

Are you prepared for H.R.1540: National Defense Authorization Act for Fiscal Year 2012 (Sec. 818. Detection and Avoidance of Counterfeit Electronic Parts)?

Phil Zulueta
Consultant
Chairman, SAE International G-19
Counterfeit Electronic Components Committee
Telephone: 661-400-4294
Email: phillipzulueta@gmail.com

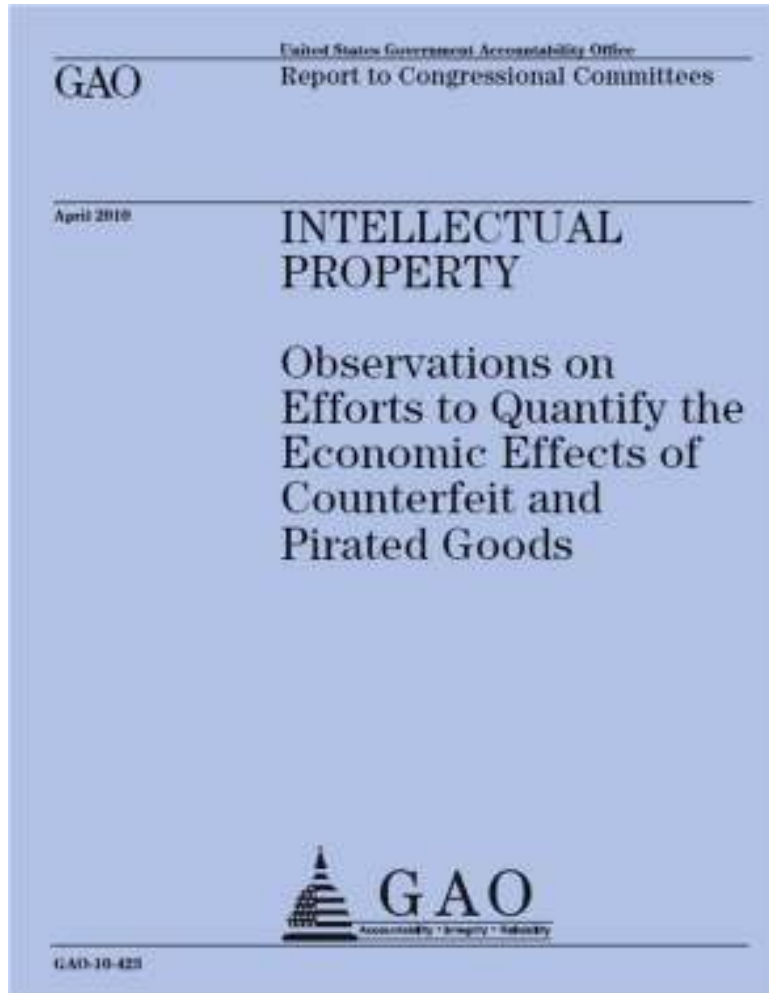
Why Are We Here?

- Review of H.R.1540: National Defense Authorization Act for Fiscal Year 2012 (Sec. 818. Detection and Avoidance of Counterfeit Electronic Parts) as it relates to Contractors and Subcontractors
- Discuss where we are
- Discuss concerns, issues and possible solutions

Participant Questions/Comments

What is the actual concern about Counterfeit Parts? copy rights? performance or operation, the preservation of life, or safety of operating personnel? what is the real intent?

GAO 10-423 Report – April 2010



- Counterfeiting and piracy have produced a wide range of effects on consumers, industry, government, and the economy as a whole
- Certain types of counterfeit goods can have harmful effects on consumers' health and safety, causing serious illness or death
 - pharmaceuticals, automotive parts, electrical components, toys, and household goods
- U.S. industry may include:
 - lost sales
 - lost brand value
 - reduced incentives to innovate
 - U.S. government may lose tax revenue
 - incur IP enforcement expenses
 - face risks of counterfeits entering supply chains with national security or civilian safety implications
 - U.S. economy as a whole may grow more slowly because of reduced innovation and loss of trade revenue

DOC BIS OTE Assessment – January 2010



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://www.bis.doc.gov/defenseindustrialbaseprograms/index.htm>



DOC BIS OTE Assessment – January 2010

Focus on Defense Industrial Base:

- June 2007 - 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,
 - provide an understanding of industry and government practices that contribute to the problem, and
 - identify best practices and recommendations for handling and preventing counterfeit electronics



DOC BIS OTE Assessment – January 2010

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.



DOC BIS OTE Assessment – January 2010

Recommendations for U.S. defense and industrial supply chains:

- 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;



DOC BIS OTE Assessment – January 2010

Recommendations for U.S. defense and industrial supply chains:

- 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.



DOC BIS OTE Assessment – January 2010

Recommendations for US Government:

- 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;



DOC BIS OTE Assessment – January 2010

Recommendations for US Government:

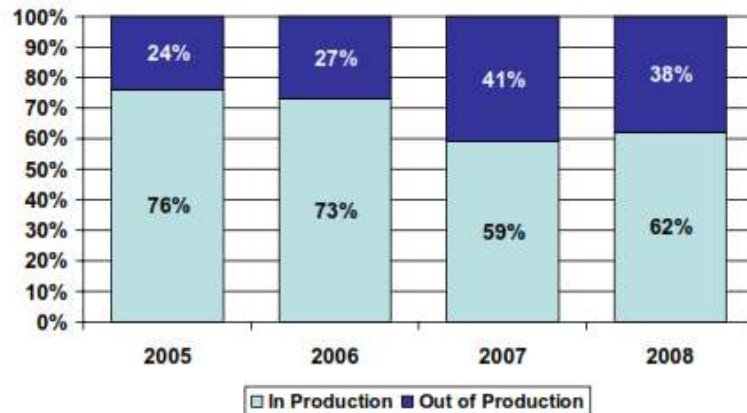
- establish a dialogue with law enforcement agencies on the potential need to increase prosecution of counterfeiters and those entities knowingly distributing counterfeit electronic parts;
- consider establishing a government data repository of electronic parts information and for disseminating best 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.

Participant Questions/Comments

Do you think older components or ones which are more prolific are more susceptible to counterfeit?

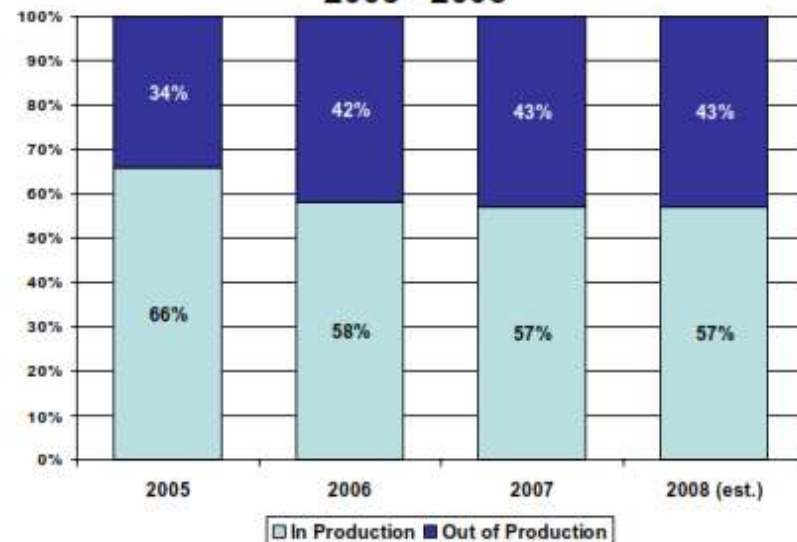
Counterfeit Incidents - In/Out of Production Parts

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.

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.

Participant Questions/Comments

Are there any good design for avoidance practices which can be shared?

GAO-10-389 Report – March 2010

GAO

United States Government Accountability Office
Report to Congressional Requesters

March 2010

DEFENSE SUPPLIER BASE

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



GAO
Accountability • Integrity • Reliability

GAO-10-389

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

Why GAO Did This Study

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

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

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

What GAO Recommends

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

View GAO-10-389 or key components. For more information, contact Silvia Martin at (202) 512-4806 or smartin@gao.gov.

March 2010

DEFENSE SUPPLIER BASE

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

What GAO Found

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

Examples of Counterfeit Parts in DOD's Supply Chain

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

Source: DOD.

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

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

United States Government Accountability Office



GAO-10-389 Report – March 2010

General Findings:

- DOD does not have a common definition for counterfeit parts
- DOD databases do not capture data on counterfeit parts
- Counterfeit parts have been found in DOD's supply chain
- DOD is in the early stages of gathering information on the counterfeit parts problem
- DOD relies on existing procurement and quality control practices that are not specifically designed to address counterfeit parts
- Some DOD components and contractors have taken initial steps to address counterfeit parts
- Companies have developed anti-counterfeiting practices to address vulnerabilities to counterfeit parts
- Industry associations identify and share anti-counterfeiting practices (references AS5553)



GAO-10-389 Report – March 2010

Conclusions:

- As DOD draws from a large network of suppliers in an increasingly global supply chain, there can be limited visibility into these sources and greater risk of procuring counterfeit parts, which have the potential to threaten the reliability of DOD's weapon systems and the success of its missions
- DOD needs a department-wide definition and consistently used means for detecting, reporting, and disposing of counterfeit parts
- Collaboration with government agencies, industry associations, and commercial-sector companies that produce items similar to those used by DOD and have reported taking actions to mitigate the risks of counterfeit parts in their supply chains offers DOD the opportunity to leverage ongoing and planned initiatives in this area
- Some of these initiatives, such as MDA practices and industry detection and disposal processes, can be considered for DOD's immediate use. However, as DOD collects data and acquires knowledge about the nature and extent of counterfeit parts in its supply chain, additional actions may be needed to help better focus its risk mitigation strategies.



GAO-10-389 Report – March 2010

Recommendations for Executive DOD Action:

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

Participant Questions/Comments

Who are the industry leaders or role models in setting up effective programs?

Participant Questions/Comments

Are there government agencies or other resources which might be leveraged or watched for new learning's?

MDA issues SBIR/STTR RFP for Component Authentication Marking



DoD SBIR / STTR DETAILS - Topics Search Results

Proposals Accepted: May 24, 2012 - June 27, 2012

Program: SBIR

Topic Number: MDA12-026 (MDA)

Title: Marking of Components for Avoidance of Counterfeit Parts

Research & Technical Areas: Air Platform, Chemical/Bio Defense, Ground/Sea Vehicles, Sensors, Electronics, Battlespace, Space Platforms, Human Systems, Weapons, Nuclear Technology

Topic Author: Tom Davidson, Phone: 256-450-4264, Email: tom.davidson@mda.mil
Barry Birdsong, Phone: 256-450-4265, Email: barry.birdsong@mda.mil

Acquisition Program:

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), which controls the export and import of defense-related material and services. Offerors must disclose any proposed use of foreign nationals, their country of origin, and what tasks each would accomplish in the statement of work in accordance with section 3.5.b.(7) of the solicitation.

