INSIGHT

Dear ERAI Members and Colleagues,

It's hard to believe that another year has come to a close. With a new year quickly approaching, it's time to reflect on the events that have shaped ERAI and the industry over the past year.

In April the ERAI Executive Conference was held in San Diego, CA and featured a wide range of topics from our theme of "Succeeding in the Age of Counterfeits, Cyber Attacks, Seized Shipments & Diminishing Resources" and a well-balanced combination of attendees representing all facets of the industry and government.

Member input led to the creation of new features such as the Reported Parts Search Log, ERAI Blog Subscriptions, US Consolidated Screening Search, Nonconformance Photo Library and the new Nonconformance Photo Library Slideshow training tool.

The overall number and pattern of suspect counterfeit parts reported to ERAI persisted from 2014 to 2015, posing a continuing challenge to the industry.

Continued standards development and document revisions aim to assist purchasers and integrators of electronic parts mitigate the risk posed by counterfeit parts. We anticipate seeing published revisions from SAE in 2016 including AS5553 and AS6081 and the publication of AS6171.

Government indictments and sentencings have intensified for trafficking counterfeit military goods, violations of U.S. export laws and smuggling of restricted components to Russia and China resulting in significant fines and prison sentences.

Changes to the FAR and DFARS are setting US Government supplier expectations and providing further clarifications with regard to supply chain flowdown and source selection.

We hope 2015 was a productive year for you and wish you the best in 2016. On behalf of all at ERAI we want to thank you for your continued support and wish you and your families a wonderful holiday season and a Happy New Year!

Anne-Liese Heinichen
Editor-in-Chief
anne@erai.com

INSIGHT

ERAI New Features and Website Changes

By Damir Akhoundov

New Features

High Risk and Suspect Counterfeit Parts Classification Icons

Parts reported by ERAI were previously classified three different ways:

- SC (Suspect Counterfeit) - A part that displays one or more nonconformances and shows evidence of counterfeiting.
- NC (Nonconforming) - A part that displays one or more nonconformances.
- SC NC (Suspect Counterfeit/Nonconforming) - A part that displays one or more nonconformances and shows evidence that it is a used part sold as new. According to the U.S. DoD Defense Federal Acquisition Regulation Supplement: Detection and Avoidance of Counterfeit Electronic Parts (DFARS Case 2012-D055) published in the Federal Register on May 6, 2014, a used part represented as new is considered suspect counterfeit.

ERAI recently added a fourth designation of:

- FN (Federal Notice) - A part or list of parts which are publically released as part of a U.S. federal/ government agency notice. These parts may require additional evaluation based on your organization's internal risk mitigation procedures

Additionally, a new filter has been made available in the High Risk & Suspect Counterfeit Parts Advanced Search to enable users to include/omit FN parts from part search results. Please note the default setting includes Federal Notice parts.

Nonconformance Photo Library and Training Slideshow

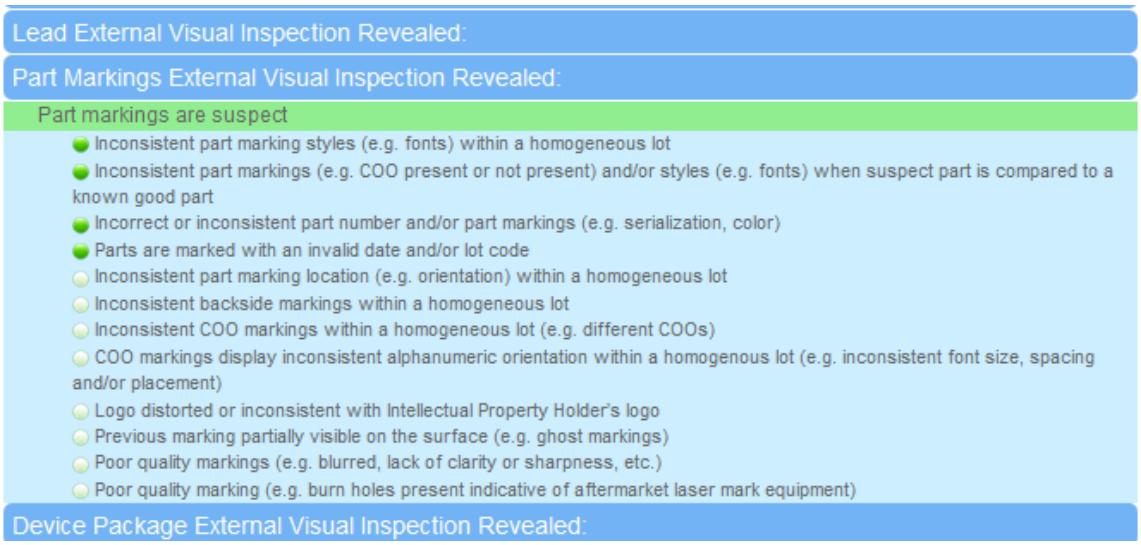
Over a year ago, ERAI compiled a library of photographs and a search engine to enable Members to locate images of specific part non-conformances specified from a list of categories from our Nonconformance Photo Library. We then then further enhanced this search by providing a set of filters enabling Members to narrow down searches to include images of specific part numbers or parts from a specific manufacturer. We have received great Member feedback and based on Member requests and reviews, we have now improved this feature by adding the capability to create slideshow presentations based on search criteria from the Nonconformance Photo Library in order to provide our Members with a powerful and educational training and presentation tool.

The Nonconformance Photo Library Training Slideshow displays images contained within part reports culled directly from ERAI's High Risk and Suspect Counterfeit Parts Database based on criteria you select.

TO CREATE YOUR CUSTOM MADE SLIDESHOW:

SELECT THE NONCONFORMANCE CATEGORIES TO INCLUDE IN THE SLIDESHOW

Members can locate images containing examples of specific nonconformances. Select the radio button next to each nonconformance(s) category you want included in your search results and only images containing one or more of your selections will be displayed. You can select one or multiple categories – whatever is relevant for your needs. If you check more than one nonconformance category, the system will display images that include at least one of the categories you selected. You can use the filters described below to further narrow down the results based on part number and manufacturer.

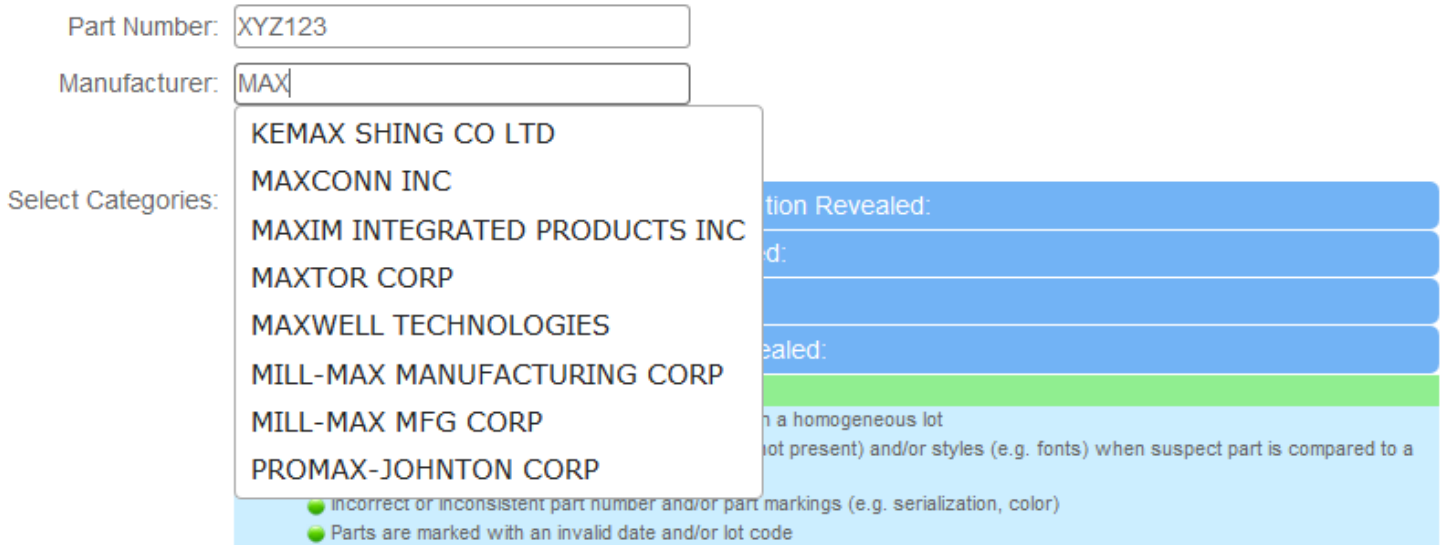


APPLY PART NUMBER FILTERS (OPTIONAL)

