit boards, and assembled circuit boards infiltrate parts inventories and have been integrated into critical defense and civilian systems.

Companies need to take actions to prevent the infiltration of counterfeit parts through management strategies, employee practices, and cross-sector communication. The government also needs to take similar action and learn from industry best practices. Successful implementation of best practices by all parties would create a layered approach that would help safeguard U.S. Government, critical infrastructure, and industrial assets.

To that end, OTE asked each survey participant to list five "best practices" that companies and organizations should adopt to reduce the infiltration of counterfeit electronics into supply chains. OTE also conducted separate interviews with companies, participated in numerous counterfeit mitigation conferences and workshops, and consulted open source material on the subject. A best practice is considered to be an efficient and effective standard process that can be adopted by multiple organizations. This resulted in more than 1,300 suggested best practices, which have been categorized and analyzed for this chapter.[96]

This chapter is divided into the following sections on best practices for:

- the overall supply chain;
- original component manufacturers (OCMs);
- procurement of parts;
- receiving and storing parts;
- managing counterfeits; and
- overall U.S. Government procurement.

[95] The term "unauthorized distributors" is not intended to imply that these companies are engaged in illicit activities, but rather that they are not party to a legal agreement to distribute OCM/OEM products.
[96] Respondents were not asked to identify the time or resources necessary to carry out their suggested best practices.

There is also a section of recommended actions for the U.S. Government.

OVERALL SUPPLY CHAIN BEST PRACTICES

Several best practices provided by survey respondents relate to all sectors of the U.S. supply chain. These best practices include implementing institutional policies and procedures, counterfeit part training programs, and internal and external communication processes.

INSTITUTIONALIZED POLICIES AND PROCEDURES

Respondents from all five surveyed sectors stressed the importance for organizations to have institutionalized policies and procedures in place on how to avoid and handle counterfeit components, regardless of whether they have experienced counterfeits to date. Employees need clear direction from management on combating counterfeits as well as written guidance on how to: avoid purchasing counterfeit parts; test, handle, and track incoming and outgoing parts; and manage and dispose of suspected counterfeit components.

Established counterfeit avoidance policies and procedures help remove confusion for employees with different responsibilities in an organization. They also create standardization and mitigate the impact resulting from departing employees. Moreover, such procedures should be routinely updated and audited to make sure they adequately address existing and emerging concerns and problems.

The U.S. Government and several industry associations have published standards regarding counterfeit parts, testing, quality assurance, and general inventory and procurement practices. For example, in the beginning of 2009, SAE International published the standard *AS5553: Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition*, which provides “uniform requirements, practices and methods to mitigate the risks of receiving and installing counterfeit electronic parts."[97] These types of standards can be used as a basis for an organization's counterfeit avoidance policies and procedures. The Bureau of Industry and Security also has developed a quality management program for export controls that could be emulated to address counterfeits.[98]

All institutionalized policies and procedures must conform to existing U.S. law regarding counterfeits. Counterfeiting was criminalized under the Trademark Counterfeiting Act of 1984, codified at 18 U.S.C § 2320. This statute allows the prosecution of individuals and companies that have engaged in trafficking counterfeit trademarks, service marks, and certification marks. As a legal resource, the U.S. Department of Justice created Cybercrime.gov, which contains guidance on how to report cyber and intellectual property crimes, copies of legal statutes, and frequently asked questions on counterfeiting issues.

COUNTERFEIT PART TRAINING PROGRAMS

In addition to instituting policies and procedures, organizations need to implement corresponding counterfeit avoidance and management training programs. A majority of survey participants identified a need for training on how to inspect parts and identify possible counterfeits (e.g., non-conforming part markings). This training – preferably hands-on – should be given to all employees that handle electronic parts, including purchasing, quality assurance, and receiving personnel. Refresher training should be given regularly to update employees on new threats, identification techniques, and communication strategies. Several industry associations, such as the Independent Distributors of Electronics Association (IDEA), have information on identifying counterfeit parts that can be used as the basis for such training.[99] The training must also stress management's commitment to combating counterfeits throughout its entire procurement chain.

[97] Information on SAE AS5553 can be found at http://www.sae.org/technical/standards/AS5553

[98] See Appendix H for a version of BIS' export management and compliance program that has been modified to address counterfeit part avoidance.

[99] IDEA Standard 1010-A specifically deals with inspection procedures and has a section on unacceptable characteristics for electronic components. More information is available at http://www.idofea.org/products.

Internal and External Communication

A key element to any counterfeit prevention policy is communication. Employees involved in the movement of electronic components need to be made aware of counterfeits and their implications (e.g., brand-integrity, compromise of critical programs). This includes employees that order, receive, test, store, ship, and install parts, as well as their supervisors and management. Everyone must know and understand the problem in order to address it.

Organizations emphasized the need for communication within an organization, be it a government agency or a company, between operating units and between employees and management. Employees that handle electronic parts need to be able to express their concerns, knowledge, and opinions to those that set and implement an organization's policy.

Organizations need to communicate with external entities, as well. One level of communication involves sharing information with the overall industry and supply chain (i.e., suppliers, customers, and competitors), including details about counterfeit parts, methods of counterfeiting, and sources for entry into procurement chains. Organizations should be encouraged instead of penalized for reporting counterfeit components.

Suppliers need to discuss the risks associated with procuring obsolete and hard-to-find parts, parts that require long lead times, and parts from unauthorized. Survey respondents said OCMs in particular need to alert customers and industry in a timely manner when parts will no longer be manufactured. In return, customers need to make clear to suppliers what procurement practices are acceptable, including the legal requirements, inventory process controls, paperwork pedigree, and testing protocols necessary to affirm the authenticity of parts.

In addition to sharing data with suppliers and customers, communication through industry associations and government-sponsored agencies, such as the Government-Industry Data Exchange Program (GIDEP) and the Semiconductor Industry Association (SIA), further educates and alerts consumers about counterfeit trends. However, these information-sharing avenues need to be more accessible and used by organizations. Survey respondents often did not know about these types of associations or found them difficult to use.

BEST PRACTICES FOR ORIGINAL COMPONENT MANUFACTURERS (OCMS)

OCMs are in a unique position in the supply chain as manufacturers of the parts being counterfeited. Therefore, OCMs require tailored counterfeit avoidance practices to meet their distinctive needs and experiences, which include:

- using authentication or encryption codes, which would be provided to the purchaser;
- embedding security markings in parts;
- using unique, harder to copy labels and markings;
- identifying distinct lot and serial codes on external packaging; and
- embedding radio frequency identification (RFID) into high-value parts.

Many OCMs are actively developing different methods to secure electronic parts, to varying degrees of success. Some methods, however, such as RFID, are not cost-effective for less expensive parts. Counterfeiters are also becoming more sophisticated, challenging the abilities of OCMs to stay a step ahead with regard to tamperproof markings and security measures. Efforts to secure the authenticity of parts for distributors and consumers must keep evolving.

OCMs also can prevent counterfeits from entering the supply chain through the physical destruction of all defective, damaged, and sub-standard parts that are by-products of the manufacturing process. Survey data showed that these types of parts have routinely escaped destruction and have entered the supply chain remarked as authentic working parts. Respondents suggested that as a best practice, OCMs destroy the parts on-site, instead of sending them to an external contractor for disposal. In-house destruction of scrap parts and tight control of disposal processes reduce the opportunities for diversion and re-circulation of defective components into the supply chain. This practice should also apply to contract manufacturers hired by OCMs. If OCMs contract-out production or removal of scrap, then the contracts they use must address proper disposal requirements.

Another best practice for OCMs is to secure their facilities to prevent unauthorized access to proprietary information, which could bolster counterfeiting operations. Several surveyed OCMs recommended that manufacturers limit who has access to processes and equipment, and only allow authorized personnel onto the production floor and in stockrooms. Others suggested OCMs implement rigid shipping requirements and tightened security measures for items leaving OCM facilities. Contractual obligations should be imposed by OCMs to prohibit the use of production equipment and related materials except as authorized by the OCM. These actions can prevent products and designs from being manufactured or stolen for counterfeit purposes.

OCMs also need to address product return, buy back, and inventory control practices. According to survey data, lax return and buy back practices can result in counterfeit parts entering OCM inventories and then inadvertently resold as legitimate product. Since it is impractical for an OCM to refuse all returns, it is important that all returned parts and materials be segregated and put through an inspection process to verify authenticity. While such a process can be cumbersome and costly, it would ensure OCM inventories remain free of counterfeits.

As stated previously, communication is a key element to all counterfeit avoidance efforts, including those of OCMs. The information OCMs have about their authentic products can help prevent the trafficking of counterfeit. Several survey respondents said OCMs should cooperate more with companies that have questions about the authenticity of parts they purchased. As noted in Chapter II, OCMs sell their products to entities other than their authorized distributors, yet OCMs have been reluctant to work with unauthorized distributors or customers that have purchased OCM parts on the open market. Counterfeit avoidance efforts throughout the supply chain would be greatly improved if OCMs could develop a method to share authenticity information in a way that would not jeopardize proprietary data.

Survey respondents also said OCMs should work with U.S. Customs and Border Protection (CBP) to educate CBP officials on how to identify counterfeits.[100] Without this training, CBP

[100] The Semiconductor Industry Association has already undertaken efforts to educate U.S. Customs officials on how to identify counterfeit components. It has also worked with U.S. and European customs authorities to stop shipments of counterfeit electronic parts.

officials are constrained with regard to targeting and seizing illegitimate products. This cooperation should also extend to other U.S. law enforcement agencies, such as the Federal Bureau of Investigation (FBI) and the Defense Criminal Investigative Service (DCIS).

BEST PRACTICES FOR PROCUREMENT OF PARTS

Survey data indicates that the procurement process has become a main entry point for counterfeits due to the use of unapproved suppliers, lack of part authentication procedures, lack of communication and cooperation between suppliers and customers, insufficient inventory control procedures, and limited counterfeit avoidance procurement policies and practices. To this end, respondents recommended steps that organizations can take to reduce the vulnerabilities in procurement processes.

WHERE AND HOW TO SOURCE PARTS

The most widely suggested best practice to avoid purchasing counterfeits is to buy parts directly from OCMs and authorized distributors, rather than from parts brokers, independent distributors, or the gray market.[101] Survey data showed OCMs and their authorized distributors have been the least risky source of supply for electronic parts. Nevertheless, due diligence is still required with regard to traceability of parts purchased from OCMs and their authorized distributors.

However, a policy of not buying from the parts brokers, independent distributors, or the gray market is not practical for many organizations. This is especially true for those organizations that work on systems that require out-of-production or obsolete parts, or those that require extremely short lead times.

Moreover, such a policy broadly labels all unauthorized distributors as untrustworthy, when many provide authentic products for critical defense and civilian needs. OCMs and aftermarket

[101] A gray market is the trade of parts through distribution channels which, while legal, are unofficial, unauthorized, or unintended by OCMs.

manufacturers, for example, may no longer produce a needed part, might require an extensive lead time, or have too high a purchase price. There are also legitimate parts available in the gray market due to surplus sales, bankruptcies, and direct sales of authentic product outside of authorized channels. While there can be more risk involved when purchasing components from the gray market, there are steps organizations can take to mitigate most of that risk.

Traceability

Traceability is a key means for verifying legitimate parts in any supply channel. Organizations should require their suppliers to trace parts back to OCMs in order to prove part authenticity. Furthermore, suppliers should provide the names and locations of all intermediary companies that handled the parts. This information allows organizations to determine if a secure supply chain was maintained or if it is likely that the parts were compromised. Many respondents said this is particularly necessary for parts coming from overseas, especially China and other Asian countries.

The most common way to map a part's traceability is through a certificate of conformance. This formal document, given to the purchaser and signed by the supplier, affirms that all purchase order requirements have been met. These requirements can include not only specific information about the parts, such as quantity and lot and date codes, but also information about the OCM and all distributors participating in the sale. It is important to note that certificates of conformance can be counterfeited or forged, so they need to be carefully examined.

Some suppliers said organizations can also require suppliers to provide a testing certification. This type of certification is a formal document signed by the supplier and given to the purchaser that affirms the parts were tested and found to conform to requirements. The document can include information on the location of part's testing, the sample size tested, and what tests were conducted. A testing certification can provide additional assurance of a part's authenticity, especially when a certificate of conformance is not available. The purchaser can even have the parts tested at a third-party testing house to further ensure the validity of the testing certification.

Traceability documentation is only effective if reviewed and verified to be consistent with the received parts. Organizations should instruct employees to check certificates of conformance, testing certifications, and packing slips with the related shipments and look for anomalies, such as part numbers, lot codes, and date codes that do not match the incoming parts. This documentation should also be kept on file for as long as the parts are in use in case problems arise.

All of these elements should be part of a comprehensive procurement strategy. Organizations should provide for realistic procurement lead times during the planning process to avoid reliance on higher risk part suppliers or to allow for testing of parts that have to be purchased from riskier sources. Organizations should also have proactive obsolescence management plans when parts go out of production, including designing obsolete parts out of systems.