Objective: Develop and demonstrate capability for guaranteeing authenticity of critical electronic components in MDA hardware. Ensure that physical marking techniques are sufficiently robust to withstand handling through supply chain intermediaries and program installation and maintenance processes. Demonstrate confidence in the marking process as a viable, affordable, reliable method of increasing confidence in the authenticity of DoD and MDA electronic components.

Description: MDA uses thousands of different electronic components in their mission and safety critical hardware. This includes systems such as missile

Partial List of Problems

- Counterfeit electronic parts are found in U.S. defense systems and pose a risk to our national security, the reliability of our defense systems, and the safety of our military men and women
- Numerous instances have been identified in which defense contractors installed counterfeit or suspect counterfeit parts on systems or subsystems manufactured for the U.S. military and those contractors have and not provided timely notification to the government
- The defense industry has no influence on market supply and is critically reliant on technology that is made in unsecure locations and obsoletes itself every 1-2 years
- It is impossible to predict how or when these parts or systems will fail
- Supply chain integrity of heritage parts, although necessary, is illusive due to the global nature of the electronic parts supply chain



H. R. 1540

One Hundred Twelfth Congress
of the
United States of America

AT THE FIRST SESSION

*Begun and held at the City of Washington on Wednesday,
the fifth day of January, two thousand and eleven*

An Act

To authorize appropriations for fiscal year 2012 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

*Be it enacted by the Senate and House of Representatives of
the United States of America in Congress assembled,*

SECTION 1. SHORT TITLE.

This Act may be cited as the "National Defense Authorization Act for Fiscal Year 2012".

NDAA 2012 Sec. 818. Detection and Avoidance of Counterfeit Electronic Parts

- a) Assessment of Department of Defense Policies and Systems**
- b) Actions Following Assessment**
- c) Regulations**
 - 1) In General**
 - 2) Contractor Responsibilities**
 - 3) Trusted Suppliers**
 - 4) Reporting Requirements**
 - 5) Construction of Compliance with Reporting Requirement**
- d) Inspection Program**
- e) Improvement of Contractor Systems for Detection and Avoidance of Counterfeit Electronic Parts**
 - 1) In General**
 - 2) Elements**
- f) Definitions**
 - 1) Covered Contractor**
 - 2) Electronic Part**
- g) Information Sharing**
 - 1) In General**
 - 2) Sunset**
 - 3) Lanhan Act Defined**
- h) Trafficking in Inherently Dangerous Good or Services**

Participant Questions/Comments

Per the NDAA Sec 818, is the only concern electronic components and assemblies? how does this apply to materials, chemicals and mechanical parts? or is it not applicable?

OMB - Office of the U.S. Intellectual Property Enforcement Coordinator (IPEC)

2011 Implementation of Enforcement Strategy Action Item - Establish U.S. Government-Wide Working Group to Prevent U.S. Government Purchase of Counterfeit Products

- IPEC convened an interagency group consisting of subject matter experts to develop an anti-counterfeiting framework
- Leadership Roles: OFPP, DOD, DOJ, and NASA
- Other members include: DOC, DOE, HHS, DHS, DOT, EPA, MDA, GSA, SBA, NRC, and NRO
- Main focus is to ensure that the U S Government has the necessary tools to ensure that it does not purchase or use counterfeit products
- They developed six objectives to focus the group's efforts to identify legislative, regulatory, or policy, gaps and propose solutions to fill those gaps:
 - Counterfeit Risk Assessment
 - Supplier Requirements
 - Traceability
 - Testing and Evaluation of Goods
 - Counterfeit Training and Outreach
 - Enforcement Remedies



Memorandum from Acting USD/AT&L Overarching Anti Counterfeit Guidance

- Addresses an area of critical concern while DoDI is in coordination
- Provides definition
- Emphasizes
 - Risk-based approach
 - Directs use of existing contracting clauses and data elements to ensure traceability and reporting on critical items for contractors and subcontractors
 - Use of anti-counterfeiting standards
 - Disposal of counterfeit items
 - Training



The Honorable Frank Kendall
Acting Under Secretary of
Defense for AT&L

Issued March 16, 2012

Kendall Memo

While the Department is concerned about counterfeits in all supply classes, particular focus is required for mission critical components, critical safety items, electronic parts, and load-bearing mechanical parts. DoD Components should immediately take action to decrease the probability of counterfeit items across the Department to include the following:

1. Ensure program managers are notified by their suppliers and contractors when critical items are not obtained from the original equipment manufacturer, original component manufacturer, or an authorized distributor, particularly where electronic parts are included. This requirement should apply to suppliers below the prime contract as well.
2. Require program managers to follow the Program Protection Plan Outline and Guidance (Reference (a)), which includes the requirement to evaluate counterfeit risk and implement countermeasures for mission critical components.
3. For other than mission-critical components, where the program or item manager has determined there is counterfeit risk that warrants action, the program manager or item manager must document risk mitigation within the program risk management plan or systems engineering plan.

DOD Internal Actions



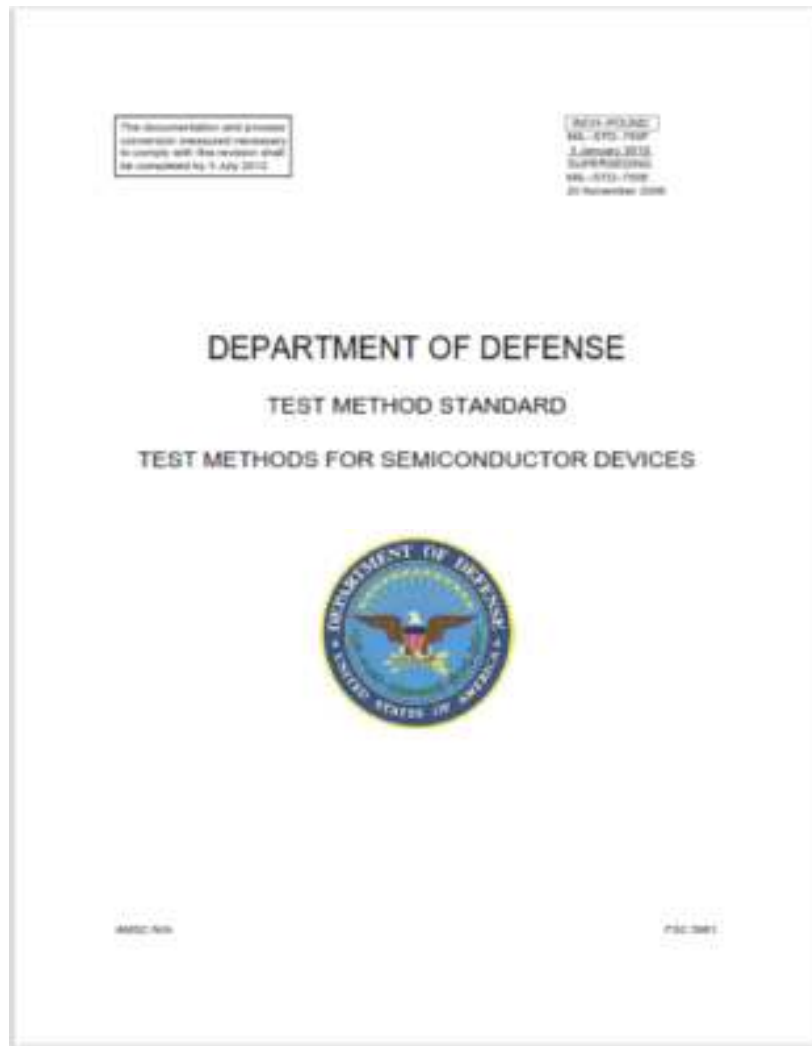
101-11.6	Assessment of Department of Defense Policies and Systems
101-11.6-1	Assessing Following Requirements
101-11.6-2	Regulations
101-11.6-2-1	In General
101-11.6-2-2	Contractor Responsibility
101-11.6-2-3	Trusted Suppliers
101-11.6-2-4	Reporting Requirements
101-11.6-2-5	Conducting of Compliance with Reporting Requirement
101-11.6-3	Inspection Program
101-11.6-3-1	Improvement of Contract System for Detection and Avoidance of Counterfeit Electronic Parts
101-11.6-3-2	In General
101-11.6-3-3	Elements
101-11.6-4	Definitions
101-11.6-4-1	Covered Contract
101-11.6-4-2	Electronic Part
101-11.6-5	Information Sharing
101-11.6-5-1	In General
101-11.6-5-2	Source
101-11.6-5-3	Learn from Failure
101-11.6-6	Staffing in Inherently Dangerous Good or Service

- a) Conduct an assessment of Department of Defense acquisition policies and systems for the detection and avoidance of counterfeit electronic parts
- b) After the assessment and not later than 180 days after the date of the enactment of the Act,:
 - (1) Define “counterfeit electronic part” and “suspect counterfeit electronic part”, which definitions shall include previously used parts represented as new;

Participant Questions/Comments

Is there a definitive definition for what is classified as counterfeit versus parts which do not meet specification? Can anyone make the call? How does one get calibrated for “borderline cases”? I see some confusion already.

MIL-STD-750 Nonconforming Parts



4.9 Laboratory suitability. Prior to processing any semiconductor devices intended for use in any military system or sub-system, the facility performing the test(s) shall be audited by the DLA Land and Maritime, Sourcing and Qualification Division and be granted written laboratory suitability status for each test method to be employed. Processing of any devices by any facility without laboratory suitability status for the test methods used shall render the processed devices **nonconforming**.

SAE G-19 Terms and Definitions

Part(s) - One or more pieces joined together, which are not normally subject to disassembly without destruction or impairment of intended design use. For the purposes in this document, “part” is synonymous with “component”.

Suspect Part - A part in which there is an indication that it may have been misrepresented by the supplier or manufacturer and may meet the definition of fraudulent part or counterfeit part provided below.