To filter parts relative to a specific part number, please enter at least 3 characters in the part number field. Please note that this is not a required field. The search results will display part numbers that include the sequence of characters you have entered – e.g. if you search for "103", the search results will display parts that start with 103 or have 103 contained in the part number such as INA10386 or XCS10-3VQ100I. The part search will disregard hyphens.

APPLY MANUFACTURER FILTER (OPTIONAL)

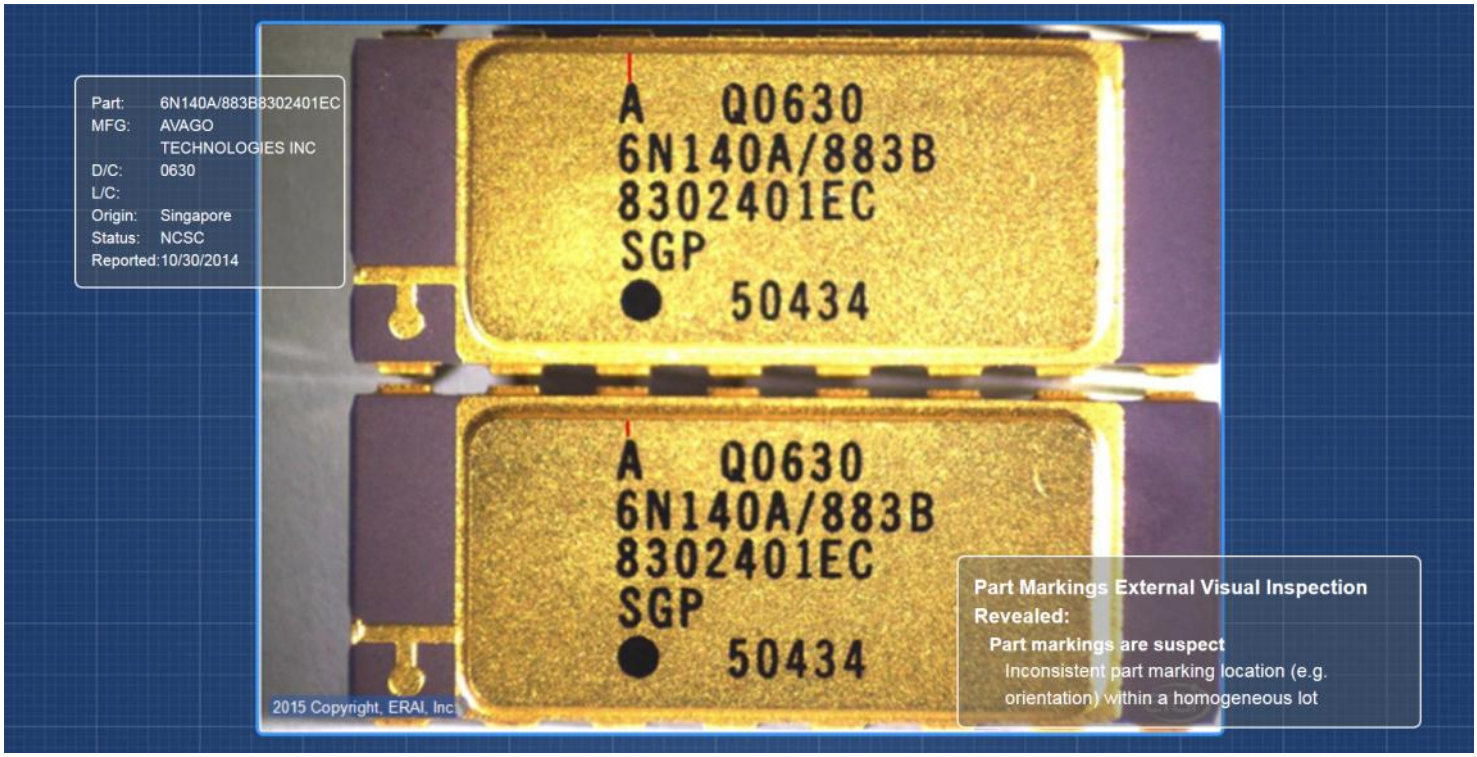
A manufacturer pull down is provided if you wish to restrict your image results to a selected manufacturer. Just type in the first 3 letters of manufacturer name and the system will offer you a list of matching manufacturers.



START SLIDE SHOW

After selecting your search criteria, click on the "Start Slide Show" button. The resulting images will be compiled into a slideshow that can be used for training and education purposes. The images will be presented in a full browser or full screen format (depending on your choice of display mode). Basic part information as well as a detailed description of the specific nonconformance illustrated will be presented in draggable data popups. You can start a slide show in a full screen mode by clicking on the START FULL SCREEN SLIDE SHOW button.

The slideshow will then be launched.

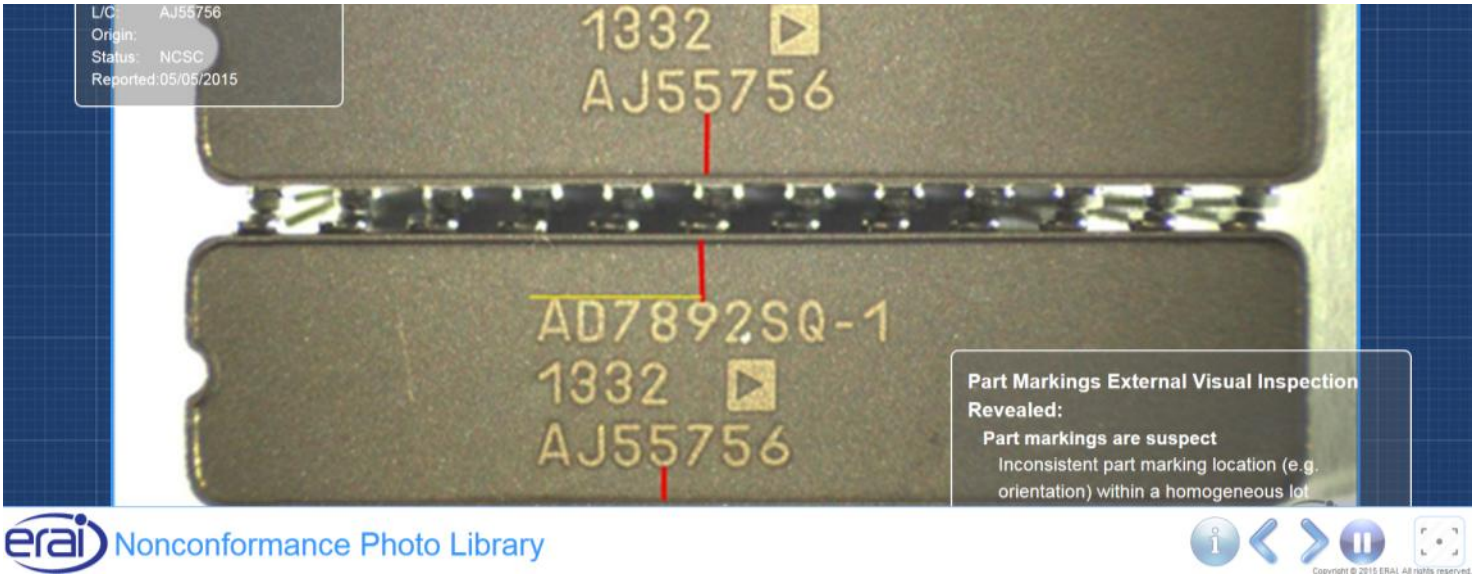


SLIDE SHOW CONTROLS

During the Training Slide Show you can control the presentation in several different ways.

