Machine Vision Pilot (MVP)
Counterfeit Microelectronics Policy Analysis

Prof. Patricia E. Campbell

Section 843 Machine Vision Pilot Program Report Generation and Policy Analysis (MVP)
Contract Number: HQ0727-19-P0030, CDRL A003
PWS No. DMEA 19-9E2
DMEA Project Engineer: Jeff Carlile, DMEA/MEXB

Submitted by: Center for Advanced Life Cycle Engineering (CALCE)

Department of Mechanical Engineering

University of Maryland, College Park

Principal Investigator: **Dr. Michael H. Azarian**

Research Scientist

Co-Principal Investigator: **Dr. Diganta Das**

Associate Research Scientist

Sub-Contractor (MVP):

University of Maryland Carey School of Law

University of Maryland Baltimore

Principal Investigator (sub-contract): **Prof. Patricia E. Campbell**

Director, Intellectual Property Law Program

Original Submission: November 30, 2020

Final Revision: December 22, 2020

Project Team

Principal and Co-Principal Investigators:

Dr. Michael H. Azarian, Dr. Diganta Das: CALCE, University of Maryland College Park

Prof. Patricia E. Campbell: University of Maryland Carey School of Law

Contributors from University of Maryland College Park:

Mr. Devon Richman, Mr. Jesse Hearn, Mr. Peter Kuffel, Mr. John Freal

Contributors from University of Maryland Carey School of Law:

Mr. George (Kenny) Eichelman, Ms. Kirsten Gallo, Mr. Jared MacKenzie, Mr. Troy Walker

I. Executive Summary

Section 843 of the 2019 National Defense Authorization Act (NDAA) (known as the "John S. McCain National Defense Authorization Act for Fiscal Year 2019") authorized funding to establish a "Pilot program to test machine-vision technologies to determine the authenticity and security of microelectronic parts in weapon systems." In order to accomplish this, the act provided that the Undersecretary of Defense for Research and Engineering work in coordination with the Defense Microelectronics Activity to establish the program, which was to be completed no later than December 30, 2020. The Defense Microelectronics Activity (DMEA) established two contracts to carry out the tasks identified in the 2019 NDAA §843: HQ0727-19-P0030 ("MVP") and HQ0727-19-C0008 ("MASER"). DMEA contracted the Center for Advanced Life Cycle Engineering (CALCE) at the University of Maryland at College Park to lead the pilot program under both contracts.

Under the contract titled "Section 843 Machine Vision Pilot Program Report Generation and Policy Analysis (MVP)" a policy analysis was conducted to identify potential impediments to effective implementation of existing laws and regulations, and to indicate steps that can enhance the effective application of such rules, regulations, or processes to mitigate counterfeit microelectronics proliferation throughout the DoD. It also identified the policy considerations and recommended actions necessary for Machine Vision to be implemented in counterfeit detection and authentication of electronic parts.

This policy analysis was sub-contracted to the University of Maryland Carey School of Law at the University of Maryland, Baltimore. The principal investigator on the sub-contract was Professor Patricia E. Campbell. The report that was authored by Prof. Campbell under the sub-contract was incorporated into the final report submitted to DMEA for both contracts and is reproduced herein in isolation from the sections concerning the pilot study.

Overview of Laws, Regulations, Policies, and Standards Relating to Counterfeit Electronic Parts

The laws, regulations, policies, and DoD Instructions relating to counterfeiting form a complex web of requirements for the DoD and its contractors and suppliers. DoD Instruction 4140.67 adopted a risk-based approach to reduce the frequency and impact of counterfeit materiel in DoD acquisition systems. The DFARS likewise requires CAS-covered contractors to establish and maintain an acceptable counterfeit electronic part detection and avoidance system, which must include risk-based policies and procedures that address at least 12 separate criteria, including inspection and testing of electronic parts. All contractors are responsible for inspection and testing when they obtain parts of questionable provenance. In addition, all contractors must have risk-based processes that enable tracking of electronic parts from the original manufacturer to product acceptance by the Government.

Inspection, testing, and authentication of electronic parts is to be carried out in accordance with applicable industry standards. Several standards provide guidance on testing and inspection procedures, including IDEA-STD-1010-B and the SAE family of standards. SAE AS6171A, in particular, provides a risk assessment model to quantify the level of risk associated with use of a part obtained from an unauthorized supplier, followed by recommended testing sequences based on a resulting risk score.