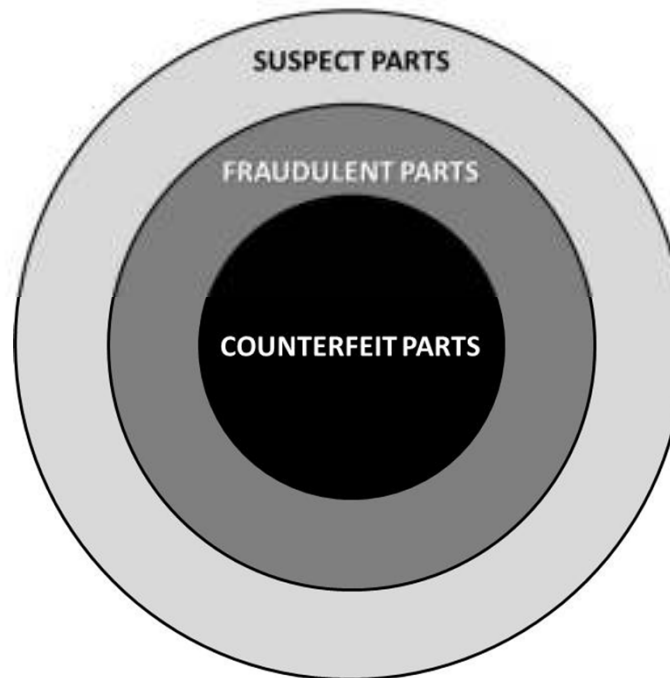
Fraudulent Part - Any suspect part misrepresented to the Customer as meeting the Customer’s requirements.

Counterfeit Part - A fraudulent part that has been confirmed to be a copy, imitation, or substitute that has been represented, identified, or marked as genuine, and/or altered by a source without legal right with intent to mislead, deceive, or defraud.

SAE G-19 Terms and Definitions

NOTE: The following diagram (Figure 1) depicts the above interrelationship between Suspect, Fraudulent and Counterfeit Parts. A Suspect Part may be determined to be, fraudulent or counterfeit through further evaluation and testing. All counterfeit parts are fraudulent, but not all fraudulent parts are counterfeit.

FIGURE 1. INTERRELATIONSHIP BETWEEN SUSPECT, FRAUDULENT AND COUNTERFEIT PARTS





THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

MAR 16 2012

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Overarching DoD Counterfeit Prevention Guidance

References: (a) PDUSD(AT&L) Memorandum, "Document Streamlining - Program Protection Plan (PPP)," July 18, 2011
(b) Defense Federal Acquisition Regulations Supplement, clause 252.246-7003, Notification of Potential Safety Issues, current edition

Counterfeit items are a serious threat to the safety and operational effectiveness of Department of Defense (DoD) systems. The Department is developing, with the participation of your staffs, policy and strategies designed to detect and prevent the introduction of counterfeit materiel. The policy and strategies will focus on those items that affect system performance or operation, the preservation of life, or safety of operating personnel. While we establish new DoD policy and procedures along with appropriate changes to the Defense Federal Acquisition Regulation Supplement (DFARS), this memorandum provides a broad framework and emphasizes the importance of taking action now to apply existing policy and procedures. This memorandum directs specific actions to prevent, detect, remediate, and investigate counterfeiting in the DoD supply chain. For purposes of this memorandum, counterfeit materiel is defined as "an item that is an unauthorized copy or substitute that has been identified, marked, and/or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source." Additionally, a used item represented as a new item may also be subject to fraudulent representation procedures.

DOD Internal Actions



43	Assessment of Department of Defense Policy and Systems
44	Actions Following Assessment
45	Regulations
46	1.1 In General
47	1.2 Contractor Responsibilities
48	1.3 Trusted Suppliers
49	1.4 Reporting Requirements
50	1.5 Coordination of Compliance with Reporting Requirement
51	Inspection Program
52	1.1 Improvement of Contractor Systems for Detection and Avoidance of Counterfeit Electronic Parts
53	1.2 In General
54	1.3 Elements
55	1.4 Definitions
56	1.5 Covered Contractor
57	1.6 Elements Risk
58	Information Sharing
59	1.1 In General
60	1.2 General
61	1.3 Lateral Risk Transfer
62	1.4 Trafficking in Inherently Dangerous Good or Services

(2) issue or revise guidance applicable to Department components engaged in the purchase of electronic parts to implement a risk-based approach to minimize the impact of counterfeit electronic parts or suspect counterfeit electronic parts on the Department, which guidance shall address requirements for training personnel, making sourcing decisions, ensuring traceability of parts, inspecting and testing parts, reporting and quarantining counterfeit electronic parts and suspect counterfeit electronic parts, and taking corrective actions (including actions to recover costs as described in subsection (c)(2));

Risk-based Approach

- The contractor has the ability to balance cost against the level of processing applied to mitigate counterfeit electronic parts
- A risk-based approach can imply that counterfeit “escapes” will occur
- There may be times when the contractor cannot obtain specific parts from the OCM or their franchised/authorized distributors and is forced to source the parts from the open market. These parts will likely not have any trace documentation to the OCM. Under this scenario, for example, the level of product verification testing that the contractor specifies under a risk-based approach to minimize counterfeits, will have a direct function on the assurance of receiving legitimate parts

Participant Questions/Comments

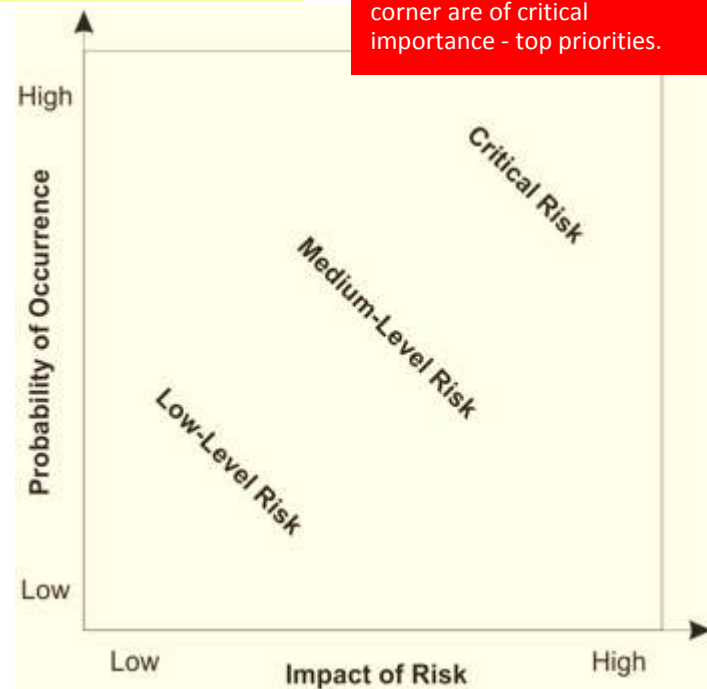
How do you accurately gage risk?

Risk Impact/Probability Chart

- Evaluating every risk in all but the most critical environments can be too expensive, both in time and resources. Instead, prioritize risks and focus on the most important risks.
- **Probability** – A risk is an event that "may" occur. The probability of it occurring can range anywhere from above 0 percent to below 100 percent.
- **Impact** – A risk always has a negative impact. Size of the impact varies in terms of cost and impact on health, human life, or some other critical factor.
- The Risk Impact/Probability Chart allows you to rate potential risks on these two dimensions and gives a quick, clear view of the priority to then decide what resources to allocate to manage that particular risk.

Low impact/high probability –
Risks in the top left corner are of moderate importance – cope with them, try to reduce their likelihood and move on.

High impact/high probability –
Risks towards the top right corner are of critical importance - top priorities.



Low impact/low probability –
Risks in the bottom left corner are low level - ignore them.

High impact/low probability –
Risks in the bottom right corner are of high importance but very unlikely to happen - do what you can to reduce the impact and have contingency plans in place.

How to Use the Tool

- List all of the likely risks that your project faces. Make the list as comprehensive as possible.
 - Assess the probability of each risk occurring, and assign it a rating. For example, you could use a scale of 1 to 10. Assign a score of 1 when a risk is extremely unlikely to occur, and use a score of 10 when the risk is extremely likely to occur.
 - Estimate the impact on the project if the risk occurs for each risk on your list. Using your 1-10 scale, assign it a 1 for little impact and a 10 for a huge, catastrophic impact.
 - Map out the ratings on the Risk Impact/Probability Chart.
 - Develop a response to each risk, according to its position in the chart.
- Risk Severity Index = Probability x Highest Impact

	10	20	30	40	50	60	70	80	90	100
	9	18	27	36	45	54	63	72	81	90
	8	16	24	32	40	48	56	64	72	80
	7	14	21	28	35	42	49	56	63	70
	6	12	18	24	30	36	42	48	54	60
	5	10	15	20	25	30	35	40	45	50
	4	8	12	16	20	24	28	32	36	40
	3	6	9	12	15	18	21	24	27	30
	2	4	6	8	10	12	14	16	18	20
	1	2	3	4	5	6	7	8	9	10
Probability										
	Highest Impact of the Risk Event									


DOD Internal Actions

43	Assessment of Department of Defense Policy and Systems
44	Actions Following Assessment
45	Regulations
46	1.1 In General
47	1.2 Contractor Responsibility
48	1.3 Trusted Suppliers
49	1.4 Reporting Requirements
50	1.5 Consideration of Compliance with Reporting Requirement
51	Inspection Program
52	Improvement of Contractor Systems for Detection and Avoidance of Counterfeit Electronic Parts
53	1.1 In General
54	1.2 Elements
55	Deficiencies
56	1.1 Covered Contractor
57	1.2 Elements
58	Information Sharing
59	1.1 In General
60	1.2 Elements
61	1.3 Lateral and Indirect
62	1.4 Trafficking in Inherently Dangerous Goods or Services

(3) issue or revise guidance applicable to the Department on remedial actions to be taken in the case of a supplier who has repeatedly failed to detect and avoid counterfeit electronic parts or otherwise failed to exercise due diligence in the detection and avoidance of such parts, including consideration of whether to suspend or debar a supplier until such time as the supplier has effectively addressed the issues that led to such failures;

Excluded Parties List System (EPLS)

<http://www.gsa.gov/portal/content/101991>

 **U.S. General Services Administration**

Search This Site

[WHAT GSA OFFERS](#) [DOING BUSINESS WITH GSA](#) [LEARN MORE](#) [BLOG](#)


[Home](#) > [Policy & Regulations](#) > [Acquisition Policy](#) > [Integrated Acquisition Environment \(IAE\)](#) > [Excluded Parties List System \(EPLS\)](#)

Acquisition Policy

- Overview
- Acquisition Policy Library
- Acquisition Regulations
- CAO's Corner
- Center for Acquisition Excellence
- Contracting Requirements
- FAR Staff by Assignment
- Integrated Acquisition Environment (IAE)
- Catalog of Federal Domestic Assistance
- ▶ **Excluded Parties List System (EPLS)**
- casu.gov

Excluded Parties List System (EPLS)

EPLS is an electronic, web based system that identifies those parties excluded from receiving federal contracts, certain subcontracts, and certain types of federal financial and non-financial assistance and benefits. The EPLS keeps the user community aware of administrative and statutory exclusions across the entire government, suspected terrorists, and individuals barred from entering the United States. Users are able to search, view, and download both current and archived exclusions.