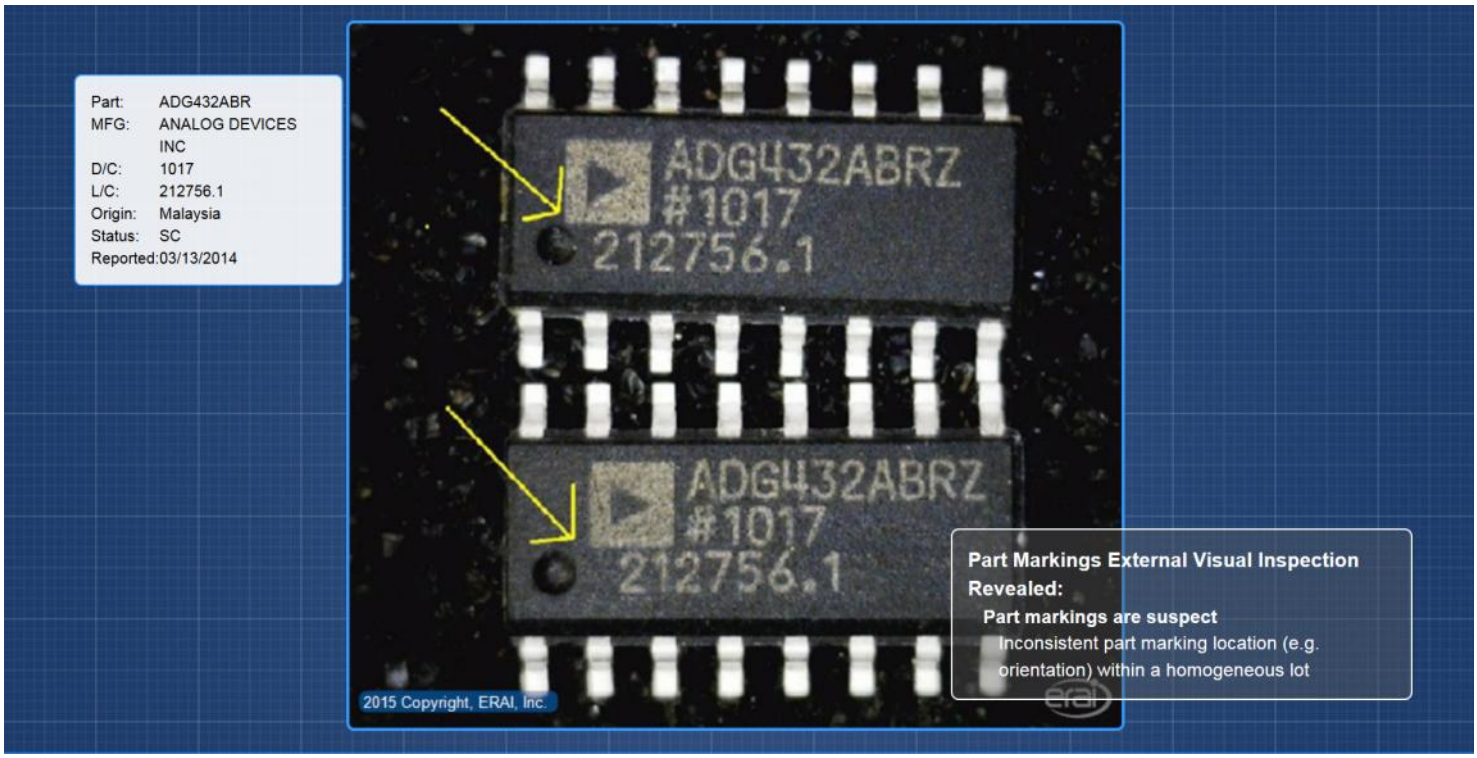
1. SLIDESHOW TOOLBAR

A slideshow toolbar will briefly appear on the bottom of the display area at the beginning of the slideshow. You can retrieve the toolbar at any time by simply moving your mouse cursor to the bottom of the display area. The toolbar provides basic controls such as "PAUSE", "SLIDE FORWARD", "SLIDE BACKWARD", "SWITCH FULL SCREEN MODE ON/OFF", "TURN DATA POPUPS ON/OFF".



2. DATA POPUPS

Each slide in the slideshow you create will display two data popups that provide basic information about the nonconforming part that is displayed in the picture as well as a detailed description of the specific nonconformance(s) illustrated by the picture. These popups are semitransparent and are designed to provide minimum interference with the main image that is being viewed. These popups will become fully visible if the mouse cursor is placed over them and the slideshow will pause for you to be able to read the information in detail. Upon removal of the mouse cursor from the data popup, the slideshow will proceed to the next slide. The data popups are also draggable so you can custom position them on the screen.



3. PAUSING AND RESTARTING THE SLIDESHOW

At any time the slideshow can be paused in three different ways:

- Clicking anywhere on the slideshow background will pause the slideshow. One more click anywhere in the background of the slideshow will resume the slideshow.
- Moving your mouse cursor over one of the two data popups will pause the show and brighten the data displayed within that data field. Upon removing the cursor from the data field, the slideshow will automatically resume.
- Clicking on the "PAUSE" button within the hidden slideshow navigation toolbar will pause the slideshow. Simply move your mouse cursor to the bottom of the slideshow screen and the toolbar will appear. To resume the show, click on the same button or click anywhere within the background of the slideshow.

CUSTOM SLIDESHOW LINKS

Company Administrators are additionally capable of creating a stand-alone slideshows. These slideshows can be created upon request and you will be provided with an encoded link that will launch the slideshow on any computer that has a browser and Internet connection. ERAI membership is not required to use these custom-made slideshows and they are made available only for a specified period of time after which they will be auto-deleted.