TRUSTED AND UNTRUSTED SUPPLIERS LISTS

Another recommended way organizations can avoid purchasing counterfeit components is to establish a list of trusted or approved suppliers. A supplier would have to meet established criteria to be put onto the list. Procurement officials would be limited to buying parts from approved companies, unless there are exceptional circumstances and corresponding risk mitigation strategies in place (e.g., electronic testing, regular inventory audits for counterfeits). There are many criteria an organization can use to identify trusted suppliers, including:

- the number of years the supplier has been in business;
- references from past and current customers;
- counterfeit screening, tracking, and testing procedures;
- adherence to industry and government standards;
- membership in industry associations such as SIA, IDEA, or ERAI;
- previous problems recorded in industry association databases, GIDEP, FAA's Suspected Unapproved Parts listing, or the Better Business Bureau;
- quality of warehouse/storage facilities; and
- existing counterfeit avoidance policies.[102]

[102] JEDEC Standard JESD31, *General Requirements for Distributors of Commercial and Military Semiconductor Devices*, has basic criteria for distributors and can be found at http://www.jedec.org.

An organization's trusted supplier list should be assessed and adjusted accordingly at least once a year to determine if any new information of concern has come to light. It is important that a list of trusted suppliers be a living document, and changed as the circumstances changes.

To that end, organizations should conduct audits of suppliers as part of their contractual obligations to determine if their counterfeit avoidance policies and screening and testing procedures are adequate. Absent stringent authentication procedures, these audits should take place before an organization initially purchases any product from a supplier, and then at regular intervals after the initial purchase.

Organizations should also have a list of unapproved suppliers, which identifies companies that have a documented history of selling counterfeit components. Suppliers can also be placed on the unapproved supplier list if they do not meet all of the trusted supplier criteria. Procurement officials should be restricted from using the suppliers on the unapproved list except in extenuating circumstances (e.g., sole supplier) and require extensive proof of authenticity (e.g., physical testing) prior to purchase and installation. Both the approved and unapproved lists should be amended as suppliers improve their counterfeit avoidance policies and as untrustworthy companies are discovered.

Supply Chain Requirements

Organizations should confirm suppliers use desired counterfeit avoidance policies and practices. This can be done through contract requirements and language in purchase orders. Organizations can legally require certificates of conformance, testing certification, and procedures for handling any counterfeit parts that slip through. All requirements must be communicated to an organization's suppliers instead of assuming that suppliers take unilateral actions to prevent counterfeits.

Organizations should also implement requirements for their subcontractors and contract manufacturers to reduce the possibilities of encountering counterfeit components. These requirements should include thorough counterfeit part screening and testing procedures, strict facility security, and meticulous disposal practices. Subcontractors and contract manufacturers should also adhere to trusted suppliers and unapproved suppliers lists when possible.

Organizations, including their subcontractors and contract manufacturers, should remain vigilant about "red flags" that arise during the procurement process. These include: suppliers offering very low prices, especially when other sellers have prices listed as much higher; providing much shorter lead time than other sellers; and listing products that are hard to find but which suddenly appear readily available upon request.

One practice growing in popularity is using an escrow service, such as the one offered by the organization ERAI. The buyer places the money into a third-party escrow account and the money is held until the buyer receives and tests the product. If the product is legitimate, the money is released to the supplier. If the product is not legitimate, the money is returned to the buyer. This practice may be a deterrent to companies with counterfeit parts and would be a useful practice when dealing with more risky suppliers.

Ultimately, organizations must weigh the level of risk and the legitimacy of an offer when purchasing electronic parts. It is therefore important that final procurement decisions not reside solely with an automated system. While an automated system can be programmed to look for specific characteristics, it cannot determine if a sale is "too good to be true" or if a company is a legitimate supplier. Only trained personnel can make those determinations, and it is such judgments that can save organizations money, safeguard strategic assets, and protect company reputations.

BEST PRACTICES FOR RECEIVING AND STORING PARTS

Even with safeguards in place during the procurement process, counterfeit parts can still infiltrate inventories upon receipt and storage of components. OCMs and distributors with screening processes, for example, can miss counterfeit parts and inadvertently ship them to customers. Other times, parts need to be bought outside of trusted suppliers. Organizations should implement procedures to mitigate the risk posed by counterfeits when they take possession of purchased parts.

VISUAL INSPECTION

Survey respondents suggested that employees should verify not only that the parts meet the purchase order requirements, but that information on the parts matches the information in the accompanying documentation. This would include checking that part numbers, lot codes, dates of manufacturing, and logos on the parts and documentation are the same. This simple, non-invasive step could reveal counterfeit components early in the inventory process.

After verifying the documentation, employees should conduct visual inspections of parts for evidence of counterfeiting. Many survey respondents said all incoming parts should go through visual inspection. While time consuming, visual inspection is the easiest and cheapest counterfeit-detection method. There are many factors employees should evaluate during visual inspection, including:

- differences in surface texture and coating;
- bent leads;
- poor quality part markings;
- broken or damaged packaging; and
- markings that are inconsistent with OCM markings and data.[103]

Employees need to have the equipment necessary for visual inspection, such as microscopes and cameras. If possible, employees should have access to photographs of what the parts should look like in order to compare incoming parts with authentic parts. Ideally, employees serving as parts inspectors should be trained and certified by organizations like IDEA, which has a Professional Inspector's Certification Exam.[104] Such certification ensures that employees are properly trained on how to identify counterfeit components.

[103] SAE's standard AS5553 and IDEA-STD-1010-A both have detailed lists of criteria to look for during a visual inspection.

[104] Information on IDEA's Professional Inspector's Certification Exam can be found at http://www.idofea.org/products

COMPONENT TESTING

The next step after visual inspection is component testing. The level of necessary testing and the number of parts tested depends on the criticality of the part, the kind of supplier, and the results of the visual inspection. Parts that are considered mission critical or sensitive, are going into military items, or were purchased from non-trusted suppliers should undergo rigorous testing to identify counterfeits. In addition, some respondents suggested that any components pulled from lots or orders to be tested should be pulled randomly, as some counterfeiters place legitimate parts at the beginning and end of lots to pass testing.

When a part is deemed to have differences in its surface texture or coating, a sample from that part's lot and/or date code should undergo surface testing. For example, respondents said the sample parts should be rubbed with a chemical such as acetone or have their surfaces scraped in order to detect remarking. This testing may reveal sanding marks, original part numbers, or original surfacing.

X-ray analysis is another recommended non-invasive testing method. It allows inspectors to view the inside of the part. X-ray analysis can show if the part packaging is empty, if the die is the wrong size, and if the internal wiring looks authentic.

A step beyond x-ray analysis is destructive physical analysis, including de-lidding or de-capping. This method of testing requires dismantling a part in order to inspect what is inside of the packaging. It is more in-depth than x-ray analysis, as inspectors physically examine the die and connections to determine authenticity. If this approach is used, at least one part per date and/or lot code should undergo destructive physical analysis.

There are also several types of electrical testing that can be used to detect counterfeits. The main activity recommended involves plugging a part into a circuit board in order to determine its performance. Electrical testing can reveal parts that simply do not work and parts that do not meet performance requirements.

Another type of electrical testing is temperature or thermal cycling. This method tests a part’s resistance to extreme high and low temperatures, which is not done during standard electrical testing. Temperature cycling exposes parts to alternating extreme temperatures, and can reveal components that were remarked as military or higher-grade but cannot perform as such.[105]

Burn-in testing is a third, more intense type of electrical testing. This method stresses microcircuits at or above maximum-rated operating conditions in order to screen out early lifetime failures. Burn-in testing can also reveal used parts that were remarked as new and would otherwise pass regular electronic testing and temperature cycling.[106]

TESTING FACILITIES AND INVENTORY STORAGE

Many survey respondents suggested that organizations should establish internal testing capabilities. If an organization chooses to use external, third-party testing facilities, it should put those facilities through the same level of scrutiny recommended earlier for suppliers. A testing facility should not be used until an organization has determined it can be trusted to conduct required tests in a thorough manner and provide valid testing certification.

Incoming parts that pass all levels of inspection and testing can be placed into an organization’s inventory, but several survey respondents said the inventory should be kept under strict control. Parts for different customers should be kept separate, especially if customers required that the parts be purchased from different suppliers. Parts purchased from different suppliers should not be co-mingled unless those parts are kept in separate, sealed packaging and can be easily tracked. If it is later discovered that counterfeit parts were placed into inventory, it will be easier and less costly to find them.

[105] MIL standard MIL-STD-883, *Test Method Standard, Microcircuits*, has specific information on testing procedures, including thermal cycle testing.

[106] MIL standard MIL-STD-883, *Test Method Standard, Microcircuits*, has specific information on testing procedures, including burn-in testing.

BEST PRACTICES FOR MANAGING COUNTERFEITS

Organizations not only have to take steps to avoid counterfeits, they also must consider what to do if they encounter counterfeit components. As with all other counterfeit avoidance policies and procedures, employees need clear, written guidance on what steps to take if they suspect a part is counterfeit.

Organizations should remove suspected and confirmed counterfeit parts from regular inventory and quarantine them. This action will keep the parts from accidentally being sold or incorporated into systems. According to conversations with the U.S. Attorney's Office, the Federal Bureau of Investigation (FBI), and the Defense Criminal Investigative Agency (DCIS), the parts should not be returned to suppliers but turned over to the proper authorities.[107]

All organizations should maintain an internal database to track all suspected and confirmed counterfeit components. A database allows an organization to maintain knowledge related to counterfeits after employees leave, track trends, and avoid counterfeits in the future. The database could maintain and track many variables, including:

- companies and individuals known and suspected of selling counterfeit parts;
- parts known and suspected of being counterfeit, including lot and date codes, part numbers, and part images;
- countries of origin;
- sources of reporting;
- U.S. Customs seizures; and
- GIDEP reports and other database notifications.

In addition to keeping an internal database, organizations should report all information on suspected and confirmed counterfeit parts to industry associations and databases. One of the more prominent information-sharing mechanisms for organizations conducting business with the U.S. Government is GIDEP. Participants receive GIDEP alerts on reported counterfeit issues,

[107] See Appendix I for law enforcement agency contact information.

and the information is kept in a central database.[108] The industry associations ERAI and IDEA also maintain databases on reported counterfeit incidents.[109]

Suspected and confirmed counterfeit parts need to be reported to law enforcement agencies in order for them to investigate incidents and stop counterfeiters. All counterfeits connected to defense-related programs should be reported to the Defense Criminal Investigative Service (DCIS), while those related to aviation should be reported to the FAA Suspected Unapproved Parts program. Counterfeits that are purely commercial in nature should be reported to the FBI.[110]

BEST PRACTICES FOR U.S. GOVERNMENT PROCUREMENT

In addition to the previously mentioned practices, BIS cataloged best practices for Department of Defense (DOD) entities. [111] DOD parts procurement and storage activities are bound by different rules than industry, and require supplemental counterfeit avoidance policies to fit their unique circumstances using industry-wide and unique best practices.

As with industry, a successful DOD counterfeit avoidance policy requires increased awareness and knowledge of counterfeits throughout the armed services. DOD personnel involved with procurement, handling, storing, and consuming electrical components, both domestically and at military bases overseas, need to be informed of the problem of counterfeits and instructed on how to avoid them. This will require specific guidance on counterfeits to be implemented throughout DOD and the armed services.

There is also a need for increased communication between all DOD units that procure, handle, store, and consume electrical components. While individual counterfeit avoidance efforts within

[108] OMB Policy Letter 91-3 instructs all parts of the Executive Branch to participate in GIDEP.
[109] ERAI and IDEA limit access to their databases to members.
[110] See Appendix I for law enforcement agency contact information.
[111] Many of the best practices suggested for DOD can also be used for non-DOD U.S. Government agencies.

each military service are necessary, those efforts need to be shared and discussed with the other services. This type of cooperation allows successful coordination of best practices and could improve all actions to keep counterfeits out of the defense supply chain.

Depots, bases, and field units need to increase intra-departmental communication, as well. Survey responses indicate that there is little information on malfunctioning and non-operational electronic parts going from field units and end-users back to the depots and command units, which gives a false impression of supply chain security. Personnel that use parts need to file Product Quality Deficiency Reports (PQDRs) in a timely manner to report non-working electronic components. If this proves to be impractical for the field units, then another system of reporting needs to be developed in order for information on possible counterfeit parts to be shared with proper authorities.

DOD survey respondents also indicated a need for changes to be made in the Federal Acquisition Regulations (FAR) and Defense Federal Acquisition Regulations (DFAR). Higher procurement standards and stricter policies should be implemented for mission critical and sensitive components in order to limit the possibilities for counterfeits to cause serious damage to defense systems and personnel. One approach involves amending the regulations to clarify the importance of “best value” instead of “lowest bid” solicitations for highly sensitive electronic components. This could lead to more expensive parts but ensure quality (including an authenticity determination) is a factor in sourcing. It could also limit opportunities for counterfeits to enter the supply chain, as illegitimate parts are often the cheapest available.

RECOMMENDATIONS FOR THE U.S. GOVERNMENT

Based on survey responses, interviews, and field visits, the Bureau of Industry and Security has developed recommendations for the U.S. Government in responding to the problems of counterfeit electronics. These recommendations are designed to curtail the inflow of counterfeit electronic parts into manufacturing and maintenance supply chains.