CONTACTS

Priscilla Owens
(703) 605-3408

- priscilla.owens@gsa.gov
- [View Contact Details](#)

Last Reviewed 03/13/2012

Excluded Parties List System (EPLS)

<https://www.epls.gov/>

EPLS
Excluded Parties List System

Search - Current Exclusions

- Advanced Search
- Multiple Names
- Exact Name and SSN/ID
- MyEPLS
- Recent Updates
- Browse All Records

View Cause and Treatment Code Descriptions

- Reciprocal Codes
- Procurement Codes
- Nonprocurement Codes

Agency & Acronym Information

- Agency Contacts
- Agency Descriptions
- State/Country Code Descriptions

OFFICIAL GOVERNMENT USE ONLY

- System Maintenance
- Administration
- Upload Logs

Important Notice - System for Award Management (SAM)

SAM
SYSTEM FOR AWARD MANAGEMENT

EPLS and other systems will be migrating to the System for Award Management (SAM) on May 29, 2012. If you are a current registrant, this is what to expect. If you use EPLS data in one of your systems today, please visit SAM.gov for additional information.

Introduction

This World Wide Web site is provided as a public service by General Services Administration (GSA) for the purpose of efficiently and conveniently disseminating information on parties that are excluded from receiving Federal contracts, certain subcontracts, and certain Federal financial and nonfinancial assistance and benefits, pursuant to the provisions of 31 U.S.C. 6101, note, E.O. 12549, E.O. 12689, 48 CFR 9.404, and each agency's codification of the Common Rule for Nonprocurement suspension and debarment.

Security Notice

This system and related software and equipment are intended solely for the communication, transmission, processing, and storage of U.S. Government information. For site security purposes and to ensure that this Web site remains available to all users, GSA monitors network traffic to identify unauthorized attempts to upload or change information or to otherwise cause damage to the site. **Anyone using this Web site expressly consents to such monitoring.**

Resources

- Search Help
- Advanced Search Tips
- Public User's Manual
- FAQ
- Acronyms
- Privacy Act Provisions
- News
- System for Award Management (SAM)

Reports

- Advanced Reports
- Recent Updates
- Dashboard

Archive Search - Past Exclusions

- Advanced Archive Search
- Multiple Names
- Recent Updates
- Browse All Records

Contact Information

- For Help: Federal Service Desk

DOD Internal Actions

43	Assessment of Department of Defense Policy and Systems
44	Adopting Following Resolutions
45	Regulations
46	1.1 In General
47	1.2 Contractor Responsibility
48	1.3 Trusted Suppliers
49	1.4 Reporting Requirements
50	1.5 Consequence of Compliance with Reporting Requirement
51	Inspection Program
52	1.1 Improvement of Contractor Systems for Detection and Avoidance of Counterfeit Electronic Parts
53	1.2 In General
54	1.3 Elements
55	1.4 Definitions
56	1.5 Covered Contractor
57	1.6 Elements of Risk
58	Information Sharing
59	1.1 In General
60	1.2 General
61	1.3 Lateral Risk Transfer
62	1.4 Trafficking in Inherently Dangerous Goods or Services

(4) establish processes for ensuring that Department personnel who become aware of, or have reason to suspect, that any end item, component, part, or material contained in supplies purchased by or for the Department contains counterfeit electronic parts or suspect counterfeit electronic parts provide a report in writing within 60 days to appropriate Government authorities and to the Government-Industry Data Exchange Program (or a similar program designated by the Secretary); and

(5) establish a process for analyzing, assessing, and acting on reports of counterfeit electronic parts and suspect counterfeit electronic parts that are submitted in accordance with the processes under paragraph (4).

DOD Internal Actions

- 4) Assessment of Requirements of Defense Policies and Systems
- 5) Actions Following Assessment
- 6) Regulations
 - (1) In General
 - (2) Contract Responsibility
 - (3) Trusted Suppliers
 - (4) Reporting Requirements
 - (5) Coordination of Compliance with Reporting Requirement
- 7) Inspection Program
- 8) Improvement of Contract Systems for Detection and Avoidance of Counterfeit Electronic Parts
 - (1) In General
 - (2) Elements
- 9) Challenges
 - (1) Covered Entities
 - (2) Covered Parts
- 10) Information Sharing
 - (1) In General
 - (2) Sources
 - (3) Lateral due Diligence
- 11) Trafficking in Inherently Dangerous Good or Services

c) Regulations

- 1) Not later than 270 days after the date of the enactment of this Act, the Secretary shall revise the Department of Defense Supplement to the Federal Acquisition Regulation (DFARS) to address the detection and avoidance of counterfeit electronic parts

Participant Questions/Comments

What are the expected revision(s) to the FAR?

Kendall Memo

4. Reaffirm the requirement to include DFARS clause 252.246-7003, "Notification of Potential Safety Issues" (Reference (b)) in solicitations and contracts for the acquisition of: (1) repairable or consumable parts identified as critical safety items; (2) systems and subsystems, assemblies, and subassemblies integral to a system; or (3) repair, maintenance, logistics support, or overhaul services for systems and subsystems, assemblies, subassemblies, and parts integral to a system. This clause directs actions to be taken concerning non-conformances and deficiencies that could result in a critical safety impact to parts or to systems or subsystems, assemblies, subassemblies, or parts integral to a system. Follow the procedures at section 246.371 of "Procedures, Guidance, and Information" for the handling of notifications received under the clause.
5. Participate in a Department-level review to identify appropriate industry standards for anti-counterfeiting and address those standards in contracting requirements as appropriate. In addition, ensure that any such requirements flow down to appropriate lower-tier subcontracts.
6. Establish testing and verification requirements for items not received from an original equipment manufacturer, original component manufacturer, or authorized distributor that are identified as having high risk for counterfeit potential. These requirements apply to prime contracts, and to subcontracts or suppliers below the prime contracts.

Participant Questions/Comments

How does this meet all the internal and external requirements of the proposed DFAR?

Contractor Responsibilities

- 41. Assessment of Requirements of Defense Policies and Systems
- 42. Actions Following Assessment
- 43. Regulations
 - 43.1 In General
 - 43.2 Control for Responsibilities
 - 43.3 Trusted Suppliers
 - 43.4 Reporting Requirements
 - 43.5 Coordination of Compliance with Reporting Requirement
- 44. Inspection Program
- 45. Improvement of Contractor Systems for Detection and Avoidance of Counterfeit Electronic Parts
 - 45.1 In General
 - 45.2 Elements
- 46. Challenges
 - 46.1 Covered Contractor
 - 46.2 Government Part
- 47. Information Sharing
 - 47.1 In General
 - 47.2 Scope
 - 47.3 Lessons Learned
- 48. Trafficking in Inherently Dangerous Good or Services

- 2) CONTRACTOR RESPONSIBILITIES.—The revised regulations issued pursuant to paragraph (1) shall provide that—
- (A) covered contractors who supply electronic parts or products that include electronic parts are responsible for detecting and avoiding the use or inclusion of counterfeit electronic parts or suspect counterfeit electronic parts in such products and for any rework or corrective action that may be required to remedy the use or inclusion of such parts; and
- (B) the cost of counterfeit electronic parts and suspect counterfeit electronic parts and the cost of rework or corrective action that may be required to remedy the use or inclusion of such parts are not allowable costs under Department contracts.

Participant Questions/Comments

The responsibility for “escapes” and the cost to the contractor for recall, cost of rework and/or corrective action is open ended.

May 10 2012, Committee Overwhelmingly Passes the FY13 National Defense Authorization Act

- NOTE: HR 4310 as approved by HASC includes amendments to Section 818 of the FY 2012 NDAA...
- Log 100 – This amendment would direct the SecDef to assess risks associated with obsolete or obsolescent electronic parts, and counterfeits thereof, to the defense supply chain and to brief the defense committees on findings and recommendations.
- Log 101 – This amendment would create an exception for DOD contractors who take certain precautions for detecting and avoiding the use of counterfeit electronic parts. The cost of rework or corrective action is unallowable, unless 1) contractor has a counterfeit avoidance/detection system approved by DoD, 2) the counterfeit parts were either procured from a trusted supplier or provided as government property per FAR Part 45, and 3) contractor provides timely notice of finding.

H.R.4310 – National Defense Authorization Act for Fiscal Year 2013

SEC. 816. CONTRACTOR RESPONSIBILITIES IN REGULATIONS RELATING TO DETECTION AND AVOIDANCE OF COUNTERFEIT ELECTRONIC PARTS. *Section 818(c)(2)(B) of the National Defense Authorization Act for Fiscal Year 2012 (Public Law 112–81; 125 Stat. 1493; 10 U.S.C. 2302 note) is amended to read as follows:*

*“(B) the cost of counterfeit electronic parts and suspect counterfeit electronic parts and the cost of rework or corrective action that may be required to remedy the use or inclusion of such parts are not allowable costs under Department contracts, **unless—***

“(i) the covered contractor has an operational system to detect and avoid counterfeit parts and suspect counterfeit electronic parts that has been reviewed and approved by the Department of Defense pursuant to subsection (e)(2)(B);

“(ii) the counterfeit electronic parts or suspect counterfeit electronic parts were— “(I) procured from a trusted supplier in accordance with regulations described in paragraph (3); or “(II) provided to the contractor as Government property in accordance with part 45 of the Federal Acquisition Regulation; and

“(iii) the covered contractor provides timely notice to the Government pursuant to paragraph (4).”.

Participant Questions/Comments

Can the contractor price this in his quotations?
Is he allowed to do so and will any guidelines be
provided to assist in implementing this?

Participant Questions/Comments

What is the remedial responsibility or liability of lower tier suppliers? How many levels down the supply chain will be affected?

Participant Questions/Comments

How do we limit the liability exposure, despite all of our preventative measures?

Participant Questions/Comments

How do we limit the risk of small businesses who do not necessarily have the infrastructure to manage the issue of counterfeit parts and as such, large businesses will bear the burden?

An increasing trend in Contractor (OEM) Contract Clauses?