Changed Features

Nonconformance Photo Library Search Logic Changes

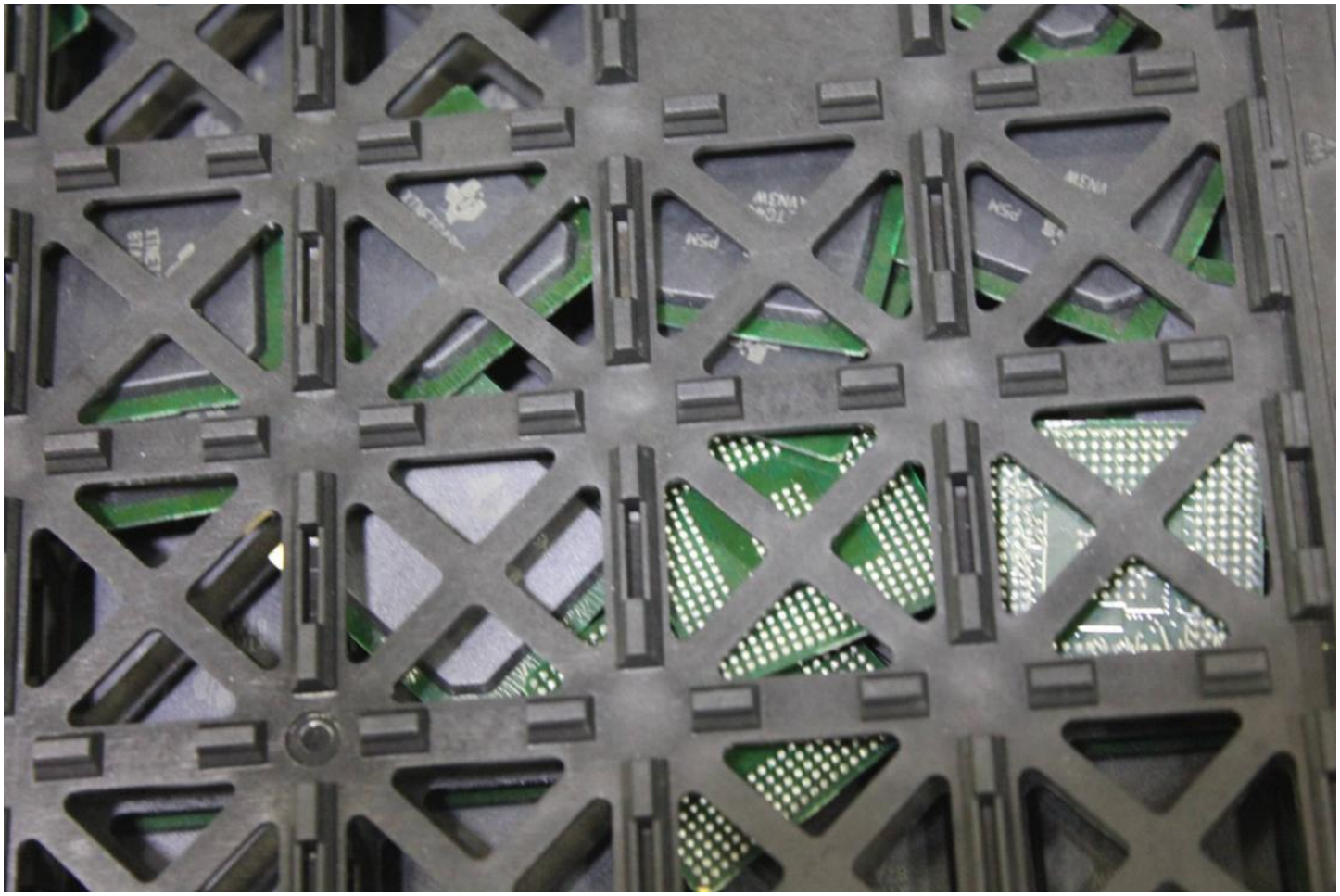
You spoke, we listened! Feedback from ERAI Members stated the Nonconformance Photo Library search was too specific and required multiple searches to get many results. The issue was that the non-conformance categories were used cumulatively (e.g. if multiple specific nonconformance categories were selected, the results would only offer images that contained ALL of the selected nonconformance categories resulting in a limited data set due to the fact that the majority of images illustrate only three or fewer categories). Members would be forced to go back to refine the results and after removing some of the selected categories, more results would be attained.

The new logic revisions allow users to select any number of non-conformance categories and the results will include all images that have at least one of the selected categories assigned. The default sorting of resulting images will be based on images with the highest number of selected categories assigned appearing first followed by images with a lesser number of selected categories. This new logic ensures that the majority of searches conducted will now result with images illustrating the categories chosen by the Member. Members can still further narrow the search results by applying the part number and/or manufacturer filters.

Report Goods Damaged by CBP

By Anne-Liese Heinichen

A U.S.-based distributor placed an order with an international supplier for goods that were subsequently inspected by U.S. Customs and Border Protection (CBP). Because the goods were not properly repackaged, the parts were severly damaged in transit causing a financial loss to the importer. CBP bears no financial responsibility or liability even if their negligence contributed to the damage of the goods.



ERAI has begun documenting these types of incidents in an effort to demonstrate to Customs the importance of proper handling and repacking. Our objective is to raise awareness and provide feedback from the industry that might lead to changes in how shipments containing sensitive devices are inspected and repackaged. Your input is vital. If you receive a damaged shipment that is the result of improper handing or repacking by CBP, please submit a report to ERAI at http://www.erai.com/customuploads/ERAI_CBP_Damage_Report.docx.

Avoiding Counterfeit Electronic Parts: How DoD's Proposed Rule May Affect You

By Robert S. Metzger Rogers Joseph O'Donnell, PC*

On September 21, 2015, DoD published a Proposed Rule to modify its existing regulations on detection and avoidance of counterfeit electronic parts. 80 Fed. Reg. 56939. DoD held a public meeting to get input on the proposed rule on November 13, 2015. By action taken on October 21, 2015, DoD extended the comment period until December 11, 2015. 80 Fed. Reg. 63735. For information on how to submit comments, see http://www.gpo.gov/fdsys/pkg/FR-2015-10-21/pdf/2015-26749.pdf.

For smaller companies, the most important changes in the Proposed Rule are in a new contract clause, presently named DFARS 252.246-70XX ("Sources of Electronic Parts"), that Department of Defense purchasing activities are to use in solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, when procuring— (1) Electronic parts; (2) End items, components, parts, or assemblies containing electronic parts; or (3) Services, if the contractor will supply electronic parts or components, parts, or assemblies containing electronic parts as part of the service. Small business set-asides are subject to the rule.

Before, the regulations covering counterfeit electronics required larger DoD contractors – namely, companies whose DoD contract revenues are large enough to make them subject to Cost Accounting Standards requirements – to have systems and procedures to detect and avoid counterfeit electronic parts. These companies were under a flow-down obligation, so some smaller vendors who support the big defense contractors already have seen their customers include solicitation requirements and special terms and conditions that to reduce the risk of counterfeit parts on purchases intended for DoD customers. Before, however, there was no mandatory DFARS clause that would apply to all solicitations and that would mandate specific measures on the part of the entire supply chain.

These rules follow enactment of Section 818 of the NDAA for FY 2012, following Senate hearings that revealed the danger of counterfeit electronic parts. DoD is especially vulnerable because many of its fielded systems were built and deployed years or even decades ago. That makes it hard to support this equipment, because parts needed for sustainment all too often cannot be found through "trusted sources" such as original manufacturers or their authorized distributors. Unscrupulous parties have exploited the continuous demand for these parts though they may be obsolescent and out of production for years. Following enactment of Section 818, DoD published the final DFARS rule, on May 9, 2014, 78 Fed. Reg. 26092, that is the subject of the proposed revision.

DoD systems draw upon an enormous and diverse supply chain. In fact, the promulgation comments accompanying the proposed rule indicate that DoD estimates the rule will apply to approximately 33,000 small entities that have DoD prime contracts or subcontracts or who supply electronic parts or components to or for DoD customers. DoD and its higher tier suppliers will continue to buy and sometimes favor purchases from small business, who may react negatively to the obligations, costs and compliance risks of the proposed counterfeit rule. Similarly, DoD continues to purchase electronic parts from commercial and COTS suppliers who may react to this rule as unnecessary, intrusive and asking them to incur special costs to accommodate a particularly demanding customer – the Pentagon – who represents a very small part of their markets.

Before you reach a judgment about the proposed rule, let's consider briefly the context and the reasoning behind the extension to smaller business, commercial and COTS suppliers. Simply put, if a counterfeit electronic part is installed in a weapon system, such as a combat aircraft, when it fails there will be hazard to the flight crew and likely mission failure. The Senate's lengthy hearings and many other sources confirm

that there are many sources around the world all too ready and sometimes quite capable of selling fakes that only seem genuine. Vulnerability exists because of the continuing demand for old parts that trusted sources don't have. The consequences of a counterfeit can be severe.