1. Consider establishing a centralized federal reporting mechanism and database for collecting information on suspected/confirmed counterfeit electronic parts for use by U.S. Government suppliers and all federal agencies.

   - Require U.S. Government suppliers and federal agencies to systematically report counterfeit electronic parts to the national federal reporting mechanism
   - Determine the feasibility of opening the reporting mechanism to collect information from industry as a whole.
   - Issue regular bulletins to industry and federal agencies on counterfeit electronic parts and related counterfeit activity.
   - Provide legal indemnification to organizations and federal agencies reporting suspected/confirmed counterfeit electronic parts to protect against lawsuits from parts suppliers identified during the reporting.

2. Clarify the criteria in the Federal Acquisition Regulations (FAR), including Defense Federal Acquisition Regulations (DFAR), to promote the ability to award electronic parts contracts on the basis of “best value” rather than on the basis of “lowest price” or “low bid.”

3. The Department of Justice (DOJ), in coordination with other relevant federal agencies, should issue clear, unambiguous legal guidance to industry and U.S. federal agencies with respect to:

   - Civil and criminal liabilities under federal law for knowingly selling or otherwise dealing with trade in counterfeit electronic parts that result in financial loss, loss of property, and/or loss of life, and related liabilities for failing to report counterfeits in a timely manner;
   - Requirements for handling, holding, returning to the supplier, and/or turning suspected/confirmed counterfeit parts over to law enforcement;
   - The responsibility of purchasers of electronic parts and components to make payments to suppliers for shipments of suspected/confirmed counterfeit parts either turned over to law enforcement authorities or held by purchasers due to instruction of law enforcement authorities; and
   - Appropriate points of contact at the Federal Bureau of Investigation (FBI) for industry and federal agencies to report suspected criminal activity related to counterfeit electronic parts.

4. Establish a dialogue with law enforcement agencies on the potential need to increase prosecution of counterfeiters and those entities knowingly distributing counterfeit electronic parts.

   - Expand the capabilities of the U.S. Customs and Border Protection (CBP) to inspect and detect shipments of counterfeit electronic parts and systems.
   - The FBI, the Defense Criminal Investigative Service (DCIS), the Federal Aviation Administration (FAA), CBP, and other appropriate federal agencies should broaden counterfeit electronics-related activity to include industry.

5. DOD, NASA, and other federal agencies, in cooperation with the semiconductor and aerospace industries, should consider establishing a government data repository of electronic parts information and for disseminating best practices to limit the infiltration of counterfeits into supply chains.

   - Identify appropriate industry and/or federal standards for parts procurement and testing to evaluate suspected/confirmed counterfeit parts.
   - Create counterfeit electronic part education and training programs for relevant government personnel and contractors.

6. Develop international agreements covering information sharing, supply chain integrity, border inspection of electronic parts shipped to and from other countries, related law enforcement cooperation, and standards for inspecting suspected/confirmed counterfeits.

   - Educate countries on the risks to their economies and national security posed by counterfeit electronic parts.
   - Urge countries to discourage trade in counterfeit parts and to enforce intellectual property laws.
   - Establish guidance for the proper destruction, recycling, and/or disposal of electronic parts and systems.

7. Address funding and parts acquisition planning issues within DOD and industries associated with the procurement of obsolete parts for the U.S. Government, including:

   - Better forecasting future parts requirements;
   - Improving the timely notice by manufacturers of part production cessation; and

- Disseminating information on industry and government facilities capable of designing and fabricating legacy parts.

*****

No one practice or combination of practices will prevent counterfeit parts from entering the supply chain. Each sector of the supply chain faces different circumstances and problems, but the best practices and recommendations presented in this chapter supply a common foundation organizations can use to create effective and complementary counterfeit avoidance procedures. A comprehensive risk mitigation plan, along with cooperation throughout the supply chain, can significantly reduce the risk created by counterfeits. Ultimately, every element of the supply chain must work together to solve the problem of counterfeit parts and components.

APPENDIX A – GLOSSARY

After-Market Manufacturer: A company engaged in the manufacture of electronic products initially but no longer produced by an original component manufacturer.

Arsenal: An establishment for the manufacture and/or storage of military equipment, weapons, and related parts and materials.

Assembled Circuit Board: An engineered circuit board populated with electronic components that forms a working system or subsystem.

Authorized Distributor: A company that is authorized by an Original Component Manufacturer (OCM) or Original Equipment Manufacturer (OEM) to market, store, and ship OCM/OEM products.

Bare Circuit Board: An engineered circuit board with defined printed circuits on one or more layers of the board that serves as the foundation for integrating electronic components into a working system or subsystem.

Best Practice: An efficient and effective standard process that can be adopted by multiple organizations.

"Best Value": A purchasing strategy that seeks to identify the company that offers the highest quality product at the lowest price.

Brokers: Companies/individuals engaged in the marketing of electronic parts, often scarce parts. Brokers frequently do not actually possess in inventory the parts being sought, but act as “middle men” to arrange the sale of the part from a third party.

Burn-In Testing: A test which involves running a system or device for a period of time to ensure that all components are working properly.

Circuit Board Assembler: A company that manufacturers bare and/or assembled circuit boards.

Certificate of Conformance: Document certified by a competent authority that the supplied good or service meets the required specifications.

Contract Manufacturer: A manufacturer that produces made-to-order custom electronic parts, including assembled electronic boards, for a private or government customer. Parts and board products manufactured by the contract manufacturer are not brand-name products marketed and sold by the contract manufacturer.

Counterfeit: An electronic part that is not genuine because it 1) is an unauthorized copy; 2) does not conform to original OCM design, model, and/or performance standards; 3) is not produced by the OCM or is produced by unauthorized contractors; 4) is an off-specification, defective, or used OCM product sold as "new" or working; or 5) has incorrect or false markings and/or documentation.

Critical Safety Parts: Parts whose failure would cause loss of life, permanent disability or major injury, loss of a system, or significant equipment damage.

Die: A single integrated circuit (or chip) cut from the wafer on which it was manufactured.

Distribution Depot: Distribution depots store and distribute goods, materials and parts to the United States armed forces.

Defense Microelectronics Activity (DMEA): A Department of Defense facility located near Sacramento, CA, which manufactures integrated circuit products and electronic systems for U.S. Government national security applications.

Decapsulation (decapping): When the packing of a component is opened in hermetic conditions to allow for the examination of the die and internal features of the package.

Discrete Electronic Component: Individual components such as capacitors, diodes, resistors, transistors that can be mounted on a circuit board to form a working electronic system.

Electronic Testing: Evaluating the functionality of a discrete component or IC part and determining whether the electrical parameters of the part conform with the alternating current (AC) and direct current (DC) characteristics specified by its manufacturer. Measurements can be made at room temperature or over the recommended operating temperature range for the part.

End-User: The person or entity that uses a product.

Excess Inventory: Legitimate, genuine new electronic part product held by OCMs, OEMs, authorized distributors, contract manufacturers, and U.S. government agencies.

FEDLOG: A Defense Logistics Agency system used to retrieve management, part/reference number, supplier, Commercial and Government Entity (CAGE), freight, Interchangeability and Substitutability (I&S) and characteristics information recorded against National Stock Numbers (NSNs).

First Article Testing: A series of inspections and tests designed to ensure parts conform to drawings or part specifications.

Generalized Emulation of Microcircuits (GEM): Reengineered integrated circuit products whose manufacture has been authorized to meet the need for replacement parts for product that is obsolete. These replacement products are designed and tested to emulate all the functions of microcircuits that are no longer in production.

Gray Market: The trade of parts through distribution channels which, while legal, are unofficial, unauthorized, or unintended by Original Component Manufacturers.

Hologram: Three-dimensional printing used to validate authenticity.

Incident: Occurrences, reports, or transactions pertaining to electronic parts suspected and/or confirmed to be counterfeit. For example, a report involving 10 copies of a single electronic part model equals one incident. Occurrences, reports, and transactions involving three separate electronic part models equal three separate incidents, regardless of the volume counterfeit parts for any given model.

Independent Distributor: A company that markets and distributes electronic parts often acquired as excess inventory from OCMS, OEMs, contract manufacturers, U.S. Government organizations, and other entities. Independent distributors maintain inventories of parts and typically have controlled environments for part storage.

International Traffic in Arms Regulations (ITAR): U.S. Department of State regulations controlling the export and import of defense-related articles and services on the United States Munitions List.

Inventory control point (ICP): An organizational unit or activity within a Department of Defense supply system that is assigned the primary responsibility for the materiel management of a group of items either for a particular Service or for the Defense Department as a whole. Materiel inventory management includes cataloging direction, requirements computation, procurement direction, distribution management, disposal direction and, generally, rebuild direction.

Integrated Circuit: *See Microcircuit.*

Legal Action: Filing of warning letters, civil complaints and lawsuits; filing criminal complaints; support of criminal investigations and prosecution by law enforcement agencies.

Life of Type or Life Time Buy: A final purchase by a DOD organization of an electronic part prior to the cessation of production by its manufacturer.

"Low Bid": A purchasing strategy based upon selecting the company that offers the lowest price for a contract.

Microcircuit: A miniaturized electronic device containing multiple solid-state circuits that work in conjunction to form a complete device with defined functions, and that has been manufactured on the surface of a thin substrate of semiconductor material. In these devices many active or passive elements are fabricated and connected together on a continuous substrate, as opposed to discrete devices, such as transistors, resistors, capacitors and diodes that exist individually.

Mined Die: An integrated circuit product removed from its original OCM package and placed in a new package.

Non-Conforming Parts: Parts that do not meet standard requirements or conditions.

Non-U.S.: Foreign country where microcircuit production, purchase, or company incorporation is located.

Original Component Manufacturer (OCM): A company that manufacturers discrete electronic components and/or microcircuits.

Original Equipment Manufacturer (OEM): A company that supplies equipment to other companies to resell or incorporate into another product using the reseller's brand name.

Pedigree Paperwork: Documentation that tracks a part's history back to its original manufacturer.

Physical Evaluation: A process of confirming that materials used in a discrete component or IC part are genuine. It can involve destructive tests such as decapping the component's package to validate its authenticity; evaluation of materials used in a device's packaging materials (including connection leads and encapsulant); and examination of discrete and IC parts to verify it is genuine using various techniques including layer by layer destructive examination.

Pre-Stock Testing: Testing of products, through any means, before they are placed in a company's inventory.

Prime Contractor: A lead contractor that directs and manages the delivery of large projects or products. Typically, prime contractors rely on subcontractors to provide part or all of the major components, designs, parts, or subsystems required to complete and deliver a working product.

Product Quality Deficiency Report (PQDR): A form used by the military services and the General Service Administration to record and transmit data on defects or nonconforming conditions detected on new or newly reworked Government-owned products, premature equipment failures, and products in use that do not fulfill their expected purpose, operation or service.

Radio Frequency Identification (RFID): Any method of identifying unique items using radio waves.

Scrap: Defective, damaged, or used electronic parts or systems from which electronic parts may be scavenged.

"Seconds": Off specification, sub-standard product made by Original Component Manufacturers/Original Equipment Manufacturer that is normally destroyed by OCM/OEMs.

Subcontractor: A company that provides parts, subsystems, or systems required by a prime contractor for completion of a product or project.

Thermal/Temperature Cycling: Determines the ability of parts to resist extremely low and extremely high temperatures, as well as their ability to withstand cyclical exposures to these temperature extremes.

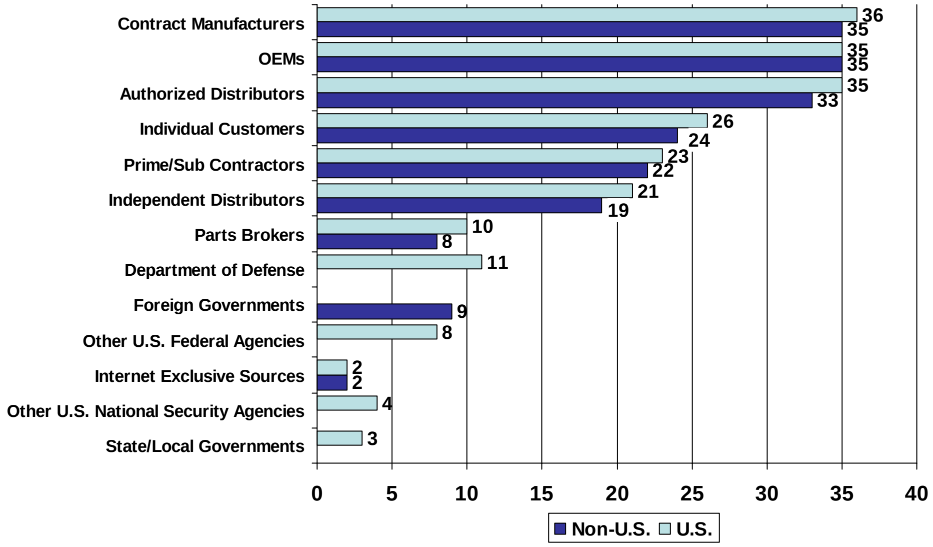
U.S. Munitions List: Articles and services designated by the President of the United States with concurrence from the Department of Defense as being specifically designed or configured for military applications; there are no equivalent civilian or commercial products.