<SUPPLIER> will indemnify, defend, and hold
<CUSTOMER> harmless from and against any and all
loss or expense incurred by <CUSTOMER> as a result of
the delivery by <SUPPLIER> to or on behalf of
<CUSTOMER> of suspect, fraudulent, or counterfeit
electronic parts or electronic assemblies

Participant Questions/Comments

What is the level of investment needed to implement and sustain an effective detection and avoidance program? In dollars and people

DOD, Contractors, Subcontractors and Trusted Supplier Actions

41	Assessment of Requirements of Defense Policies and Systems
42	Actions Following Assessment
43	Regulations
44	In General
45	Contractor Responsibilities
46	Trusted Suppliers
47	Reporting Requirements
48	Compliance with Reporting Requirement
49	Inspection Program
50	Improvement of Contractor Systems for Selection and Acquisition of Counterfeit Electronic Parts
51	In General
52	Elements
53	Challenges
54	Controlled Environment
55	Overcome Pain
56	Information Sharing
57	In General
58	Success
59	Learn from Failure
60	Refining Inherently Dangerous Good or Services

TRUSTED SUPPLIERS.—The revised regulations issued pursuant to paragraph (1) shall—

(A) require that, whenever possible, the Department and Department contractors and subcontractors at all tiers—

- (i) obtain electronic parts that are in production or currently available in stock from the original manufacturers of the parts or their authorized dealers, or from trusted suppliers who obtain such parts exclusively from the original manufacturers of the parts or their authorized dealers; and
- (ii) obtain electronic parts that are not in production or currently available in stock from trusted suppliers;

(B) establish requirements for notification of the Department, and inspection, testing, and authentication of electronic parts that the Department or a Department contractor or subcontractor obtains from any source other than a source described in subparagraph (A);

DOD, Contractors, Subcontractors and Trusted Supplier Actions

Table of Contents:

- 41 Assessment of Requirements of Defense Policies and Systems
- 42 Actions Following Assessment
- 43 Regulations
 - 43.1 In General
 - 43.2 Contract Responsibilities
 - 43.3 Trusted Suppliers
 - 43.4 Reporting Requirements
 - 43.5 Coordination of Compliance with Reporting Requirement
- 44 Inspection Program
- 45 Improvement of Contractor Systems for Detection and Avoidance of Counterfeit Electronic Parts
 - 45.1 In General
 - 45.2 Elements
- 46 Challenges
 - 46.1 Covered Contractor
 - 46.2 Government Part
- 47 Information Sharing
 - 47.1 In General
 - 47.2 Sources
 - 47.3 Lessons Learned
- 48 Trafficking in Inherently Dangerous Good or Services

(C) establish qualification requirements, consistent with the requirements of section 2319 of title 10, United States Code, pursuant to which the Department may identify trusted suppliers that have appropriate policies and procedures in place to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts; and

(D) authorize Department contractors and subcontractors to identify and use additional trusted suppliers, provided that—

- (i) the standards and processes for identifying such trusted suppliers comply with established industry standards;
- (ii) the contractor or subcontractor assumes responsibility for the authenticity of parts provided by such suppliers as provided in paragraph (2); and
- (iii) the selection of such trusted suppliers is subject to review and audit by appropriate Department officials.

Participant Questions/Comments

What will be the actual definition of “trusted supplier”?

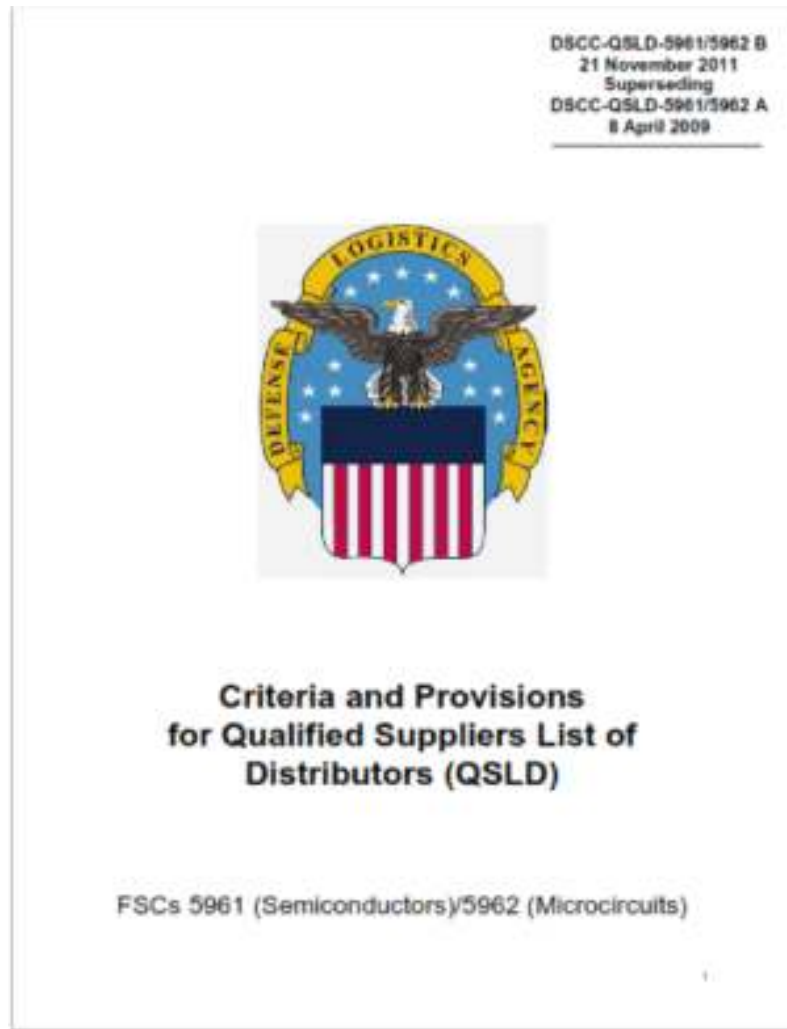
Participant Questions/Comments

What standards will the DoD use to characterize “trusted suppliers”?

Participant Questions/Comments

What are the best practices for establishing internal trusted supplier programs and testing and reporting programs?

QSLD Revision B – 21 November 2011



- QSLD Program Purpose: establish and maintain a list of pre-qualified sources for electronic components purchased and managed by DLA Land and Maritime
- Latest revision does NOT address the counterfeit parts issue

QSLD Revision B – 21 November 2011

Four key elements required of distributors:

- a. The distributor must have evidence of using a documented Quality Management System which meets DLA's criteria;
- b. The distributor must have on hand and maintain evidence that (1) the QPL/QML products supplied were produced by a Manufacturer whom is listed on the QPL or QML; (2) commercial products were produced by the specified original manufacturer (to include information tracing the product back to the specified source); and (3) products procured from another distributor are from a distributor or through a chain of distributors each listed as an approved QSLD supplier. All products pursuant to DLA's contract/purchase order requirements for items in FSCs 5961 and 5962 must be obtained from, or flow through QSLD providers, with an unbroken chain of traceability documentation back to the Manufacturer. This closed loop flow must be supported by the provider's traceability documentation;
- c. The distributor must have and maintain evidence that product is not commingled and lot identity has been maintained; and
- d. The distributor must have and maintain evidence that the quality of the product is not altered by Distributors.

What we know at this time re: OSD efforts

- Early April, an OSD team, headed by an individual from MDA with DLA personnel, proposed development of a draft document ("QSLD-Test") that will outline program requirements for those suppliers that have needed product, but do not have traceability to the manufacturer
- The DLA Criteria and Provisions document will reference AS6081 and JESD31 for program requirements (using QSLD document as core, add from AS6081 and JESD31D, propose it as the government document for meeting the NDAA trusted supplier criteria
- The new proposed program will outline testing and inspection requirements
- QSLD suppliers with full traceability will continue to be the desired source, but if no QSLD supplier bids, then source from QSLD-Test supplier
- Proposal is still being discussed by OSD stakeholders

Status of AS6081 release

- Passed second balloting phase end of April
- Addressing ballot comments and revising draft
- Re-submit for re-ballot (14- or 28-day period)
- If passes, proceed to SAE Aerospace Council ballot (as much as 28 days)
- If passes, then public released
- Overall estimated completion – end of July

Recommendations for Independent Distributors

- Implement a counterfeit parts control plan in accordance with AS5553 (AS6081 when released).
- Assure, through continuous assessment actions, that your approved and ongoing sources of supply are maintaining effective processes for mitigating the risks of supplying counterfeit electronic parts. Assessment actions may include surveys, audits, review of product alerts (e.g. GIDEP, ERAI & IDEA), and review of supplier quality data to determine past performance. Guidance for assessment actions can be obtained from AS5553 (or AS6081 when released).
- Procure electronic parts or electronic assemblies from either the OCM/OEM or the OCM's or OEM's Authorized Distributor with full supply chain traceability to the OCM/OEM.
- If procuring electronic parts or electronic assemblies from other than the OCM/OEM or the OCM's/OEM's Franchised (Authorized) Distributor with supply chain traceability to the OCM or OEM, obtain a completed Risk Assessment for every purchase order line item from the Customer and execute the mitigation requirements per this Risk Assessment or per AS5553 (or AS6081 when released).

Participant Questions/Comments

I would hope we are not creating an alternate or parallel certification process that adds expense and bureaucracy to the procurement process. Are the corresponding controls that are in, need to update for Distribution (AS9120) or is all of this complementary?

Third Party Certification Process

- G-19 management system standards supplement the requirements of a comprehensive quality management system standard (e.g., AS9100, AS9120, ISO 9001, or equivalent) and other applicable quality standards (e.g., ANSI/ESD S20.20, IDEA-STD-1010, or equivalent). They are not intended to stand alone, supersede, or cancel requirements found in other quality standards, requirements imposed by contracting authorities, or applicable laws and regulations unless an authorized exemption/variance has been obtained.
- Client controls the type of audit depending on their management system:
 - Combined audit - when a client is audited against the requirements of two or more management systems standards together
 - Integrated audit - when a client has integrated the application of requirements of two or more management systems standards into a single management system and is being audited against more than one standard

Contractor and Subcontractor Actions

40	Assessment of Department of Defense Policies and Systems
41	Actions Following Assessment
42	Regulations
43	In General
44	Contractor Responsibilities
45	Trusted Suppliers
46	Reporting Requirements
47	Construction of Compliance with Reporting Requirement
48	Inspection Program
49	Implementation of Contractor Systems for Detection and Avoidance of Counterfeit Electronic Parts
50	In General
51	Elements
52	Definitions
53	Covered Contractor
54	Electronic Part
55	Information Sharing
56	In General
57	Exemptions
58	Sanction and Offense
59	Threatening to Incentivize Dangerous Good or Services

(4) REPORTING REQUIREMENT.—The revised regulations issued pursuant to paragraph (1) shall require that any Department contractor or subcontractor who becomes aware, or has reason to suspect, that any end item, component, part, or material contained in supplies purchased by the Department, or purchased by a contractor or subcontractor for delivery to, or on behalf of, the Department, contains counterfeit electronic parts or suspect counterfeit electronic parts report in writing within 60 days to appropriate Government authorities and the Government-Industry Data Exchange Program (or a similar program designated by the Secretary).