However, several challenges must be resolved. Actions by DoD are needed, including in some cases follow-on research efforts building on the current project, to address the following:

- An agreed-upon definition of "counterfeit" is needed. The DFARS, DoD Issuances, industry standards, and other laws provide conflicting definitions, and agreement needs to be reached on the criteria for identifying a counterfeit electronic part.
- A uniform, DoD-wide set of policies and procedures to address prevention, detection, and avoidance of counterfeiting is needed.
- Electronic parts should only be sourced from OCMs and authorized distributors or authorized remanufacturers unless there is no other choice. The provision in the DFARS allowing parts that are in production or currently available in stock to be obtained from "suppliers that obtain such parts exclusively from the original manufacturers of the parts or their authorized distributors" should be removed.
- Implementation of Section 818 of the FY 2012 NDAA should be completed, including issuance of regulations that establish qualification requirements pursuant to which DoD may identify approved suppliers.
- DoD should require compliance with the SAE AS6171 standards for risk-based testing to determine authenticity and reliability of electronic parts.
- GIDEP reporting of suspect counterfeit electronic parts should be required of all DoD contractors and should not be limited to contracts subject to higher-level quality standards, critical items, and acquisitions that exceed the SAT. The reporting window should be shortened, and contractors should be provided with guidance about the safe harbor for reports submitted in good faith.
- Integration of counterfeit microelectronic part preventions and avoidance strategies into a broader hardware assurance framework that addresses cyber-physical system security is needed. DoD should include tampered parts and clones in its approach to counterfeiting.
- Further evaluation of the civil and criminal trademark laws should be conducted to consider whether additional remedies and/or enhanced enforcement is needed.

Policy-related topics that are recommended for future study include the following:

- Debarment: what are the grounds for debarment, the duration of debarments, and are these effective as a deterrent? Previous debarments should be examined to determine what actions led to those debarments and whether different practices should be adopted to make debarment a more effective deterrent; for example, to what extent have suppliers been debarred due to sale of counterfeit parts as opposed to fraud or other reasons.
- GIDEP reporting: to what extent are counterfeit parts being reported as non-conforming, and what are the reasons that contractors or DoD components may prefer to avoid reporting parts as suspect counterfeit? GIDEP reports should be analyzed and subject matter experts within contractors and DoD components should be interviewed to gain insight into reporting practices and whether GIDEP reporting is serving the notice function that it was intended to serve. An analysis is needed to determine why alternative reporting platforms, such as ERAI, are preferred by some contractors, and what actions are needed to make GIDEP reporting more effective.
- Legislative intent and DoD and industry response regarding counterfeit prevention: how did the requirement to eliminate all counterfeits in the 2012 NDAA evolve into the use of risk-based methodologies for counterfeit avoidance? How did responses from contractors, industry associations, suppliers, and the legal community shape DoD's implementation of Congress's instructions in Section 818 of the 2012 NDAA?

II. Table of Contents

VIII. Task 4: Review of Applicable Laws, Regulations, Policies, and DoD Instructions Re: Machine Vision and the Counterfeit Threat (MVP A003)

Section 843 of the 2019 National Defense Appropriations Act required the Undersecretary of Defense for Research and Engineering, in coordination with the Defense Microelectronics Activity ("DMEA"), to establish a pilot program to test the feasibility and reliability of using machine vision technologies to determine the authenticity and security of microelectronic parts in weapon systems. In connection with that effort, they were required to evaluate the rules, regulations, and processes that hinder the development and incorporation of machine vision technologies, and the application of such rules, regulations, and processes to mitigate counterfeit microelectronics proliferation through the Department of Defense. This report provides the requested analysis.

The report was compiled by reviewing numerous statutes, rules, regulations, DoD issuances, industry standards, published court opinions, journal articles, press releases, and other publications relating to mitigation of counterfeit electronics in the DoD supply chain and/or to counterfeiting more generally. In addition, over 20 subject matter experts from industry and the DoD were interviewed between late 2019 and mid-2020.[1] Eight of those individuals have agreed to contribute a written interview summary in support of this report.[2] Many other individuals elected to remain anonymous and/or were unable to obtain permission from supervisors to contribute a written interview summary; their assistance was nevertheless invaluable in helping to frame the issues discussed herein.

A. OVERVIEW OF LAWS, REGULATIONS, POLICIES AND STANDARDS RELATING TO COUNTERFEIT ELECTRONIC PARTS

While there remains much disagreement about the definition of "counterfeit" microelectronics, SAE's standard AS6171A sets out seven recognized types of counterfeit parts.[3] They include recycled parts (a part that is reclaimed from a discarded system and then modified and misrepresented as a new, genuine part); remarked parts (a part from an authorized manufacturer where a legitimate marking has been replaced with a forged marking, such as a trademark, part number, or lot code, without authorization from the manufacturer); overproduced parts (a part from a contracted facility which was fabricated