It makes no difference, in terms of the consequence of a counterfeit part that fails, if it comes from a big DoD prime or a small business vendor many tiers below. In fact, there is some reason to think that vulnerability to counterfeit parts is greater as you move "down" the supply chain to smaller and less sophisticated companies, because they are less likely to have the systems and procedures, or the test and inspection capabilities, to readily defend against this threat.

So in the view of this observer, DoD has very good reasons to impose the counterfeit avoidance rule on the whole of its supply chain. Those reasons, however, don't make the rule practicable and don't inform companies newly subject to the rule of what they are supposed to do. Nor do they answer the question of whether these new obligations are affordable.

The commercial part of the DoD supply chain should recognize the risk of counterfeits, but that risk does not apply equally to all commercial or COTS suppliers. A central premise of DoD's regulatory scheme is that larger contractors covered by the full rule should employ risk-based analysis to assess whether a particular transaction from a specific supplier for an identified electronic part carries unacceptable risks, or, perhaps, higher than ideal risks which indicate that test and inspection should be done for risk mitigation.

Applying this principle, there is low risk in purchases from established commercial and COTS suppliers who are furnishing parts that are currently in production. Additional confidence can be gained if such suppliers keep good records and, especially, where they are willing issue a "certificate of conformance" to document authenticity. "Pedigree" is the word applied to verify that the source of a purchased part is the party authorized to make or sell it. "Provenance" applies to the process after delivery by which parts are transferred, warehoused, distributed and eventually sold. Good documentation of both "pedigree" and "provenance" is referred to as "traceability" – an objective of both the original and the proposed rule. Traceability is an important prospective objective, but DoD should not expect its supply chain to invent documentation for historical purchases when the rules and expectations were different.

Compliance is more difficult for small businesses who may be called upon to acquire, install and sell equipment that has electronic parts they cannot obtain from those original, "trusted" sources. It is important for their higher tier customers, namely the defense primes who are fully covered by the counterfeit rule, to help their small business partners with compliance. This means making technical expertise and resources, including testing, available. In my opinion, through "mentoring" and cooperative engagement of challenges posed by the rule (if adopted as proposed), primes can fulfill their obligations to the Pentagon and help ease the burden and reduce the risk of noncompliance by their small business suppliers.

From a contractual standpoint, some primes have a penchant to take a DFARS obligation applied fully to them and then to demand literal compliance by all their subs at every level as a condition to continue to remain an acceptable supplier. I do not believe that primes must or should attempt to push down all the duties, risks and liabilities to their smaller vendors. They can fulfill the intent of the rule with prudent, risk-based, cooperative measures, and when necessary by seeking guidance or even approval from the government purchasing activity. It certainly would help, however, for the drafters of the DFARS to improve the rule to better inform smaller companies, COTS and commercial suppliers of what is expected of them. DoD can work with the SBA, for example, to make special support resources available. In addition, DoD should issue implementation instructions, for its contracting and oversight personnel, in the form of Procedures, Guidance and Information (PGI) and FAQs, to answer the recurring questions, dispel myths and better inform its huge industrial base of how to make this work.

Let's conclude with a brief examination of the specifics of the proposed new 252.246-70XX clause. Some of it is fairly straightforward. Other aspects make good business and engineering sense. The fundamental feature of the proposed clause is that contractors should narrow their sources of electronic parts to reduce buys from potentially untrustworthy sources. Buying parts that are in production or currently in stock from the original source or authorized dealers and suppliers is the best way to fulfill this objective. If needed parts can't be obtained from this preferred class, resort should be made to other suppliers – who may include companies qualified to act as "distributors" of hard to obtain parts – provided that certain controls are applied. First, a small business may be able to utilize distributors qualified by their customer as "trustworthy." (This is to be done by reference to a number of new industry standards and best practices. A small number of distributors have gone to great lengths and costs to establish their credentials and capabilities in counterfeit parts avoidance.) Another hedge is to arrange for test and inspection parts of at-risk parts. If a company doesn't have these abilities in house, it can ask its higher tier customer for its recommendation(s), or it can hire third party resources for this function. (Care should be taken to verify the claimed capabilities of the test and inspection resource.)

Another clause in the proposed rule is problematic and should be clarified. It states, as another condition of a contractor using a part from other than the most trusted sources, that the "Contractor" (sic) "assumes responsibility for the authenticity of parts" that it may obtain from sources of lesser assurance. I read this clause as applicable directly to the supplier who enters into a prime contract with DoD that makes it (the "Contractor") obligated to flow down the clause requirements in its subcontracts and purchase orders. I also believe that the correct interpretation is that DoD intends that its direct supplier – the "Contractor" that is in privity with DOD – bears the responsibility for authenticity. But there is some ambiguity as to who is the "Contractor" with this obligation. I do not see it as necessary, reasonable or (in most cases) as even plausible for downstream vendors to assume this responsibility. That is too much risk, with too many of the functions driving the risk outside the vendor's control. My take is that vendors should act responsibly, assess their vulnerability to counterfeits and improve their processes to reduce these risks. In dealing with particular parts, vendors should consult available industry standards and best practices. They should seek guidance and instruction from their customers, and from DoD or SBA if the resources are available. But they need not and must not be made the "guarantors" of the authenticity of electronic parts which they can purchase only from less than "trusted suppliers.

Price comes into this equation as well. Too often, lowest price has been a principal motivation of government customers who purchase supplies and support for legacy systems. This must change. Higher supply chain assurance is not free. The objectives of the counterfeit parts rule – which I consider to be important and generally well-considered – cannot be achieved without a change in purchaser practices and receipt of necessary funding to pay for higher assurance. The same principle applies to prime and higher tier customers.

There are other facets and features of the proposed rule and many strategies that can be considered to assure compliance, retain and even grow business in the defense supply chain. My team would be pleased to consult.

---

* Bob Metzger heads the Washington, D.C. office of Rogers Joseph O'Donnell, PC, a boutique law firm that has specialized in public procurement matters for more than 30 years. Bob is a nationally recognized expert in cyber and supply chain security, with numerous presentations and publications to his credit. Many of these are available at http://www.rjo.com/pub_counterfeit.html.

Risk Management and Insurance Review Tips for 2016

By Howard A. Miller, L/B/W Insurance & Financial Services, Inc.

Being adaptable is the key to survival. Your ability to review and adapt to changing and emerging threats is critical to your long term success. The world changes and so does your business. This is why you need to review your risk management and insurance program every year. Has your business grown or contracted over the past year? Here are a few things to consider:

1. **Audits:** Update your sales, property values and workers compensation payroll figures. Workers compensation and general liability policies can be auditable. Insurance carriers have the right to inspect your books and records to verify you are paying on accurate sales and payroll values. If you are getting bills from your insurance companies based on audited figures that you underestimated from the previous year, you can avoid this by reviewing and updating your payroll and sales figures. If you know you are in a growth mode, and you would rather pay over the course of the policy term, follow this advice and update your insurance carrier so you don't get stuck owing money on last year's policy with limited or no options for a pay plan.

2. **Property:** Maybe you need to reduce your insurance coverage – why overpay for coverage you cannot use. On the other hand, some policies will penalize you if you are not insured to value on your buildings and property at the time of the loss. Understand your co-insurance and valuation terms and conditions and make sure you are insured to value. You will thank yourself after a loss and, in some cases, there is not that much difference in price for being insured with the correct limits. If you own property, you can usually determine a certain value for the cost of replacement. What about obsolete inventory that is no longer being manufactured? How will you value this so you are adequately compensated in the event of a loss?