(5) CONSTRUCTION OF COMPLIANCE WITH REPORTING REQUIREMENT.—A Department contractor or subcontractor that provides a written report required under this subsection shall not be subject to civil liability on the basis of such reporting, provided the contractor or subcontractor made a reasonable effort to determine that the end item, component, part, or material concerned contained counterfeit electronic parts or suspect counterfeit electronic parts.

Kendall Memo

7. Ensure contractors and subcontractors reports of suspected or confirmed counterfeit items are entered into the Government-Industry Data Exchange Program (GIDEP) system, which will serve as the DoD central reporting repository.
8. Report suspected or confirmed counterfeit items discovered by DoD activities in GIDEP using the Product Quality Deficiency Reporting process as appropriate.
9. Investigate suspected counterfeit incidents discovered or reported, and report incidents confirmed as counterfeit to the appropriate criminal authorities. In the case of suspect counterfeits, the parts should be held until resolution of the potential non-conformance is complete. If items are confirmed to be counterfeit, they should not be returned to the actual or a potential supplier at any time prior to criminal authorities' release for disposition.
10. Develop and provide training to DoD personnel involved with the development, acquisition and procurement, supply, maintenance, and protection of weapon systems on proper measures to address counterfeiting.

Your support in this critical area will ensure the safety and mission performance of our warfighting systems. My point of contact is Mr. Gerry Brown, ODASD(SCI), at 571-372-5259.



Frank Kendall
Acting

Participant Questions/Comments

There are concerns around the US trusted supplier list and international companies not able to access GIDEP.

GIDEP Contact

GOVERNMENT-INDUSTRY DATA EXCHANGE PROGRAM



GIDEP OPERATIONS CENTER

P.O. Box 8000
Corona, CA 92878-8000

RUDY BRILLON

Director

Voice: (951) 898-3303
Fax: (951) 898-3250

Cell: (951) 545-9517
rbrillon@gidep.org

Homeland Security Action

41	Assessment of Requirements of Defense Policies and Systems
42	Actions Following Assessment
43	Regulations
44	In General
45	Contractor Responsibilities
46	Trusted Suppliers
47	Reporting Requirements
48	Compliance of Compliance with Reporting Requirement
49	Inspection Program
50	Improvement of Contractor Systems for Detection and Avoidance of Counterfeit Electronic Parts
51	In General
52	Elements
53	Challenges
54	Covered Contractor
55	Covered Part
56	Information Sharing
57	In General
58	Screen
59	Lenses and ZedBoard
60	Refining Inherently Dangerous Good or Services

(d) INSPECTION PROGRAM.—The Secretary of Homeland Security shall establish and implement a risk-based methodology for the enhanced targeting of electronic parts imported from any country, after consultation with the Secretary of Defense as to sources of counterfeit electronic parts and suspect counterfeit electronic parts in the supply chain for products purchased by the Department of Defense.

DOD (and Supply Chain) Action

43	Assessment of Department of Defense Policies and Systems
54	Actions Following Assessment
40	Regulations
11	In General
21	Contractor Responsibilities
21	Trusted Suppliers
41	Reporting Requirements
41	Conformance of Compliance with Reporting Requirement
45	Inspection Program
41	Improvement of Contracted Systems for Detection and Avoidance of Counterfeit Electronic Parts
11	In General
21	Elements
41	Definitions
11	Covered Contractor
11	Electronic Part
41	Information Sharing
11	In General
21	Source
41	Lawful Use of Board
41	Refueling in Inherently Dangerous Good or Services

(e) IMPROVEMENT OF CONTRACTOR SYSTEMS FOR DETECTION AND AVOIDANCE OF COUNTERFEIT ELECTRONIC PARTS.—

(1) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act, the Secretary of Defense shall implement a program to enhance contractor detection and avoidance of counterfeit electronic parts.

(2) ELEMENTS.—The program implemented pursuant to paragraph (1) shall—

(A) require covered contractors that supply electronic parts or systems that contain electronic parts to establish policies and procedures to eliminate counterfeit electronic parts from the defense supply chain, which policies and procedures shall address—

- (i) the training of personnel;
- (ii) the inspection and testing of electronic parts;
- (iii) processes to abolish counterfeit parts proliferation;
- (iv) mechanisms to enable traceability of parts;
- (v) use of trusted suppliers;

DOD (and Supply Chain) Action

43	Assessment of Department of Defense Policies and Systems
54	Addressing Reporting Requirements
60	Regulations
61	1.1 In General
62	2.1 Contractor Responsibilities
63	3.1 Trusted Suppliers
64	4.1 Reporting Requirements
65	5.1 Coordination of Compliance with Reporting Requirements
66	Inspection Program
67	1.1 Improvement of Contracted Systems for Detection and Avoidance of Counterfeit Electronic Parts
68	2.1 In General
69	3.1 Elements
70	Definitions
71	1.1 Covered Contract
72	2.1 Electronic Part
73	Information Sharing
74	1.1 In General
75	2.1 General
76	3.1 Labeled Kit Board
77	Trafficking in Inherently Dangerous Goods or Services

(vi) the reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts;

(vii) methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit;

(viii) the design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts; and

(ix) the flow down of counterfeit avoidance and detection requirements to subcontractors; and

(B) establish processes for the review and approval of contractor systems for the detection and avoidance of counterfeit electronic parts and suspect counterfeit electronic parts, which processes shall be comparable to the processes established for contractor business systems under section 893 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111–383; 124 Stat. 4311; 10 U.S.C. 2302 note).

Participant Questions/Comments

The big concerns our company has at the moment are around seeking customer approval before any grey market component purchase. We predominately manufacture COTS products, purchasing parts in advance of customer orders and do not pre-allocate them to particular orders. Therefore customer pre-approval of component purchases is not easily managed.

Participant Questions/Comments

Some topics of particular interest are how to address pre-existing inventory and addressing the issue of obsolescence. There will always be risk in the gray market and our military has systems that require support for decades.

Recommendations for Existing or Customer-supplied Inventory

- Confirm traceability to the OCM or their Franchised (Authorized) Distributor with supply chain traceability to the OCM
- Perform product verification testing per accepted industry standards or per contractual Customer specifications
- Perform testing at the component level prior to manufacture. Include electrical test for COTS assemblies at the assembly level with component inspection and verification at the part level

Recommendations for Parts Obsolescence

- For products where the Contractor or OEM Supplier (e.g., COTS Supplier) has design responsibility, implement a Parts Obsolescence Management Program
 - MIL-STD-3018, Department of Defense Standard Practice – Parts Management,
 - Defense Standardization Program Office SD-19 - Parts Management Guide.
 - Defense Standardization Program Office SD-22 - Diminishing Manufacturing Sources and Material Shortages (DMSMS) Guidebook
- Parts Obsolescence Management Program should include:
 - Periodic assessment of Product Bill of Materials (BOMs) to identify any long-lead or parts obsolescence issues that will impact product deliveries
 - Obsolescence mitigation plan to resolve each obsolescence issue, including both product and part life-cycle analyses, package fabrication/material support
 - Re-design (schedule and cost) considerations
 - Customer notification

Definitions

(a)	Assessment of Department of Defense Policies and Systems
(b)	Autonomous Following Assessment
(c)	Regulations
(1)	In General
(2)	Contractor Responsibilities
(3)	Trusted Suppliers
(4)	Reporting Requirements
(5)	Continuation of Compliance with Reporting Requirements
(d)	Inspection Program
(e)	Improvement of Contracted Systems for Detection and Avoidance of Counterside Electronic Parts
(1)	In General
(2)	Elements
(f)	Definitions
(1)	Covered Contractor
(2)	Electronic Part
(g)	Information Sharing
(1)	In General
(2)	Contract
(3)	Contract due Delivery
(h)	Termination in Involuntary Emergency Good or Services

(f) DEFINITIONS.—In subsections (a) through (e) of this section:

(1) The term “covered contractor” has the meaning given that term in section 893(f)(2) of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011.

(2) The term “electronic part” means an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly.

Relevant Terms and Definitions

Covered Contractor - a contractor that is subject to the cost accounting standards under section 26 of the Office of Federal Procurement Policy Act (41 U.S.C. 422).

Covered Contract – a cost-reimbursement contract, incentive-type contract, time-and-materials contract, or labor-hour contract that could be affected if the data produced by a contractor business system has a significant deficiency.

Contractor Business System - an accounting system, estimating system, purchasing system, earned value management system, material management and accounting system, or property management system of a contractor.

Significant Deficiency - in the case of a contractor business system, means a shortcoming in the system that materially affects the ability of officials of the Department of Defense and the contractor to rely upon information produced by the system that is needed for management purposes.

Relevant Terms and Definitions

SAE G-19 Documents

Part(s): One or more pieces joined together, which are not normally subject to disassembly without destruction or impairment of intended design use. For the purposes in this document, “part” is synonymous with “component”.

Electrical, Electronic, and Electromechanical (EEE) Part: Electrical, electronic, and electromechanical parts are components designed and built to perform specific functions, and are not subject to disassembly without destruction or impairment of design use. Examples of electrical parts include resistors, capacitors, inductors, transformers, and connectors. Electronic parts include active devices, such as monolithic microcircuits, hybrid microcircuits, diodes, and transistors. Electromechanical parts are devices that have electrical inputs with mechanical outputs, or mechanical inputs with electrical outputs, or combinations of each. Examples of electromechanical parts are motors, synchros, servos, and some relays.

Information Sharing

(a)	Assessment of Department of Defense Policies and Systems
(b)	Actions Following Assessment
(c)	Regulations
(1)	In General
(2)	Contractor Responsibilities
(3)	Trusted Suppliers
(4)	Security Requirements
(5)	Continuation of Consultation with Reporting Requirement
(d)	Inspection Program
(e)	Improvement of Contracted Systems for Detection and Avoidance of Counterfeit Electronic Parts
(1)	In General
(2)	Elements
(f)	Excluded
(1)	Contract Continuation
(2)	Unexcused Part
(g)	Information Sharing
(1)	In General
(2)	Notice
(3)	Lanham Act Defined
(h)	Tracking in Inherently Dangerous Good or Services

(g) INFORMATION SHARING.—

(1) IN GENERAL.—If United States Customs and Border Protection suspects a product of being imported in violation of section 42 of the Lanham Act, and subject to any applicable bonding requirements, the Secretary of the Treasury may share information appearing on, and unredacted samples of, products and their packaging and labels, or photographs of such products, packaging, and labels, with the rightholders of the trademarks suspected of being copied or simulated for purposes of determining whether the products are prohibited from importation pursuant to such section.