United States: The "United States" or "U.S." includes the 50 states, Puerto Rico, the District of Columbia, the island of Guam, the Trust Territories, and the U.S. Virgin Islands.

Visual Inspection: Non-destructive evaluation involving visual examination for correct labeling, shape, size and dimension, form, fit, color, security coatings, etc. Visual inspection can include use of other non-destructive evaluation such as X-ray, XRF (X-ray fluorescence), and scanning acoustic microscopy.

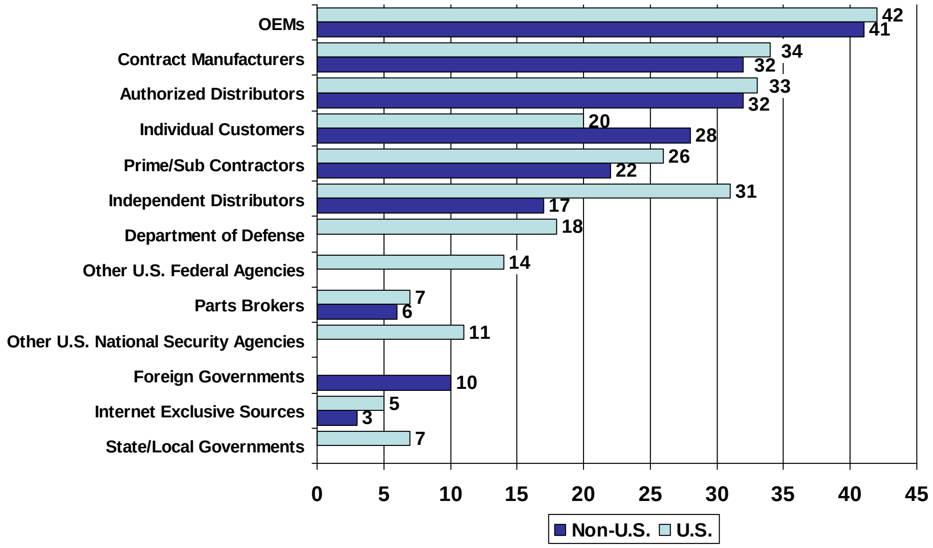
APPENDIX B – ORIGINAL COMPONENT MANUFACTURERS (OCMS) CHAPTER ADDITIONAL CHARTS

Figure B-1: Type of Customers for Discrete Electronic Component Manufacturers



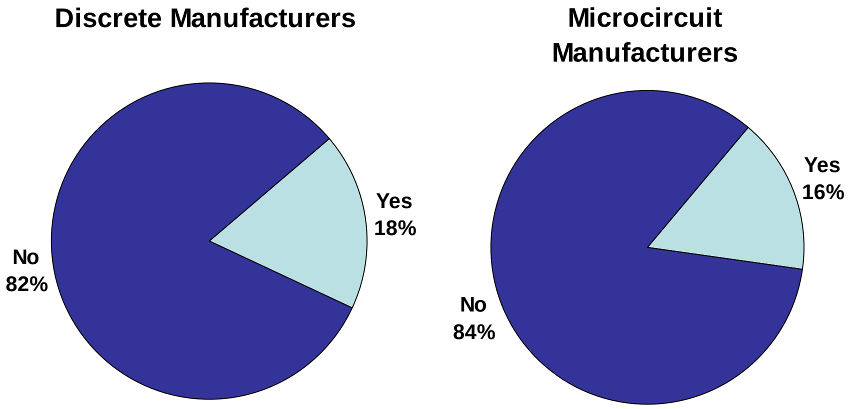
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure B-2: Type of Customers for Microcircuit Manufacturers



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure B-3: Percent of OCMs Auditing Their Inventory for Counterfeit Products



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure B-4: OCMs Experiencing Problems at Contractor-Operated Testing Facilities		
Location of Testing Facility	Number of Companies Indicating a Problem	Problems
U.S.-Based	1	Mismanagement of scrap material.
Non-U.S.	5	Mismanagement of scrap material, stolen rejected products.

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure B-5: Authorities Notified After A Counterfeit Incident – OCMs*

None at All	36%
Customs & Border Protection (CBP)	29%
Government-Industry Data Exchange Program (GIDEP)	12%
Federal Bureau of Investigation (FBI)	12%
Other	12%
Internal Management/Security	10%
Defense Logistics Agency (DLA)	2%
State/Local Authorities	2%
Defense Related Investigative Services (e.g., DCIS, etc.)	2%
Department of Justice (DOJ)	2%
NASA	2%

*** Only includes those companies with counterfeit incidents**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

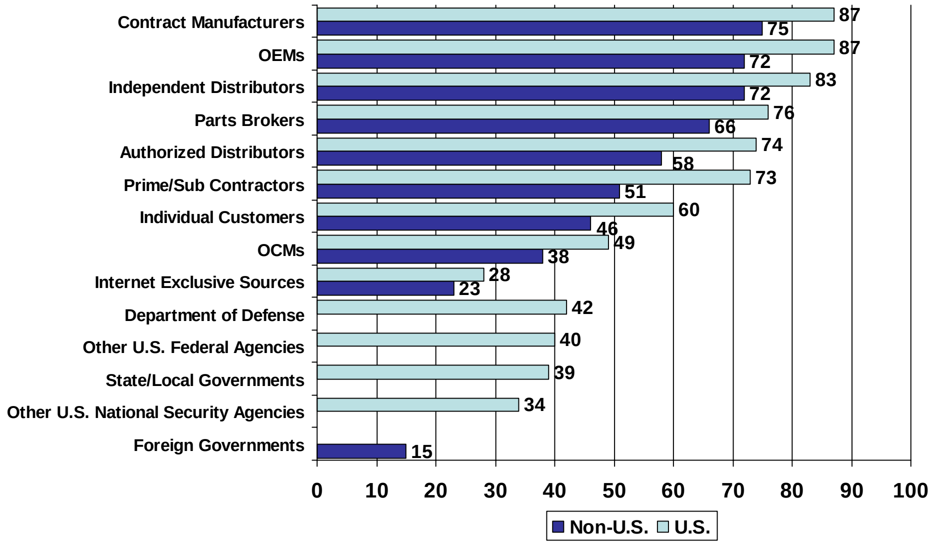
Figure B-6: Authorities Authorized Distributors/End-Users are Told To Contact in Case of Counterfeit Incidents

My Company (Survey Respondent)	66%
None	28%
State/Local Authorities	5%
Other	2%
Defense Logistics Agency (DLA)	2%
Customs & Border Protection (CBP)	1%
Department of Justice (DOJ)	1%
Government-Industry Data Exchange Program (GIDEP)	1%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

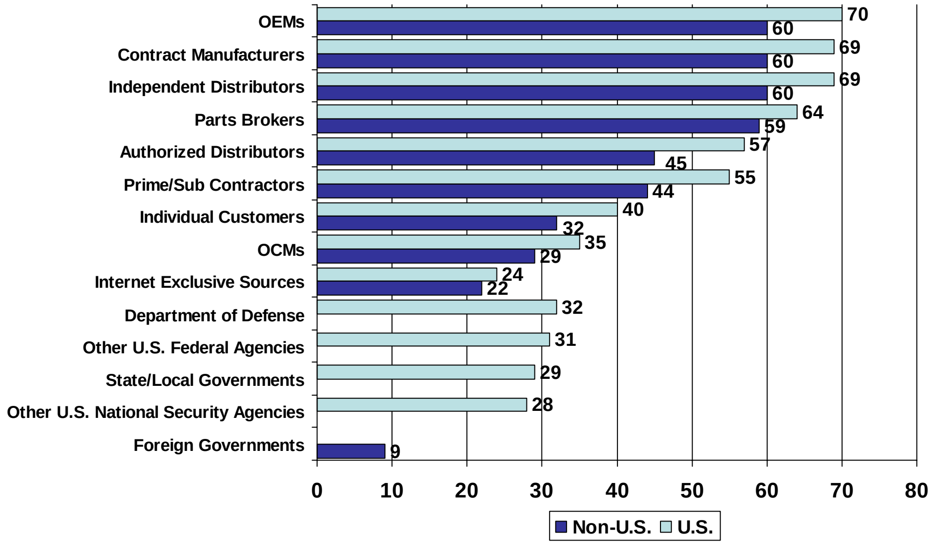
APPENDIX C – DISTRIBUTORS: AUTHORIZED AND UNAUTHORIZED CHAPTER ADDITIONAL CHARTS

Figure C-1: Type of Customers for Discrete Electronic Components - Distributors



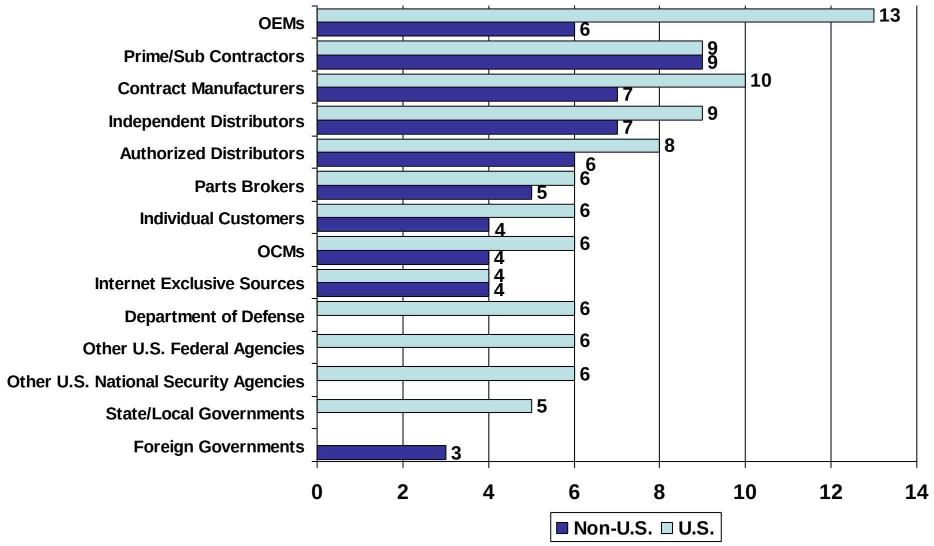
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure C-2: Type of Customers for Microcircuits - Distributors



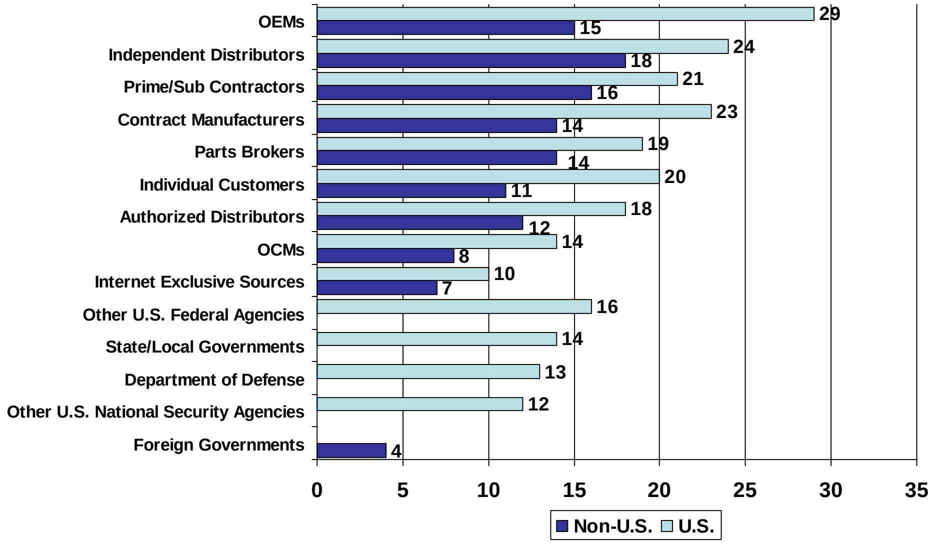
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure C-3: Type of Customers for Bare Circuit Boards - Distributors



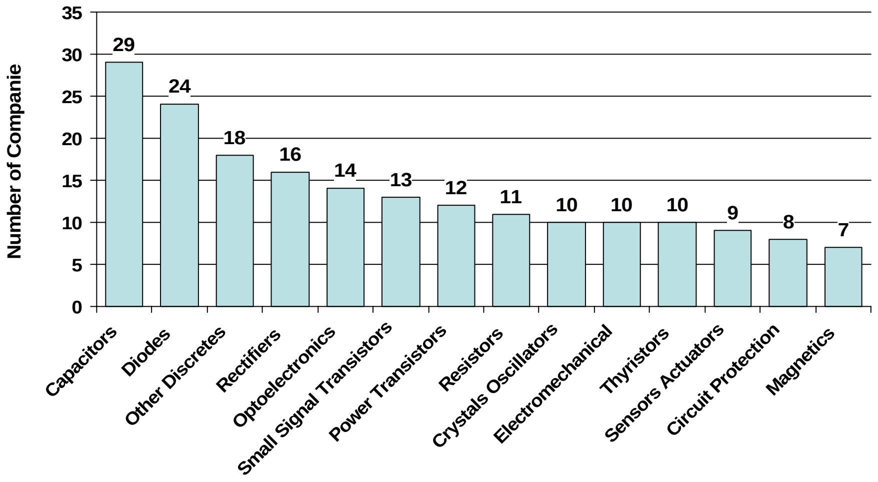
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure C-4: Type of Customers for Assembled Circuit Boards - Distributors