3. **Liability:** Review your operations and products. Has anything changed? Are you providing new services or products that you have not done in the past? Professional advice and analytical services can create new exposures. Insurance is a puzzle. It's about getting the right pieces. I had a client once tell me they just wanted an insurance policy, with no exclusion, that covered them for everything. A couple comments about this: One, you would not want to complete the application. Two, you would not want to see the price. Get the right coverage for your unique exposures and what you feel are priorities for your organization. One main trigger for your general liability policy is bodily injury and property damage. Professional services that cause a third party to sue you for financial damages are not typically covered under general liability. Another great question might be to ask: What am I not covered for? I recommend looking at your exposures to loss and the causes of loss, not just your existing insurance.

4. **Emerging Risk:** The world is changing. Information is a new currency. To take a holistic view of your risk requires looking at your digital exposures as well as traditional analog risk. A few things to consider: What are the ramifications of digital risk? Could a virus infect our network and disrupt our operations? What about a denial of service attack? How much money could be lost due to this disruption? Digital information can be copied, transmitted, modified or destroyed in a matter of seconds. Three questions to ask before you review your insurance in this area: How would the breach of confidentiality of our communications or data impact our organization? Could the destruction or inability to access our data disrupt our operations? When you look at any exposure you need to consider certain variables. One variable to be conscious of is your custody and access of the information of others to whom you may be liable either by contract, industry standards or regulatory compliance. Are there other third parties who are relied upon to maintain the confidentiality of your information in their care, custody or control? Which leads to the next point.

5. **Review your contractual and legal obligations:** How much liability insurance should you purchase? It depends on how much you could be legally liable for. A discussion with a knowledgeable attorney who has a risk management mindset could offer real life examples of the cost and ramifications of potential liability to your organization. This may influence your insurance buying decisions and your risk control strategies.

6. **Review your risk control plans:** These are plans that are put in place to control the frequency or severity of a potential loss. Review your policies, procedures, training and incident response in areas such as: human resources including key executives, workplace safety and the security of digital and intellectual property.

Taking the time to look back and focus on the negative impact of risk once a year could make you much more confident in your ability to meet your goals for the year to come.

If you have any questions, please contact Howard Miller at HowardM@lbwinsurance.com.

Jeff Krantz Avoids Jail Term

On July 28, 2015, after an extensive, multi-year investigation involving the Defense Criminal Investigative Service (DCIS) and the U.S. Department of Transportation, Office of Inspector General, Jeff Krantz pleaded guilty to supplying falsely remarked Intel microprocessor chips, many of which were used in U.S. military and commercial helicopters.

Krantz, who pleaded guilty to one count of wire fraud, was sentenced on December 10, 2015 to three years' probation and fined $100,000.00. He was also ordered to pay $402,650.00 in restitution.

As part of his guilty plea Krantz agreed to a two-year ban on the purchase or sale of electronic parts. He also forfeits all direct or indirect control over his company, Harry Krantz LLC, authorities said.

Additional Reading

DOJ Press Release: New York Man Admits Supplying Falsely Remarked Computer Chips Used in U.S. Military Helicopters

United States of America v. Jeffrey Krantz – Wire Fraud Charge

United States Department of Justice – The Plea And Offense

United States of America v. Jeffrey Krantz – Jeff Krantz Statement

United States of America v. Jeffrey Krantz – Government's Memorandum In Aid Of Sentencing

United States of America v. Jeffrey Krantz – Sentencing Memorandum On Behalf Of Jeffrey Krantz

United States of America v. Jeffrey Krantz - Sentencing

Co-Owner and Vice President of AFM Microelectronics Inc. Arrested on Charges of Illegal Military Weapons Brokering

By Kristal Snider

Since 1990 the United States has maintained an arms embargo against the People's Republic of China (PRC) that prohibits the export, re-export, or transfer of any defense article to the PRC. In its effort to bypass US Federal Regulations, the Chinese Government enlisted the assistance of "technology spies" in an attempt to obtain advanced US fighter aircraft engines and a UAV (unmanned aerial vehicle), according to recently unsealed Federal Court documents.

The documents allege that Wenxia "Wency" Man and Xinsheng Zhang attempted to acquire and export to China the General Atomics MQ-9 Reaper UAV, the Pratt & Whitney F135 engine used on the F-35 stealth fighter, the P&W F119 engine used on the F-22 Raptor stealth fighter and the General Electric F110 engine used on the F-15 and F-16 fighters.

Wexia Man was arrested on October 22, 2015 and released on bond on November 30, 2015. Man is the co-founder and Vice President of AFM MicroElectronics (aka American Function Materials Inc.), a capacitor manufacturer and supplier that markets its line of products to the wireless communications, fiber optic, medical electronics, defense, aerospace, and satellite communications markets. Wexia Man's husband, Yingkuang "William" Liang, is her business partner and the President of AFM. The company appears to still be operating and should be considered "HIGH RISK".

About AFM

AFM Microelectronics Inc.
9040 Carroll Way Suite 3,
San Diego, California, 92121 U.S.A
Tel: 1(858)222-1199
Fax: 1(858)726-2688
URL: www. afmmicroelectronics.com

AFM designs, develops, manufactures and markets RF/microwave Multilayer Capacitors, High Power High current Multilayer Capacitors, High Temperature High Voltage Multilayer Capacitors, GBBL (Grain Boundary Barrier Layer) High K substrates for Single Layer Capacitors, Ultra Low Fire Dielectric powder for multilayer capacitors. Capacitors produced range in size from 0505 to 13560, with operating voltages from 25 volts to 50,000 volts.

Additional Reading

United States of America vs. Wenxia Man a/k/a "Wency Man", and Xinsheng Zhang: Indictment
http://www.erai.com/customuploads/file0430476936084357.pdf
China Accused of Trying To Acquire Fighter Engines, UAV
http://www.defensenews.com/story/defense/policy-budget/industry/2015/10/27/china-accused-trying-acquire-fighter-engines-uav/74676946/
Feds charge woman in S. Fla. plot to broker $50M drone to China
http://www.sun-sentinel.com/local/broward/fl-defense-drone-china-20151023-story.html
Bond set for woman accused of S. Fla. plot to sell $50M drone to China
http://www.sun-sentinel.com/local/broward/fl-drone-china-plot-bond-20151110-story.html

Chinese Nationals, (Doing Business as HK Potential), Have Been Arrested for Scheme to Steal and Illegally Export Military-Grade Semiconductors

Deirdre M. Daly, United States Attorney for the District of Connecticut, today announced that three Chinese nationals have been arrested on federal criminal complaints in connection with a scheme to obtain and illegally export sophisticated semiconductors stolen from the U.S. military. **DAOFU ZHANG**, 50; **JIANG GUANGHOU YAN**, also known as "Ben," 33; and **XIANFENG ZUO**, 37, were arrested this morning in Milford.

The three defendants made initial appearances before U.S. Magistrate Judge Sarah A.L. Merriam in New Haven and were detained.

As alleged in the criminal complaints, federal law enforcement agents began investigating YAN and a Chinese company known as HK Potential in 2012 for trafficking in counterfeit semiconductors. In October 2014 and in March 2015, YAN sold a total of 45 counterfeit Intel microprocessors to an undercover agent who had advised YAN that the components would be used on a U.S. Navy contract involving submarines.

The complaints further allege that, in July 2015, YAN asked whether the undercover agent could obtain 22 Xilinx semiconductors, military grade, for which YAN would pay $37,000 each. After the undercover agent advised YAN that the Xilinx components could be stolen from a U.S. Navy base, YAN offered to provide fake Xilinx components that could be substituted for the stolen components in order to prevent detection of the theft. When asked whether the fake Xilinx components would work, YAN replied that "the fake one just look the same" but were "not ok for function." In November 2015, YAN shipped eight of the fake Xilinx components to the undercover agent.