[1] Appendix 21 contains a Counterfeit Subject Matter Expert Contact List. However, the list should not be viewed as a list of individuals who were interviewed or consulted during the preparation of this report.
[2] Appendix 19 contains summaries of interviews with Robert Bodemuller (Lockheed Martin); Dr. Brian Cohen (CyberTech Solutions, LLC; formerly of the Institute for Defense Analyses); Dan Deisz (Rochester Electronics); Robin Gray (Electronic Components Industry Association); Faiza Khan (Independent Distributors of Electronics Association); Andrew Olney (Analog Devices, Inc.); Kevin Sink (TTI, Inc.); and Richard Smith (ERAI, Inc.).
[3] SAE International, AS6171A, *Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts* (2018).

outside of the contract, also referred to as "overruns"); out-of-specification or defective parts (identified as nonconforming by the manufacturer); cloned parts (a reproduction that replicates an authentic part, without authorization from the manufacturer); forged documentation and/or substitution of an unauthorized part for the part identified in the shipping documents; and tampered parts which have been modified for sabotage or malfunction.[4]

Recycled
Remarked
Overproduced
Out-of-spec/Defective
Forged Documentation
Cloned
Tampered

Table 1: List of counterfeit Electrical, Electronic, and Electromechanical (EEE) part types.[5]

The nature of the counterfeiting problem is already well known to the U.S. Government. The DoD aptly described the risks posed by counterfeiting in a final rule that was recently published in the Federal Register:

> Counterfeits are not produced to meet higher-level quality standards required in mission critical applications and are a significant risk in causing failure to systems vital to an agency's mission. For weapons, space flight, aviation, and satellite systems, these failures can result in the [sic] death, severe injuries, and millions of dollars in system damage or loss. For example, if counterfeits are installed in a missile's guidance system, such missile may not function at all, may not proceed to an intended target, or may strike a completely unintended location resulting in catastrophic losses. Critical nonconforming and counterfeit items may cause failures in navigation or steering control systems, planes and flight control. Counterfeits can create "backdoors" into supposedly secure programmable devices which could be exploited to insert circuit functions to steal information and relay it to third parties or command or prevent the device from operating as designed. Defense, space, and aviation systems in particular must meet rigorous component specifications; failure of even a single one can be catastrophic causing serious problems and placing personnel and the public in harm's way.[6]

The Department of Homeland Security's Appendix to the U.S. Intellectual Property Enforcement Coordinator's Annual Intellectual Property Report to Congress for 2018 similarly observed:

> Counterfeiting is a significant challenge that can impair supply chains for both the public and private sectors. In the context of the U.S. Government, acquiring products or services from sellers with inadequate integrity, security, resilience, and quality assurance

[4] *Id.* at 7-9.
[5] Michael H. Azarian, *An Overview of Risk-Based EEE Counterfeit Part Detection Based on SAE AS6171,* Proceedings from the 44th International Symposium for Testing and Failure Analysis (ISTFA) (2018), at 2. Azarian notes that tampered parts are not included in the scope of AS6171A.
[6] 84 Fed. Reg. 64680, at 64681 (November 22, 2019).

> controls create significant risks, from a national security and mission assurance perspective as well as from an economic standpoint (due to the increased costs to American taxpayers). Counterfeiting can have particularly significant consequences for the Department of Defense (DoD) supply chain, by negatively affecting missions, the reliability of weapon systems, the safety of the warfighter, and the integrity of sensitive data and secure networks.[7]

DHS concluded that "[t]he goal is to reduce the risk of counterfeits entering the supply chain; quickly and collectively address those that do enter the supply chain; and strengthen remedies against those that supply counterfeit items."[8]

Explanations for the counterfeit electronics problem have long been discussed. Profit is clearly an important motivator for counterfeiters, but why are government contractors and suppliers particularly susceptible to purchasing counterfeit parts? A principle reason apparently relates to obsolescence of necessary replacement parts. Unlike commercial products such as cellphones and laptop computers, defense systems are often designed for extremely long life cycles. For example, the B-52 Stratofortress was first produced in 1954 and is expected to remain in service through the 2040s, and the F-16 Fighting Falcon, first produced in 1976, has no termination date.[9] Production of the parts contained in those systems may be discontinued long before the systems themselves are taken out of service, leading to diminishing manufacturing sources and material shortages ("DMSMS" issues). That is, parts may no longer be available from the original component manufacturer ("OCM") or an authorized distributor. If sufficient end-of-life purchases were not made,[10] the DoD and defense contractors may be forced to purchase replacement parts from outside the authorized supply chain, including from brokers and independent distributors.[11] Long manufacturing lead times have also been credited with pushing sellers to go to the open market to obtain parts for their customers, in order to ensure continued production.[12] Other factors include the military's past focus on lowest cost suppliers rather than quality of parts obtained.[13]

---

[7] United States Intellectual Property Enforcement Coordinator, *Annual Intellectual Property Report to Congress*, Appendix at 51 (February 2019).
[8] *Id*., Appendix at 51.
[9] Kirsten M. Koepsel, COUNTERFEIT PARTS AND THEIR IMPACT ON THE SUPPLY CHAIN (2d ed. 2019), at 28-29.
[10] A source explained that DoD attempts to purchase a lifetime supply of product for long life cycle systems, including through end-of-life buys, and it has stockpiles of parts in its warehouses. In addition, DoD traditionally purchased intellectual property rights along with parts or systems, so the IP would be available for future reference if needed. Interview with Anonymous Source (notes in possession of authors).
[11] Koepsel, *supra* note 9, at 29.
[12] Rob Spiegel, *Supply Chain* (March 3, 2011).
[13] *See* U.S. Dept. of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, *Defense Industrial Base Assessment: Counterfeit Electronics* (2010), at 157-58.