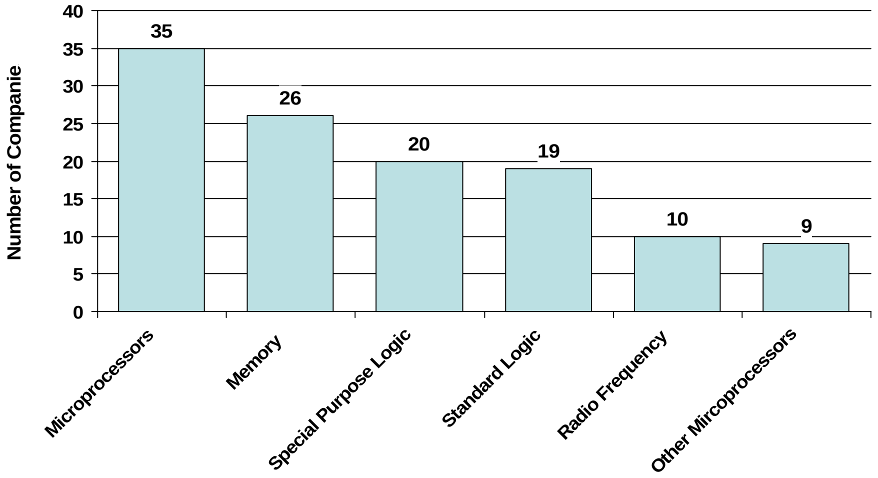
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure C-5: Type of Purchased Parts Suspected/Confirmed to be Counterfeit - Discretes



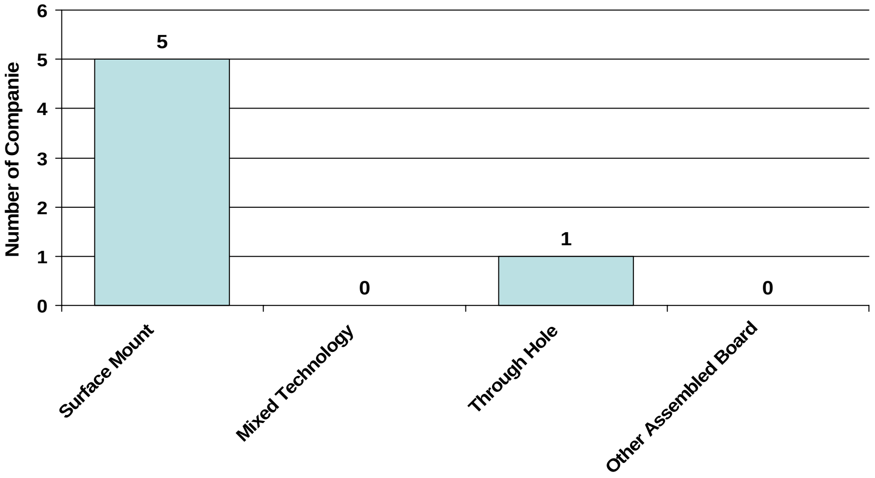
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure C-6: Type of Purchased Parts Suspected/Confirmed to be Counterfeit - Microcircuits



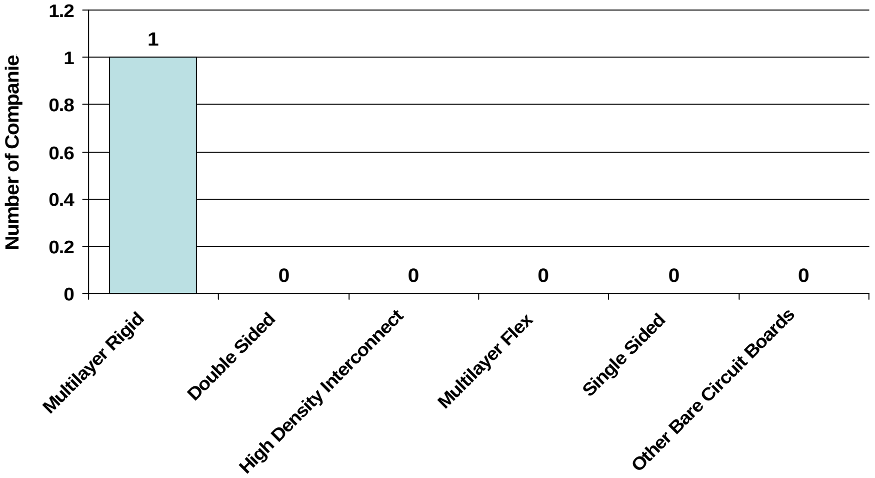
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure C-7: Type of Purchased Parts Suspected/Confirmed to be Counterfeit - Assembled Circuit Boards



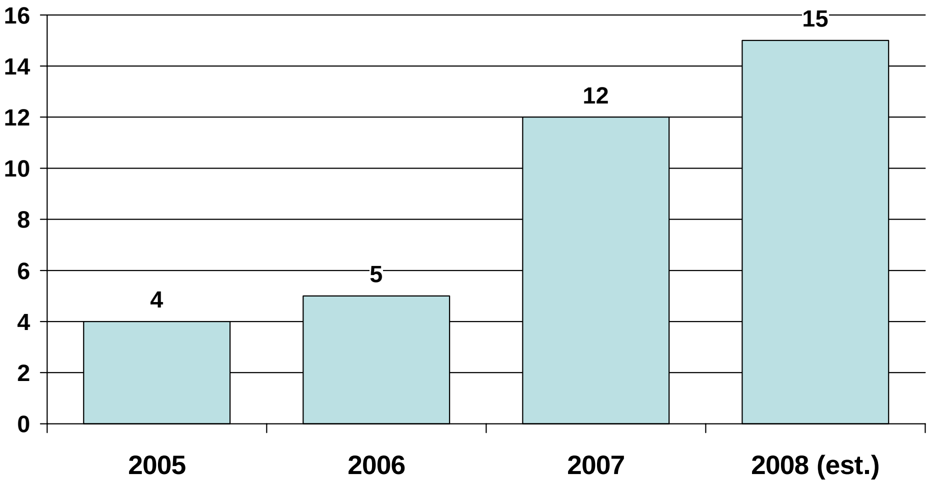
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure C-8: Type of Purchased Parts Suspected/Confirmed to be Counterfeit - Bare Circuit Boards



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

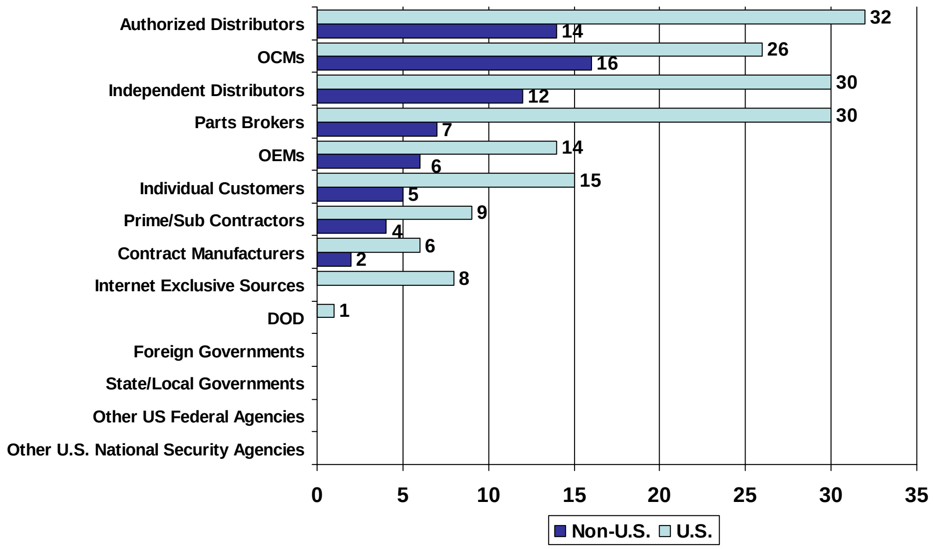
Figure C-9: Number of Incidents Reported to Government Authorities - Distributors



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

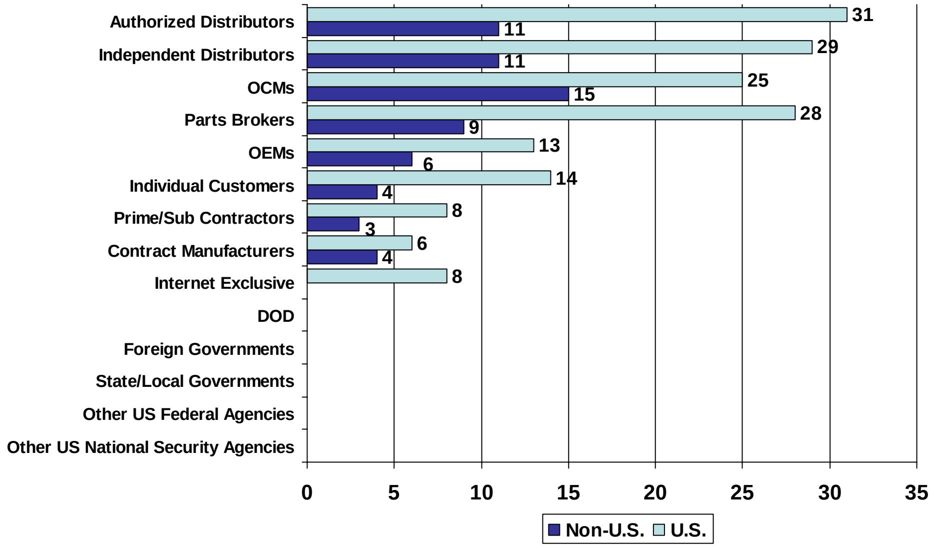
APPENDIX D – CIRCUIT BOARD ASSEMBLERS CHAPTER ADDITIONAL CHARTS

Figure D-1: Type of Suppliers of Discrete Electronic Components – Circuit Board Assemblers



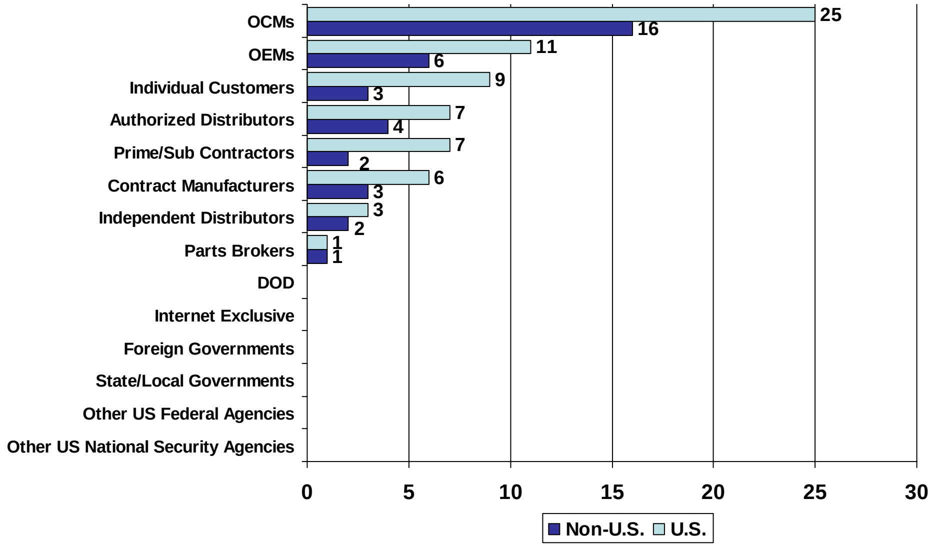
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure D-2: Type of Suppliers of Microcircuits – Circuit Board Assemblers



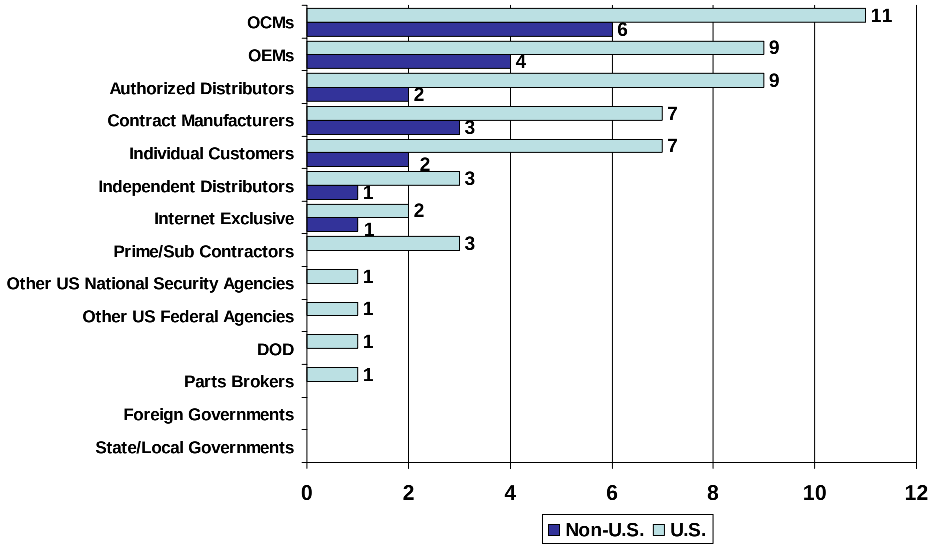
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure D-3: Type of Suppliers of Bare Circuit Boards – Circuit Board Assemblers