(2) SUNSET.—This subsection shall expire on the date of the enactment of the Customs Facilitation and Trade Enforcement Reauthorization Act of 2012.

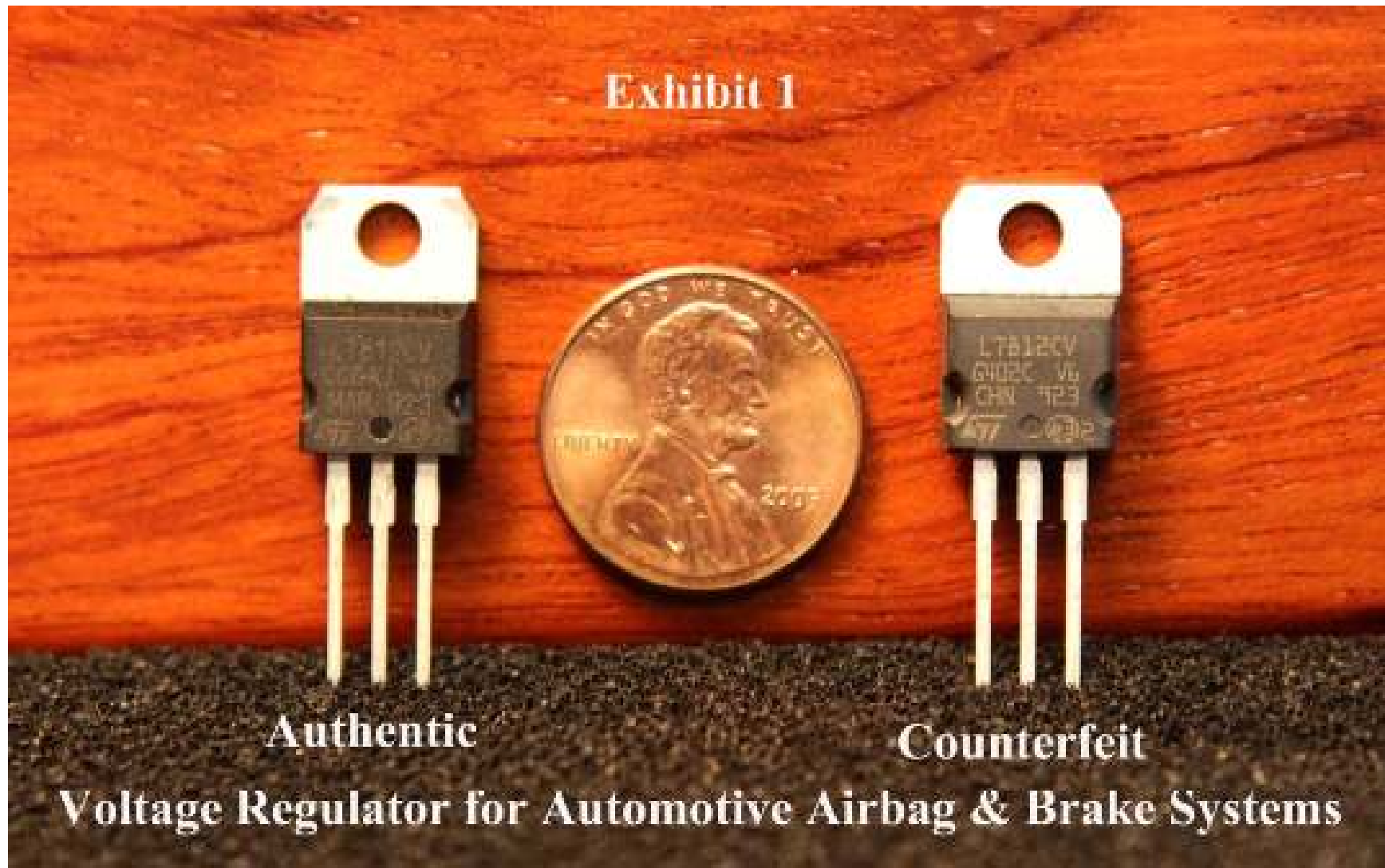
(3) LANHAM ACT DEFINED.—In this subsection, the term “Lanham Act” means the Act entitled “An Act to provide for the registration and protection of trademarks used in commerce, to carry out the provisions of certain international conventions, and for other purposes”, approved July 5, 1946 (commonly referred to as the “Trademark Act of 1946” or the “Lanham Act”).

CBP Identifying Mark Redaction Process

Extracted from Testimony of Brian Toohey, President, SIA July 7, 2011

- Historically, Customs and Border Protection (CBP) facilitated anti-counterfeiting efforts.
- Prior to 2000, when Port Officers suspected a shipment contained counterfeit chips, they would contact the trademark owner and share one of the products.
- After 2000, but before 2008, Port Officers photographed the outside of a suspect chip and sent the publicly viewable information to the chip manufacturer whose trademark appeared on the surface of the chip to determine whether the chip was counterfeit.
- Using a highly confidential database, the trademark owner could then determine very quickly, in almost 85% of the requests, whether or not the chips were counterfeits by analyzing the codes on the surface of the chip.
- In mid-2008, CBP Officers were instructed to redact any identifying marks in the photographs, except the trademark, before sending them to manufacturers, making it impossible for the industry, much less the importer or CBP, to authenticate suspected counterfeit semiconductors.
- U.S. Treasury officials argue that its policy shift is intended to shield Port Officers from criminal liability for the disclosure of confidential information.
- Before August 2008, seizures of counterfeit semiconductors were increasing year after year. Since CBP changed its policy, SIA members have reported receiving an increased number of complaints about counterfeits.

CBP Identifying Mark Redaction Process



Participant Questions/Comments

I would like initiate a discussion on the “Impact of the NDAA section 818 & 2320(attached) to Electronic Manufacturing Service (EMS) Industry” also referred to as the Electronic Contract Manufacturing(ECM) industry. Both terms are used for companies that design, test, manufacture, distribute, and provide return/repair services for electronic components and assemblies for original equipment manufacturers (OEMs)

Below is an outline reflecting the key subject matter :

- A) “ Section 818 Detection and Avoidance of Counterfeit Electronic Parts “
- B) Actual date of Implementation (i.e., 9/1/12) and the following components need to be clearly defined:
 - a. Regulation?
 - b. Contractors Responsibilities(EMS/ECM)?
 - c. Trusted Suppliers who and how defined ?
 - d. Reporting Requirements defined for clarity?
 - e. Compliance Issues ?
 - f. Inspection Program Defined?
 - g. Information Sharing ? ...

Participant Questions/Comments

... continued:

- C) “ Section 2320 Trafficking in counterfeit goods or services”
 - a. Offenses explained via legal representative?
 - b. Penalties explained via legal representative?
- D) DOD Primes flow down requirements or response in attendance?
- E) EMS/ECM Obsolescence defense via waiver requirement from DOD Primes for BOMs containing obsolete components(I.e., GIDEP/DMSMS) ?
- F) DMEA & Trusted Foundry (<http://www.dmea.osd.mil/home.html>) mitigation strategy ?

Recommendations for Contract Manufacturers or Subtier Suppliers

- Implement a counterfeit parts control plan in accordance with AS5553
- Procure electronic parts or electronic assemblies from either the OCM/OEM or the OCM's or OEM's Authorized Distributor with full supply chain traceability to the OCM/OEM
- If procuring electronic parts or electronic assemblies from other than the OCM/OEM or the OCM's/OEM's Franchised (Authorized) Distributor with supply chain traceability to the OCM or OEM, obtain a completed Risk Assessment for every purchase order line item from the Customer and execute the mitigation requirements per the subject Risk Assessment
- For legacy or existing inventory apply rigorous internal quality requirements and controls to assure that conforming product is supplied to Customer

Recommendations for Test Facilities...

that purchase electronic parts or assemblies for Customer upscreen

- Implement a counterfeit parts control plan in accordance with AS5553
- Procure electronic parts or electronic assemblies from either the OCM/OEM or the OCM's or OEM's Authorized Distributor with full supply chain traceability to the OCM/OEM
- If procuring electronic parts or electronic assemblies from other than the OCM/OEM or the OCM's/OEM's Franchised (Authorized) Distributor with supply chain traceability to the OCM or OEM, obtain a completed Risk Assessment for every purchase order line item from the Customer and execute the mitigation requirements per the subject Risk Assessment

Trafficking in Inherently Dangerous Goods or Services

40	Assessment of Department of Defense Policies and Systems
41	Action Following Assessment
42	Regulations
43	43.1 In General
44	43.2 Contracting Responsibilities
45	43.3 Trusted Suppliers
46	43.4 Reporting Requirements
47	43.5 Certification of Compliance with Reporting Requirement
48	Inspection Program
49	49.1 Improvement of Contractor Systems for Detection and Avoidance of Described Electrical Faults
50	49.2 In General
51	49.3 Elements
52	Deficiencies
53	53.1 General Contractor
54	53.2 Electronic Parts
55	Information Sharing
56	56.1 In General
57	56.2 Exports
58	56.3 Export Act Guidance
59	Trafficking in Inherently Dangerous Goods or Services

(h) TRAFFICKING IN INHERENTLY DANGEROUS GOODS OR SERVICES.—Section 2320 of title 18, United States Code, is amended to read as follows:

See Kirsten Koepsel for information
or questions on this section

Participant Questions/Comments

I am interested in the expectation of (how) this whole process will be executed and the flow down requirements within the supply chain.

Participant Questions/Comments

Counterfeit parts is a crucial issue that requires all of us in industry to understand the gravity of the responsibility we have to do all that we can to eliminate the threat to our military and to not make the cost prohibitive to do so.

Participant Questions/Comments

How do we address
“confidence in the supply chain?”

Thank you!