ZHANG, YAN, and ZUO traveled to the U.S. on December 6, and they were arrested today attempting to take delivery of the Xilinx semiconductors from the undercover agent.

"The Justice Department and our federal law enforcement partners are committed to prosecuting those who would supply our armed forces with counterfeit electronic components, as well as those who attempt to steal sophisticated U.S. military components and distribute them to places unknown," stated U.S. Attorney Daly. "I thank the collaborative efforts of our partners in this long-term investigation, including the DCIS, HSI, FBI, U.S. Department of Commerce's Bureau of Industry and Security, and U.S. Air Force's Office of Special Investigations."

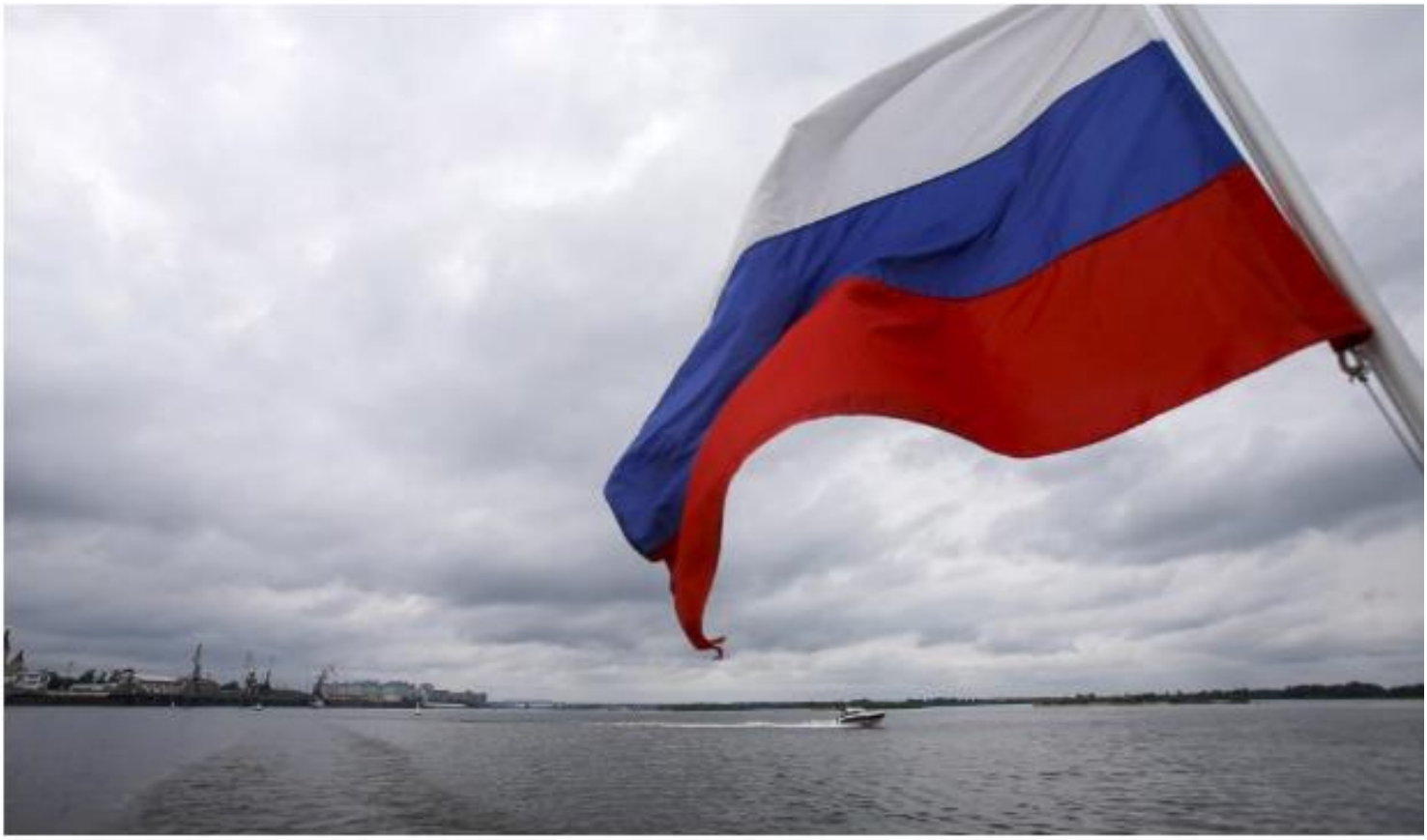
The complaint charges ZHANG, YAN, and ZUO with violating the International Emergency Economic Powers Act, which carries a maximum penalty of 20 years of imprisonment and a $1 million fine; and receipt of stolen government property, which carries a maximum penalty of 10 years of imprisonment and a $250,000 fine. ZHANG and YAN are also charged with trafficking in counterfeit goods, which carries a maximum penalty of 10 years of imprisonment and a $2 million fine; and mail fraud, which carries a maximum penalty of 20 years of imprisonment and a $250,000 fine. In addition, ZHANG and ZUO are charged with conspiracy, which carries a maximum penalty of five years of imprisonment and a $250,000 fine.

U.S. Attorney Daly stressed that a complaint is only a charge and is not evidence of guilt. Charges are only allegations, and each defendant is presumed innocent unless and until proven guilty beyond a reasonable doubt.

This matter is being investigated by the Defense Criminal Investigative Service, Homeland Security Investigations, the Federal Bureau of Investigation, the U.S. Department of Commerce's Bureau of Industry and Security, and the U.S. Air Force's Office of Special Investigations. The case is being prosecuted by Assistant U.S. Attorney Edward Chang.

DOJ Press Release: http://www.justice.gov/usao-ct/pr/three-chinese-nationals-arrested-scheme-steal-and-illegally-export-military-grade

Three Defendants Convicted of Conspiring to Illegally Export Controlled Technology to the Russian Military



Three working for a Houston-based electronics company guilty on the counts of conspiracy to export and of illegally exporting over $30 million in microelectronics to the Russian military and intelligence services.

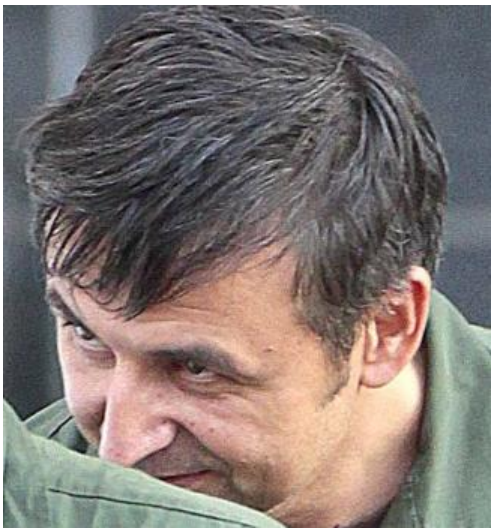
REUTERS/MAXIM SHEMETOV

"Through lies and deceit, the defendants and their co-conspirators sold over $30 million of microchips, much of which was destined for Russian military and intelligence agencies."

On October 26, 2015, after a month-long trial, Alexander Posobilov, Shavkat Abdullaev and Anastasia Diatlova were convicted of all counts, including conspiring to export, and illegally exporting, controlled microelectronics to Russia. Posobilov was also convicted of money laundering conspiracy. These defendants, all of whom worked at Arc Electronics Inc. (Arc), a Houston-based corporation, and eight other individuals were originally charged in October 2012. Five members of the conspiracy, including Arc owner Alexander Fishenko, previously pleaded guilty to related charges.