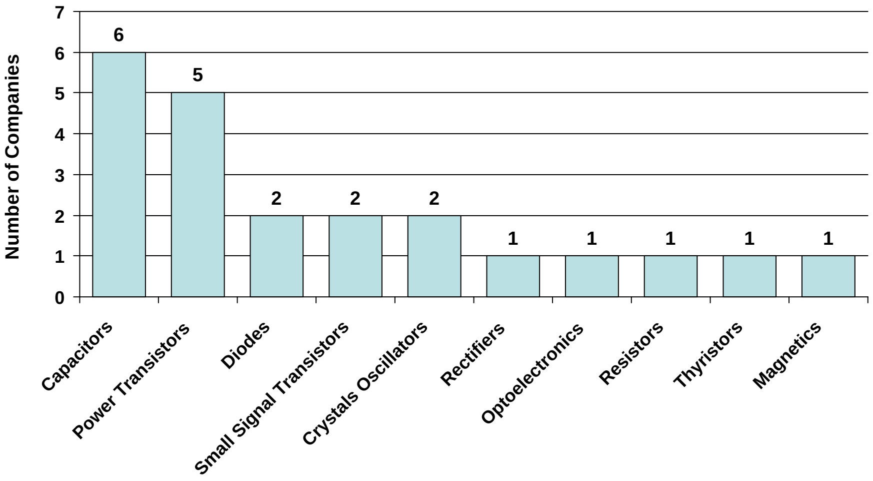
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure D-4: Type of Suppliers of Assembled Circuit Boards – Circuit Board Assemblers



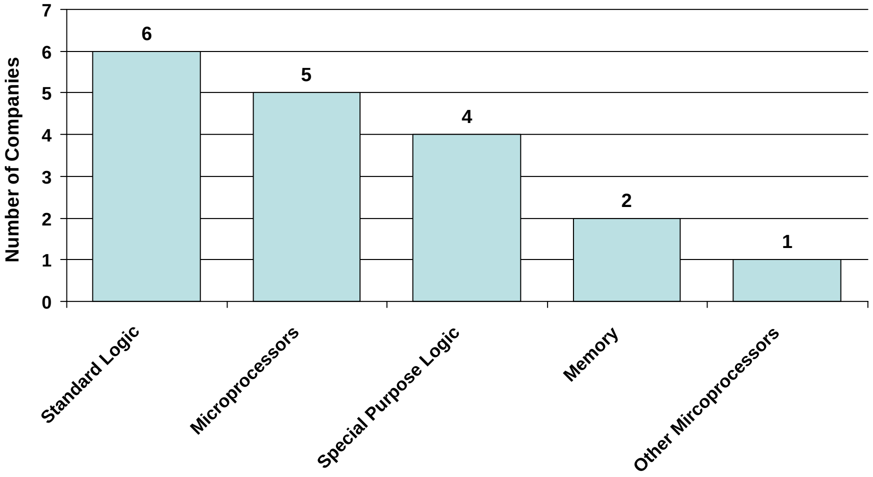
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure D-5: Type of Purchased Parts Suspected/Confirmed to be Counterfeit - Discretes



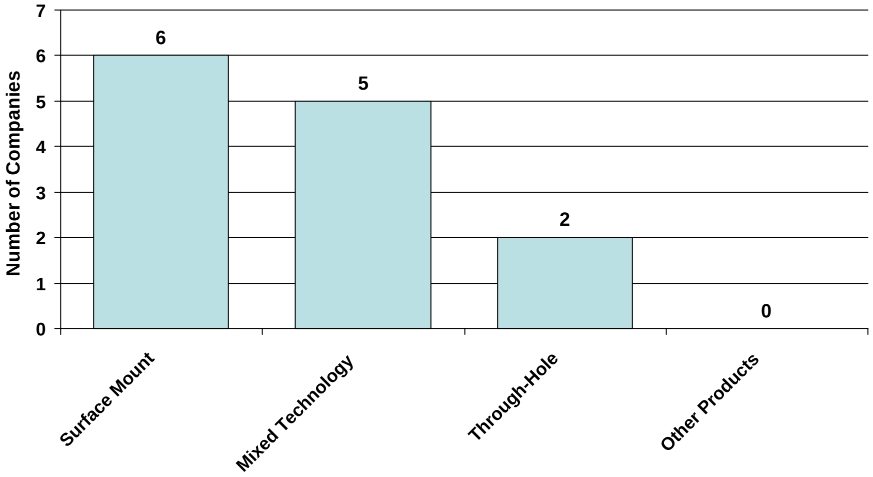
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure D-6: Type of Purchased Parts Suspected/Confirmed to be Counterfeit - Microcircuits



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

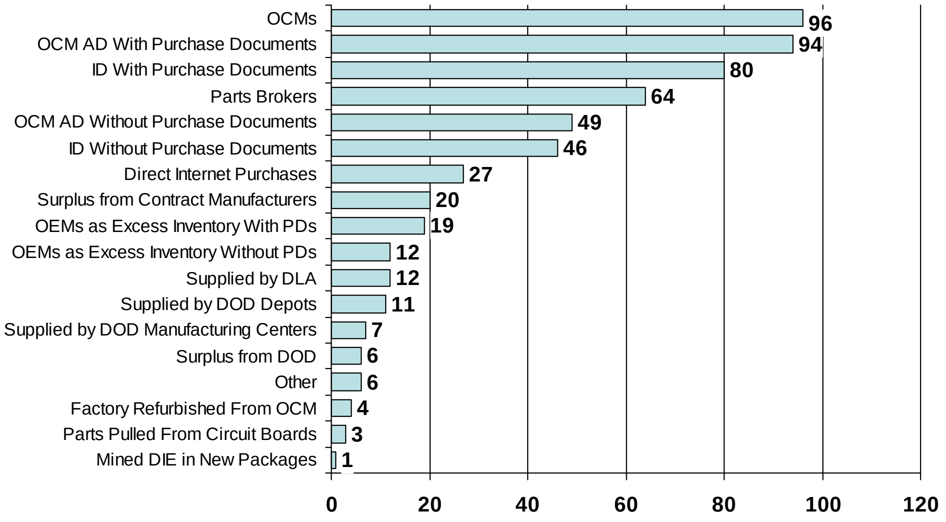
Figure D-7: Type of Purchased Parts Suspected/Confirmed to be Counterfeit – Assembled Circuit Boards



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

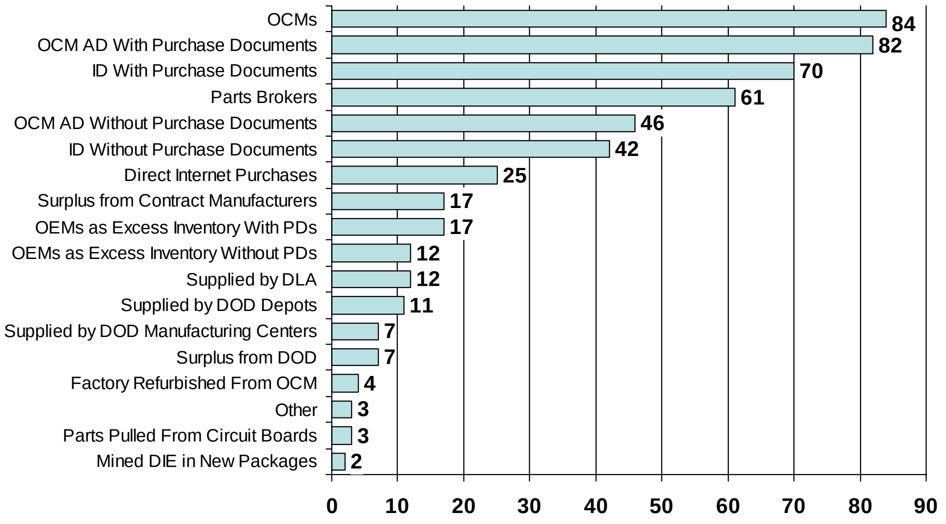
APPENDIX E - PRIME CONTRACTORS AND SUBCONTRACTORS CHAPTER ADDITIONAL CHARTS

Figure E-1: Source of Discrete Electronic Components - Prime/Sub Contractors



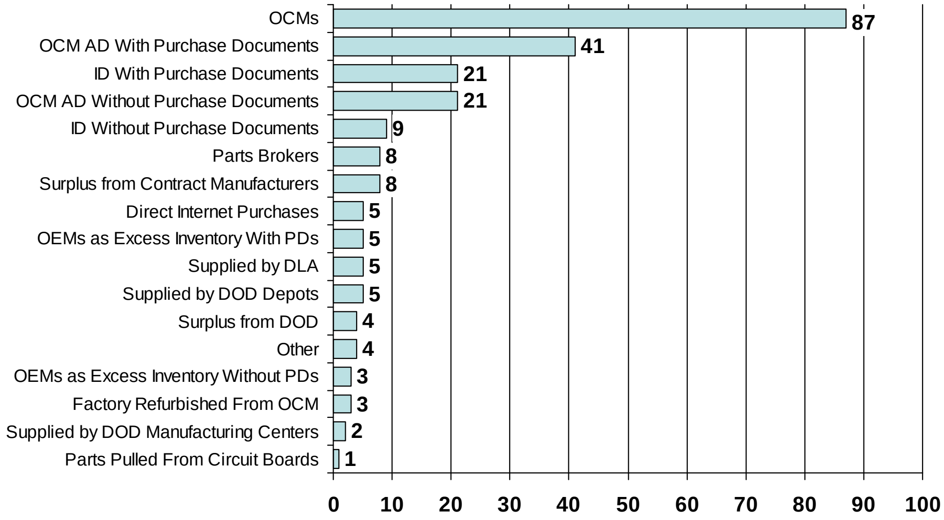
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure E-2: Source of Microcircuits – Prime/Sub Contractors



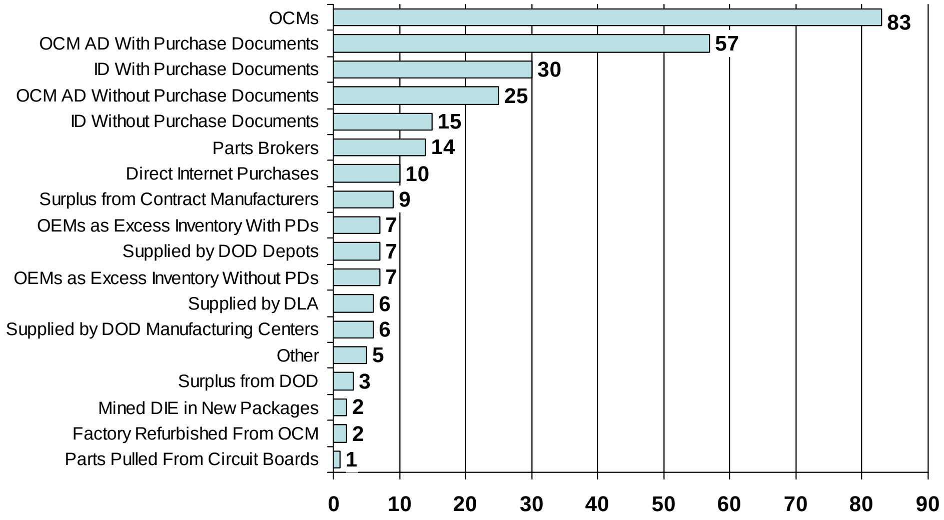
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure E-3: Source of Bare Circuit Boards – Prime/Sub Contractors



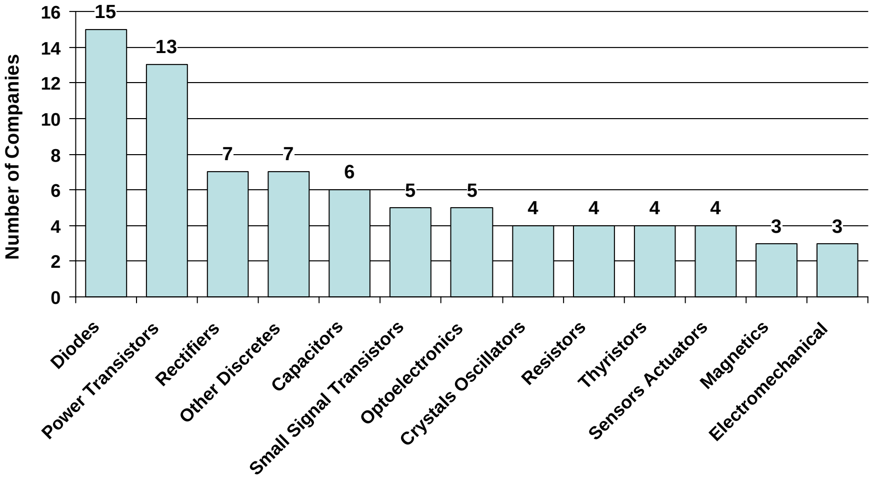
Source: U.S. Department of Commerce, Office of Technology Evaluation,
Counterfeit Electronics Survey, November 2009.