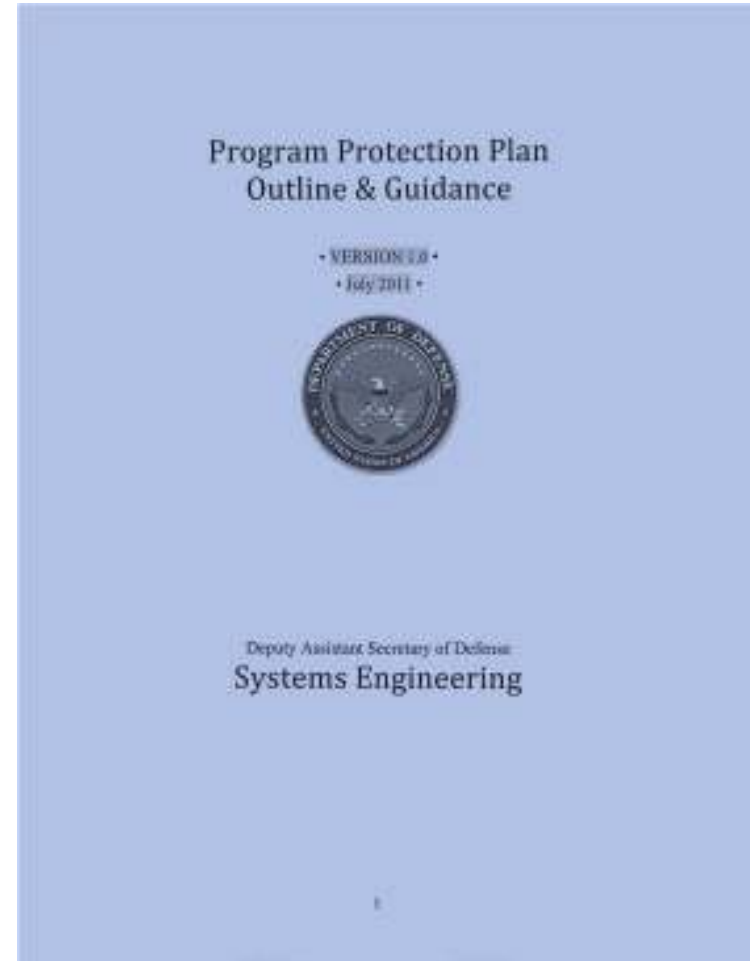
**Are you prepared for H.R.1540: National
Defense Authorization Act for Fiscal Year 2012
(Sec. 818. Detection and Avoidance of
Counterfeit Electronic Parts)?**

**Phil Zulueta
Consultant
Chairman, SAE International G-19
Counterfeit Electronic Components Committee
Telephone: 661-400-4294
Email: phillipzulueta@gmail.com**

Backup Slides

Program Protection Plan Outline & Guidance, July 2011

- Program Protection is the integrating process for managing risks to advanced technology and mission-critical system functionality from foreign collection, design vulnerability or supply chain exploit/insertion, and battlefield loss throughout the acquisition lifecycle.
- The purpose of the PPP is to help programs ensure that they adequately protect their technology, components, and information. This includes information that alone might not be damaging and might be unclassified, but that in combination with other information could allow an adversary to clone, counter, or defeat war fighting capability.



U.S.C. § 2319 : US Code - Section 2319: Encouragement of new competitors

- (a) In this section, the term "qualification requirement" means a requirement for testing or other quality assurance demonstration that must be completed by an offer or before award of a contract.
- (b) ... the head of the agency shall, before establishing a qualification requirement -
 - (1) prepare a written justification stating the necessity for establishing the qualification requirement...;
 - (2) specify in writing and make available to a potential offeror upon request all requirements which a prospective offeror, or its product, must satisfy in order to become qualified ;
 - (3) specify an estimate of the costs of testing and evaluation likely to be incurred by a potential offeror in order to become qualified;
 - (4) ensure that a potential offeror is provided, upon request and on a reimbursable basis, a prompt opportunity to demonstrate its ability to meet the standards specified for qualification...;
 - (5) if testing and evaluation services are provided under contract to the agency for the purposes of clause (4), provide to the extent possible that such services be provided by a contractor...; and
 - (6) ensure that a potential offeror seeking qualification is promptly informed as to whether qualification is attained and, in the event qualification is not attained, is promptly furnished specific information why qualification was not attained.
- (c) (1) Subsection (b) of this section does not apply with respect to a qualification requirement established by statute or administrative action before October 19, 1984, unless such requirement is a qualified products list.

252.246-7003 Notification of Potential Safety Issues

As prescribed in 246.371(a), use the following clause:

NOTIFICATION OF POTENTIAL SAFETY ISSUES (JAN 2007)

(a) *Definitions. As used in this clause—*

“Credible information” means information that, considering its source and the surrounding circumstances, supports a reasonable belief that an event has occurred or will occur. “Critical safety item” means a part, subassembly, assembly, subsystem, installation equipment, or support equipment for a system that contains a characteristic, any failure, malfunction, or absence of which could have a safety impact. “Safety impact” means the occurrence of death, permanent total disability, permanent partial disability, or injury or occupational illness requiring hospitalization; loss of a weapon system; or property damage exceeding \$1,000,000. “Subcontractor” means any supplier, distributor, vendor, or firm that furnishes supplies or services to or for the Contractor or another subcontractor under this contract.

(b) The Contractor shall provide notification, in accordance with paragraph (c) of this clause, of— (1) All nonconformances for parts identified as critical safety items acquired by the Government under this contract; and (2) All nonconformances or deficiencies that may result in a safety impact for systems, or subsystems, assemblies, subassemblies, or parts integral to a system, acquired by or serviced for the Government under this contract.

(c) The Contractor— (1) Shall notify the Administrative Contracting Officer (ACO) and the Procuring Contracting Officer (PCO) as soon as practicable, but not later than 72 hours, after discovering or acquiring credible information concerning nonconformances and deficiencies described in paragraph (b) of this clause; and (2) Shall provide a written notification to the ACO and the PCO within 5 working days that includes— (i) A summary of the defect or nonconformance; (ii) A chronology of pertinent events; (iii) The identification of potentially affected items to the extent known at the time of notification; (iv) A point of contact to coordinate problem analysis and resolution; and (v) Any other relevant information.

(d) The Contractor— (1) Is responsible for the notification of potential safety issues occurring with regard to an item furnished by any subcontractor; and (2) Shall facilitate direct communication between the Government and the subcontractor as necessary.

(e) Notification of safety issues under this clause shall be considered neither an admission of responsibility nor a release of liability for the defect or its consequences. This clause does not affect any right of the Government or the Contractor established elsewhere in this contract.

(f) (1) The Contractor shall include the substance of this clause, including this paragraph (f), in subcontracts for— (i) Parts identified as critical safety items; (ii) Systems and subsystems, assemblies, and subassemblies integral to a system; or (iii) Repair, maintenance, logistics support, or overhaul services for systems and subsystems, assemblies, subassemblies, and parts integral to a system. (2) For those subcontracts described in paragraph (f)(1) of this clause, the Contractor shall require the subcontractor to provide the notification required by paragraph (c) of this clause to— (i) The Contractor or higher-tier subcontractor; and (ii) The ACO and the PCO, if the subcontractor is aware of the ACO and the PCO for the contract.

(End of clause)

(Revised July 29, 2009)

“US Department of Defense Counterfeit Regulations Impact Global Suppliers” April 27, 2012

Revenue by Region from Suppliers to the U.S. Government for the Period From 2007 Through 2011 (in U.S. Dollars)

Region	No. of Companies Affected	Revenue Affected	% of Overall Revenue
European Union	283	\$1,023,188,872.00	50.52%
Middle East	32	\$951,248,650.00	46.97%
Asia-Pacific	38	\$35,475,070.00	1.75%
South America	2	\$9,693,771.00	0.48%
Caribbean	1	\$3,211,084.00	0.16%
Central America	1	\$2,190,856.00	0.11%
Africa	4	\$148,074.00	0.01%
Eastern Bloc	1	\$29,901.00	0.00%
Total	362	\$2,025,186,278.00	100.00%

Source: IHS iSuppli Research April 2012

- Non-U.S.-based suppliers accounted for more than \$2 billion during the five-year period from 2007 to 2011, with European Union (EU) and Middle Eastern companies accounting for the bulk of the American government’s procurement
- Data in the figure was derived from the IHS Haystack system that provides information on more than 100 million items in the U.S. Federal Supply Catalog and more than 40 U.S. Army, Navy, Air Force and related databases
- The impact of NDAA 2012, *Section. 818. Detection and Avoidance of Counterfeit Electronic Parts*, is beginning to be felt worldwide, as many international companies and global manufacturing facilities begin to see customer requests for counterfeit detection and avoidance measures flowed down through the supply chain

US Attorney's Manual

1701 Trademark Counterfeiting—Introduction

The Trademark Counterfeiting Act of 1984, Pub. L. No. 98-473, Tit. II, § 1502(a), 98 Stat. 2178 (1984), and the Anticounterfeiting Consumer Protection Act of 1996, Pub.L. No. 104-153, 110 Stat. 1386 (1996), address the growing problem of trafficking in counterfeit trademark goods, which has primarily involved the clandestine manufacture and distribution of imitations of well-known trademarked merchandise. The 1984 Act created an offense, codified at 18 U.S.C. § 2320, which provides that "whoever intentionally traffics or attempts to traffic in goods and services and knowingly uses a counterfeit mark on or in connection with such goods or services" shall be guilty of a felony. 18 U.S.C. § 2320(a). Section 2320(b) enables the United States to obtain an order for the destruction of articles in the possession of a defendant in a prosecution under this section upon a determination by the preponderance of the evidence that such articles bear counterfeit marks.

These Acts also amend the Lanham Act, 15 U.S.C. § 1501 *et seq.*, to create stronger remedies in civil cases involving the intentional use of a counterfeit trademark. They provide mechanisms for obtaining statutory damages, treble damages and attorney's fees. 15 U.S.C. § 1117. The Lanham Act also provides for ex parte application by a trademark owner for a court order to seize counterfeit materials and instrumentalities where it can be shown that the defendant is likely to conceal or transfer the materials. *Id.* § 1116(d). New amendments permit the seizure order to be served and executed either by federal law enforcement officers or by state or local law enforcement officers. *Id.* § 1116(d)(9). The Lanham Act also requires applicants to file a notice of application for an ex parte seizure order with the United States Attorney, who may participate in such proceedings if they appear to affect evidence of a federal crime. See this [Manual at 1719](#).

NOTE: The Anticounterfeiting Consumer Protection Act of 1996 requires that the Attorney General report to Congress on investigative and prosecutive activities that occur in relation to the criminal intellectual property statutes, including 18 U.S.C. § 2320. See [USAM 9-68.150](#) and this [Manual at 1703](#).

US Attorney's Manual

1702 Trademark Counterfeiting—Charging Considerations

Section 2320 is not intended to criminalize every trademark infringement for which remedies may exist under the Lanham Act, 15 U.S.C. §§ 1051 *et seq.* It is intended to deal vigorously with the burgeoning and increasingly lucrative trade in outright copies of well-known trademarked merchandise. The 1996 amendments are intended to focus prosecutive attention on the growing problems associated with the unlawful importation of counterfeit trademarked goods, and violations tied to organized criminal behavior and criminal enterprises.