The convictions were announced by Assistant Attorney General for National Security John P. Carlin, U.S. Attorney Robert L. Capers of the Eastern District of New York, Assistant Director Randall C. Coleman of the FBI's Counterintelligence Division and Director Douglas Hassebrock of the Department of Commerce's Office of Export Enforcement.

"Alexander Posobilov, Shavkat Abdullaev and Anastasia Diatlova evaded U.S. export laws to illegally send sophisticated microelectronics to Russia," said Assistant Attorney General Carlin. "By purposefully circumvent-



ing U.S. law, including the International Emergency Economic Powers Act and the Arms Export Control Act, the defendants jeopardized our national security."

"These defendants were key players in a sprawling scheme to illegally export sophisticated technology to Russia," said U.S. Attorney Capers. "Through lies and deceit, the defendants and their co-conspirators sold over $30 million of microchips, much of which was destined for Russian military and intelligence agencies."
"By putting a halt to this conspiracy, and stopping the flow of these dual-use components to the Russian military and intelligence services, this verdict represents a clear victory for our national security," said Assistant Director Coleman.

"Today's convictions send a strong message to those who willfully evade export control laws and jeopardize the national security of the United States," said Director Hassebrock. "This case is the result of outstanding collaborative investigative work by the Justice Department, the Commerce Department and the FBI to break up a network whose aim was to illegally ship sophisticated U.S.-origin technology to Russia."

The evidence at trial established that between approximately October 2008 and October 2012, these defendants and their co-conspirators obtained advanced, technologically cutting-edge microelectronics from manufacturers and suppliers located within the United States and exported those high-tech goods to Russia, while carefully evading the government licensing system set up to control such exports. The microelectronics shipped to Russia included analog-to-digital converters, static random access memory chips, microcontrollers and microprocessors. These commodities have applications, and are frequently used, in a wide range of military systems, including radar and surveillance systems, missile guidance systems and detonation triggers. Russia does not produce many of these sophisticated goods domestically.

Posobilov was the Procurement Director of Arc, Abduallev was the Shipping Manager and Diatlova was a salesperson. To induce manufacturers and suppliers to sell them these high-tech goods, and to evade applicable export controls, the defendants and their co-conspirators often provided false end user information in connection with the purchase of the goods, concealed the fact that they were resellers and falsely classified the goods they exported on export records submitted to the Department of Commerce. For example, Arc falsely claimed to be a traffic light manufacturer on its website. In fact, Arc manufactured no goods and operated exclusively as an exporter.

Despite this subterfuge, the evidence established that the defendants were supplying Russian government agencies with sophisticated microelectronics. For example, the investigation uncovered a letter sent by a specialized electronics laboratory of Russia's Federal Security Service (FSB), Russia's primary domestic intelligence agency, to an Arc customer regarding certain microchips obtained for the FSB by Arc. The letter stated that the microchips were faulty and demanded that the defendants supply replacement parts. Shortly before trial, Arc President Alexander Fishenko pleaded guilty to all charges against him, including acting as an agent of the Russian government without prior notification to the Attorney General, as well as conspiring to export, and illegally exporting, microelectronics to Russia, money laundering conspiracy and obstruction of justice. Fishenko is currently awaiting sentencing.

When sentenced by U.S. District Judge Sterling Johnson Jr. of the Eastern District of New York, defendants Posobilov, Abdullaev and Diatlova face up to five years in prison for the conspiracy conviction, and up to 20 years in prison for each violation of the International Emergency Economic Powers Act (IEEPA) and the Arms Export Control Act (AECA). Posobilov also faces up to 20 years in prison for money laundering con-

spiracy.

The case is being prosecuted by Assistant U.S. Attorneys Daniel Silver, Una Dean, Richard Tucker and Claire Kedeshian of the Eastern District of New York, as well as Trial Attorney David Recker of the National Security Division's Counterintelligence and Export Control Section.

Source: http://www.justice.gov/opa/pr/three-defendants-convicted-conspiring-illegally-export-controlled-technology-russian-military

Additional Reading

Russian Agent and 10 Other Members of Procurement Network for Russian Military and Intelligence Operating in the U.S. and Russia Indicted in New York
https://www.fbi.gov/houston/press-releases/2012/russian-agent-and-10-other-members-of-procurement-network-for-russian-military-and-intelligence-operating-in-the-u.s.-and-russia-indicted-in-new-york

Former CEO of Texas-Based Company Pleads Guilty to Being Russian Agent
http://www.wsj.com/articles/former-ceo-of-texas-based-company-pleads-guilty-to-being-russian-agent-1441828828

Texas Instruments, Xilinx Duped by Russia Export Ring, U.S. Says
http://www.bloomberg.com/news/articles/2015-09-25/texas-instruments-xilinx-duped-by-russia-export-ring-u-s-says

U.S. indicts 11 in alleged technology theft for Russia
http://articles.latimes.com/2012/oct/03/nation/la-na-russian-indict-20121004

Articles you Can't Afford to Miss

Three Chinese Nationals Arrested for Scheme to Steal and Illegally Export Military-Grade Semiconductors
http://www.justice.gov/usao-ct/pr/three-chinese-nationals-arrested-scheme-steal-and-illegally-export-military-grade

New York Man Who Supplied Falsely Remarked Computer Chips Used in U.S. Military Helicopters is Sentenced
http://www.justice.gov/usao-ct/pr/new-york-man-who-supplied-falsely-remarked-computer-chips-used-us-military-helicopters

Canada's counterfeit border protection measures - a status report
https://www.lexology.com/library/detail.aspx?g=a03cd0bf-6e04-4c29-9d2f-0ce07f370b58

Changing up the supply chain: DoD proposes to amend counterfeit electronic parts rule; finalizes national security system supply chain rule
http://www.lexology.com/library/detail.aspx?g=09a0db9c-39a7-4737-8551-571849b9b815

ES Components First Semiconductor Die Distributor to Receive AS6081 Certification
http://www.prweb.com/releases/2015/11/prweb13096085.htm

Testing for Counterfeits & Quality: The Rise of 3rd-Party Labs Fights Clones
http://www.ebnonline.com/author.asp?section_id=3785&itc=ebnonline_sitedefault&hootPostID=654534c22303c3ccc8987dd23f80e195&doc_id=279134&page_number=2

DFARS and Testing as the Quality Litmus Test, Part 1
http://electronicspurchasingstrategies.com/2015/11/05/dfars-and-testing-as-the-quality-litmus-test-part-1/

DFARS and Testing as the Quality Litmus Test, Part 2
http://electronicspurchasingstrategies.com/2015/11/05/dfars-and-testing-as-the-quality-litmus-test-part-2/

From Counterfeit Electronics to Clones: You Can't Afford to Ignore Them
http://www.ebnonline.com/author.asp?section_id=3788&doc_id=279089

Anti-Counterfeiting Update: DARPA's Chip and DoD's Revised Regulations
http://www.ttiinc.com/object/me-slovick-20151021.html

DFARS 2015: Zeitgeist or Bell Toll?
http://electronicspurchasingstrategies.com/2015/10/14/dfars-2015-zeitgeist-or-bell-toll/

Fake, Substandard Parts in American Airliners?
http://www.wealthdaily.com/articles/fake-substandard-parts-in-american-airliners/6294

Department of Defense Issues New Cybersecurity Rules for Defense Agencies That Use Contractors and Cloud Services to Hold Unclassified Defense Information
http://www.jdsupra.com/legalnews/department-of-defense-issues-new-72598/

AS6496 Anti-Counterfeit Standard is Taking Root
http://electronicspurchasingstrategies.com/2015/10/05/as6496-anti-counterfeit-standard-is-taking-root/