Figure E-4: Source of Assembled Circuit Boards - Prime/Sub Contractors



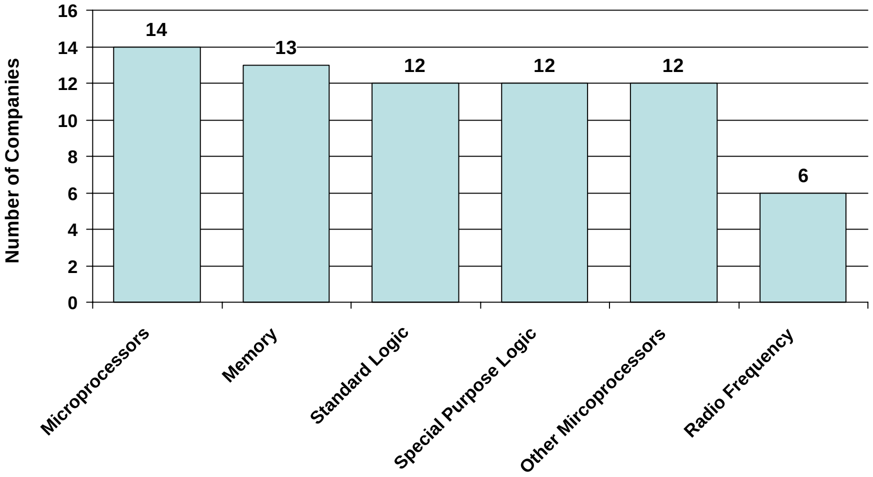
Source: U.S. Department of Commerce, Office of Technology Evaluation,
Counterfeit Electronics Survey, November 2009.

Figure E-5: Type of Purchased Parts Suspected/Confirmed to be Counterfeit - Discretes



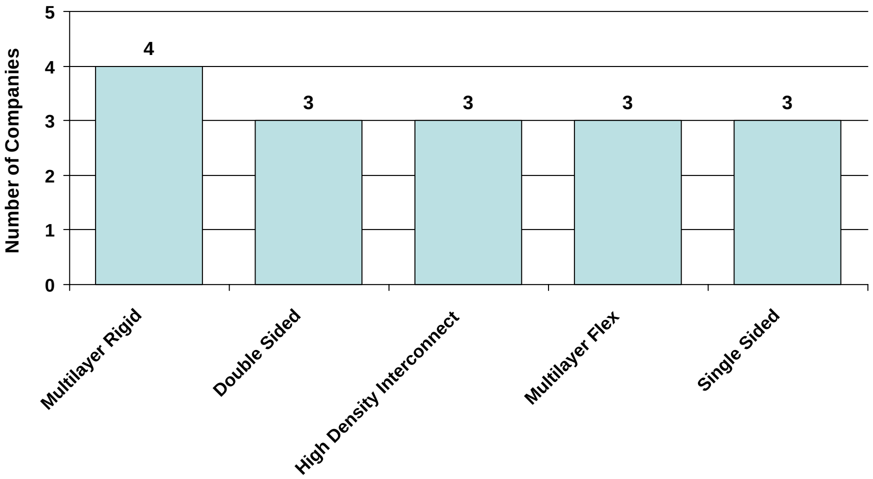
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure E-6: Type of Purchased Parts Suspected/ Confirmed to be Counterfeit - Microcircuits



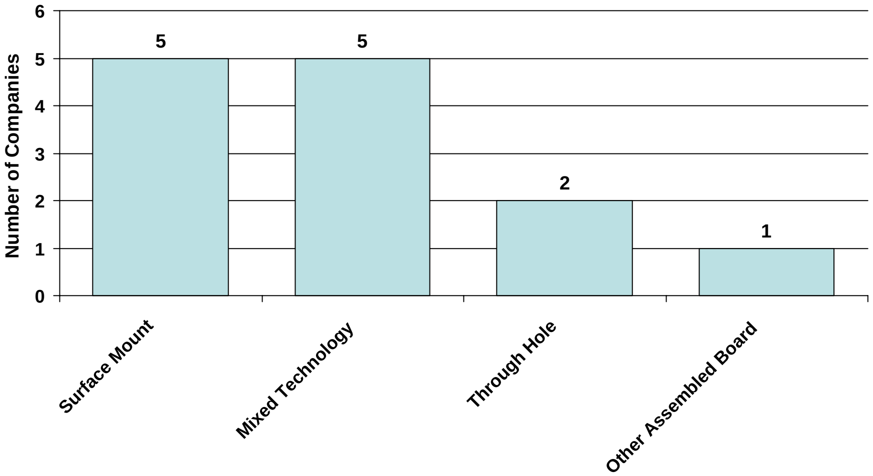
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure E-7: Type of Purchased Parts Suspected/ Confirmed to be Counterfeit – Bare Circuit Boards



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

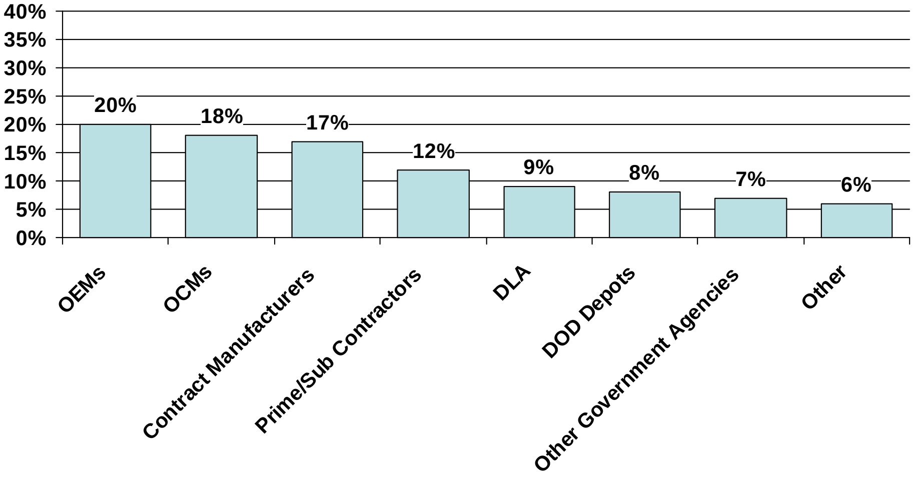
Figure E-8: Type of Purchased Parts Suspected/Confirmed to be Counterfeit – Assembled Circuit Boards



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

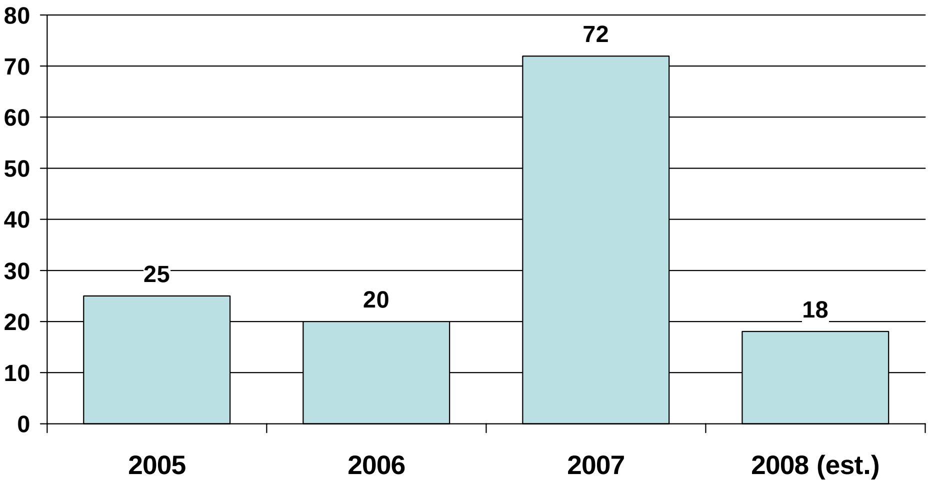
Figure E-9: How Customers Notify Prime/Sub Contractors Concerning Counterfeit Parts	
Website	14%
Other	12%
General Phone Call	11%
E-mail	11%
Hotline	6%
Through GIDEP	5%
Through Sales Contacts	2%
None	54%
*** Companies were permitted to answer 'Yes' to multiple methods.**	
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.	

Figure E-10: Percent of Prime/Sub Contractors Who Buy Back Excess Inventory by Customer Type



Source: U.S. Department of Commerce, Office of Technology Evaluation,
Counterfeit Electronics Survey, November 2009.

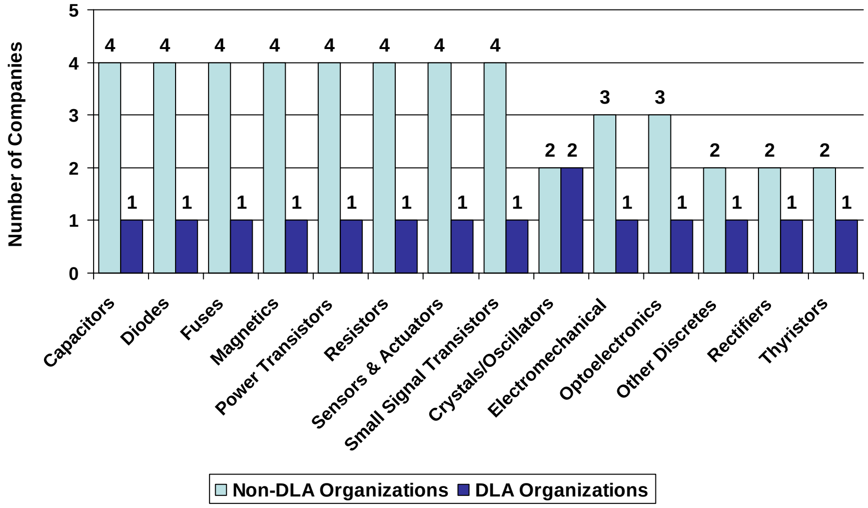
Figure E-11: Number of Incidents Reported to Government Authorities – Prime/Sub Contractors



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

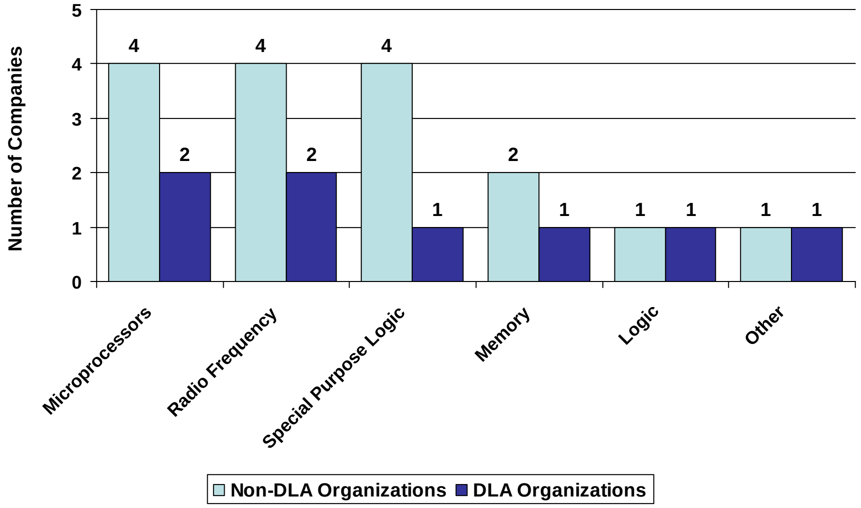
APPENDIX F – DEPARTMENT OF DEFENSE CHAPTER ADDITIONAL CHARTS

Figure F-1: Type of Purchased Parts Suspected/Confirmed to be Counterfeit - Discretes



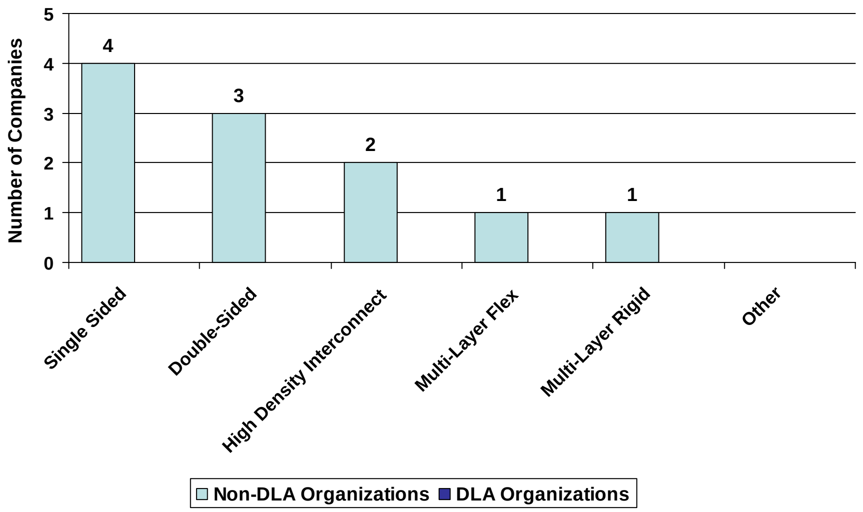
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure F-2: Type of Purchased Parts Suspected/Confirmed to be Counterfeit - Microcircuits



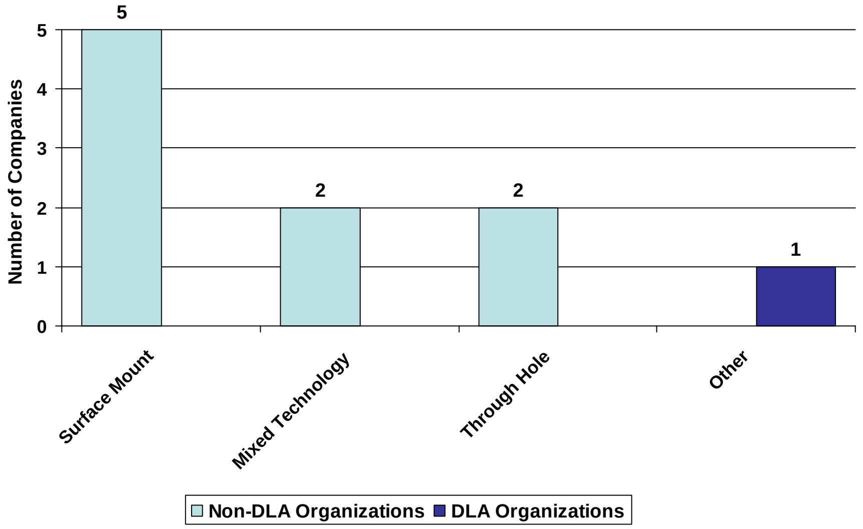
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure F-3: Type of Purchased Parts Suspected/ Confirmed to be Counterfeit – Bare Circuit Boards



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

Figure F-4: Type of Purchased Parts Suspected/ Confirmed to be Counterfeit – Assembled Circuit Boards



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

APPENDIX G – DEFENSE SUPPLY CENTER COLUMBUS COUNTERFEIT AVOIDANCE ACTIONS

The Defense Logistics Agency is taking steps to block the flow of counterfeit parts into DOD maintenance and manufacturing centers. Until late last summer, approximately 50 percent of the electronic discrete components and counterfeit electronic parts purchases executed by Defense Supply Center Columbus (DSCC) were made through its automated electronic system without significant staff oversight.

The agency buys electronic commercial-, industrial-, and military specification-grade parts. Electronic parts purchases are concentrated in two principal categories (Federal Stock Numbers 5961 and 5962), which contain 95,260 national stock numbers (NSNs). Of that total, 12,500 NSNs are for parts that are "actively" ordered – 68, 400 orders, for example, in 2008.

In response to reports from branches of the Armed Forces and industry concerning escalating rates of potential counterfeits, defective, and non-conforming parts, in August 2008 DSCC required that all purchases of discrete and microcircuit electronic parts would be made manually by staff. To accomplish this, DSCC assigned nine full-time personnel to assist the existing staff of five persons performing electronics part purchases; and authorized overtime work.

To further limit infiltration of defective, non-conforming, and counterfeit electronic parts into DOD supply chains, DSCC is implementing a Qualified Suppliers List Distributors (QSLD) program by the fall 2009.[112] This will require DSCC, whenever possible, to purchase electronic parts designated as Federal Stock Class (FSC) 5961 and 5962 from distributors that are certified as complying with JEDEC standard JESD31 and other DOD

[112] "QSLD Program," Defense Supply Center Columbus, 29 Jun 2009, Defense Logistics Agency, <http://www.dscc.dla.mil/offices/sourcing_and_qualification/offices.asp?section=QSL>.

and electronics industry standards.[113] Only factory-authorized part distributors and independent part distributors listed on the QSLD will be able to receive contact awards.

DSCC says the purpose of this prequalification program is to lower risks associated with purchasing electronic parts by removing uncertainties associated with part traceability. QSLD suppliers will be vendors that have demonstrated that they routinely adhere to high operating standards.

This approach, says, DSCC, should reduce the need for testing, engineering reviews, and other activities that can delay acquisitions and increase acquisition costs. The QSLD program also will enable DSCC to resume the use of automated electronic parts purchasing, but with a modification from past practice. All purchases made through the QSLD system will be subject to a final manual review prior to execution. About 50 percent of parts would be acquired through the system, enabling DSCC to reassign some personnel to other duties.

DSCC does not purchase all electronic parts used by DOD. Procurement offices and maintenance centers across the Armed Forces also buy parts on a limited basis. DSCC hopes that the QSLD program it is standing up will set a “gold standard” for all branches of the Armed Forces to emulate in their acquisition of parts.

There will be a continuing need to actively manage many purchases of electronic parts where they are not available through the QSLD program. In these instances, DSCC parts buyers now require suppliers to document 100 percent traceability to original component manufacturers and/or their authorized distributors. When that can not be done, testing and other engineering reviews must be performed on samples from part lots prior to the purchase, according to DSCC officials.[114] DSCC has in-house capabilities to test and

[113] JEDEC Standard JESD31, *General Requirements for Distributors of Commercial and Military Semiconductor Devices*, can be found at http://www.jedec.org.

[114] Based on information provided to the Office of Technology Evaluation on June 22, 2009, by Ernest Reid, Chief of Division 2, Maritime Supplier Operations Group, Land and Maritime Support Command, Defense Supply Center Columbus.

evaluate discrete electronic components and microcircuit parts at its Electronic Parts Testing Center.

DSCC officials state that their ability to avoid defective, non-conforming, and counterfeit parts would be enhanced with better reporting across DOD manufacturing depots, maintenance centers, and other operations that consume and/or order parts. The number of product quality deficiency reports (PDQRs) they receive from the field appear low relative to the scope of problems with suspect parts. According to DSCC officials there is no set minimum number or set value on electronic parts that must be reached in order for DOD staff or managers to file PDQR reports.[115]

Maintenance personnel may require additional direction on filing PDQRs when encountering numbers of defective parts, DSCC staff note. In addition, the process for filing PDQR reports may need to be simplified and automated on an electronic system ensure timely notification to DSCC – and as necessary to other DOD units, federal agencies, and industry. Without robust feedback from its DOD customers on parts problems, DSCC officials note, it can be hard to respond effectively to capture suspect parts in the supply chain.

[115] Capt. Roland G. Wadge, Director, Maritime Supply Operations, Defense Supply Center Columbus.

APPENDIX H – BIS EXPORT MANAGEMENT AND COMPLIANCE PROGRAM

The following is a version of the Bureau of Industry and Security's Export Management and Compliance Program that has been modified to address counterfeit part avoidance.[116] It can be used by organizations as the foundation for an internal counterfeit avoidance and management program.

An Anti-Counterfeit Compliance Program can:

- Reinforce senior management commitment to combat counterfeits and comply with relevant U.S. laws and regulations to all parties within the company.
- Provide management structure and organization for the secure processing of transactions.
- Enhance accountability for anti-counterfeiting tasks by identifying who is responsible for performing each part of the process and who is responsible for overall effectiveness of the plan.
- Provide compliance safeguards throughout a company's supply chain to ensure order processing "due diligence" checks produce secure sourcing decisions.
- Provide written instructions for employees to blend into their daily responsibilities to "screen" transactions against policies and procedures.
- Serve as a vehicle to communicate "red flag" indicators that raise questions about the legitimacy of a transaction.
- Provide personnel with tools to help them ensure they are performing their anti-counterfeiting functions accurately and consistently (e.g., internal databases for tracking, reporting to industry organizations and government authorities).
- Identify transactions that could normally proceed, but because of the source, require additional scrutiny (e.g., additional testing and validation).
- Streamline the process and reduce time spent on compliance activities when employees have written instructions, tools and on-going training.
- Protect employees through training and awareness programs from inadvertently using or introducing counterfeits into supply chains (e.g., returns, restocking, co-mingling inventory).

[116] More information on the Export Management and Compliance Program can be found at http://www.bis.doc.gov/complianceandenforcement/emcp.htm.

APPENDIX I - U.S. LAW ENFORCEMENT AND GOVERNMENT AGENCY CONTACTS

DEFENSE CRIMINAL INVESTIGATIVE SERVICE (DCIS)

- In what situations should companies/organizations contact DCIS?

  DCIS should be contacted if you uncover counterfeits or cases of product substitution related to any Department of Defense contract.

- What information should companies/organizations provide DCIS?

  Any information that can be provided. This includes, but is not limited to, part numbers, end-use of the part, testing records, supplier name, type of defect, etc.

- What should companies/organizations do with suspected/confirmed counterfeit parts?

  Keep the parts to aid in the investigation. Do not dispose of the parts or return them to their original supplier.

- Can companies/organizations who contact DCIS about counterfeits share information with industry groups or databases?

  Yes. DCIS and other law enforcement organizations monitor the Government-Industry Data Exchange Program (GIDEP) and Joint Deficiency Reporting System (JDRS) databases for information concerning counterfeits.

- How should companies/organizations get in contact with DCIS concerning counterfeit electronics?

  Contact the DCIS Hotline at:
  Phone: (800) 424-9098
  E-mail: hotline@dodig.mil
  Website: http://www.dodig.mil/hotline
  Address: Defense Criminal Investigative Service
  400 Army Navy Drive, Room 901E
  Arlington, VA 22202
  Phone: (703) 604-8600

FEDERAL AVIATION ADMINISTRATION (FAA)

- In what situations should companies/organizations contact the FAA?

  The FAA should be contacted if you uncover parts, components, or materials related to commercial aeronautical and aviation systems that are suspected of not meeting FAA approved part requirements, including counterfeits. FAA Advisory 21-29C, "Detecting and Reporting Suspected Unapproved Parts," contains information and guidance for detecting and reporting suspected unapproved parts.

- What information should companies/organizations provide the FAA?

  Companies/organizations should provide the information requested in FAA Form 8120-11, the Suspected Unapproved Parts Report.

- What should companies/organizations do with suspected/confirmed counterfeit parts?

  Keep the parts to aid in the investigation. Do not dispose of the parts or return them to their original supplier.

- How should companies/organizations get in contact with DCIS concerning counterfeit electronics?

  Companies/organizations can submit FAA Form 8120-11, the Suspected Unapproved Parts Report, through the following methods:

  - The 24-hour Aviation Safety Hotline: 1-800-255-1111
  - The Aviation Safety Hotline office: 9-awa-avs-aai-safetyhotline@faa.gov
  - Mail a hard copy:

    Federal Aviation Administration
    Aviation Safety Hotline Office
    AAI-3, Room 840
    800 Independence Avenue, SW
    Washington, DC 20591

FEDERAL BUREAU OF INVESTIGATION (FBI)

- In what situations should companies contact the FBI?

  The FBI should be contacted if you uncover counterfeits or cases of product substitution related to commercial products or systems.

- What information should companies provide the FBI?

  As much information that can be provided, including but not limited to:

  - Name and contact information of complainant
  - Name, address, and phone number of suspected supplier company
  - Information on how long the suspected supplier company has been in business
  - Type of part and destination of the part
  - Number of parts purchased
  - Name of expert witness to determine product authenticity
  - What is wrong with the part and the consequences of the part being used
  - Copies of all paperwork associated with the part
  - Whether a complaint has been submitted to any databases or other law enforcement agencies, and contact information for those agencies

- What should companies do with suspected/confirmed counterfeit parts?

  Keep the parts to aid in the investigation, along with all associated paperwork. Do not dispose of the parts or return them to their original supplier.

- How should companies get in contact with the FBI concerning counterfeit electronics?

  Companies should contact their local FBI office, which can be found at http://www.fbi.gov/contact/fo/fo.htm. Additionally, companies can use the following methods to report counterfeit electronics:

  - FBI Tips and Public Leads: https://tips.fbi.gov/
  - Cyber Crime Fraud Unit: cyber_crime_fraud_unit@ic.fbi.gov

NATIONAL INTELLECTUAL PROPERTY RIGHTS COORDINATION CENTER (IPR CENTER)

- What information should companies/organizations provide the IPR Center?

  As much information that can be provided about the complainant, the violator, and the violation. If using the online reporting form, fill in as many fields as possible.

- What should companies/organizations do with suspected/confirmed counterfeit parts?

  Keep the parts. Do not dispose of the parts or return them to their original supplier.

- How should companies/organizations get in contact with the IPR Center concerning counterfeit electronics?

  Contact the IPR Center at:
  Phone: (866) IPR-2060
  E-mail: IPRCenter@dhs.gov
  Online Reporting: http://www.ice.gov/partners/cornerstone/ipr/IPRForm.htm
  Address: The National Intellectual Property Rights Coordination Center
  2451 Crystal Drive, Suite 200
  Arlington, VA 22202