Traditionally, a major source of counterfeit parts was e-waste. Used parts were harvested from discarded products and resold as new, often after being relabeled and remarked with different date codes and performance characteristics. In a 2013 white paper, the Anti-Counterfeiting Task Force of the Semiconductor Industry Association described the typical "manufacturing process" for counterfeit components:

> 1. Using "mountains" of scrap electronics as an input, workers remove printed circuit boards (PCBs) from old electronic systems.
>
> 2. PCBs are heated over an open flame to melt the solder used to secure components to the boards. The boards are then banged against a hard surface so that the components will fall out into buckets. The components are then sorted, typically based on the package sizes and styles, and the electrical functions of the components.
>
> 3. The original markings on the components are removed using methods of increasing sophistication ranging from sanding to chemical etching to "black-topping" to "micro-blasting."
>
> 4. New markings, including trademarked OCM logos, are added to the components. These new markings generally are intended to make the parts more marketable and/or more expensive. For example, parts with old product codes may be marked with new product codes; packages that contain the element lead (Pb) may be marked to indicate they are lead-free (Pb-free); parts that have low performance may be marked to indicate they have high performance; and inexpensive commercial-grade parts may be marked to indicate they are more expensive automotive-grade or military-grade parts.
>
> 5. The external pins, pads, or solder balls on the packages are reworked to make them appear new. This sometimes entails using harsh chemicals to clean these external package connections.[14]

This stands in stark contrast to the ultra-clean, environmentally controlled, high tech wafer fabs where manufacturing of new semiconductor devices takes place.[15] Other counterfeiters may assemble packages with no die in them, or they remark used or new low-grade components to make them appear as high-grade components.[16] Some counterfeit parts may not function at all, while others may fail prematurely. "Even if counterfeits made from previously used parts and salvaged from e-waste may initially perform,

[14] Semiconductor Industry Association, Anti-Counterfeiting Task Force, *Winning the Battle Against Counterfeit Semiconductor Products* (2013), at 11, *citing* BUSINESS WEEK article and video (October 13, 2008), previously available at http://images.businessweek.com/ss/08/10/1002_counterfeit_narrated/index.htm.
[15] *Id.* at 9-11.
[16] *Id.* at 11.

there is no way to predict how well they will perform, how long they will last, and the full impact of failure."[17]

More recently, clones and tampered parts with malicious insertions have become part of the problem, leading to national security concerns. As described in a 2016 paper:

> One of the most advanced threats of EEE counterfeits are those that are considered "tampered." The SAE G-19A committee defines a tampered counterfeit part as "a part which has been modified for sabotage or malfunction." Parts of this category would likely be state sponsored by adversary countries and could have dangerous or catastrophic consequences for systems that incorporate them. Consequences include but are not limited to denial of service of a critical function of the system, side-channel attacks that enable loss of sensitive or critical information, premature or latent failure, or unauthorized access to proprietary data or system functionality.[18]

Dr. Brian Cohen, formerly of the Institute for Defense Analyses, explained that there are two types of clones: reverse engineering a product in order to duplicate it exactly, and form-fit-function equivalents passed off as authentic product.[19] Dr. Cohen indicated that in either case, if someone can clone a product, they are operating at a technology level beyond that of the original product, which means they can make the clone do things that the original product could not. While the clone might technically be a "conforming product" because it meets required specifications, it might also function in ways that the original product did not, which could be very dangerous. For example, a timer could be inserted that would cause the chip to fail at a certain time, or it could be programmed to fail in response to certain stimuli.[20]

Anonymous sources within the DoD have indicated that, while tampered parts and clones pose serious risks to national security and the safety of the warfighter, DoD does not necessarily view this category of risks as part of the counterfeiting problem. Instead, DoD continues to limit the focus of its anti-counterfeiting initiatives to traditional counterfeiting mechanisms, such as recycled parts sold as new, and it tends to view cyber physical security risks as a separate issue. One source described the DoD as very "siloed" in the way it approaches these problems. Another source explained that concerns about counterfeiting originally emerged in the community responsible for quality, and they focused on parts that either did not meet specifications or failed prematurely. They viewed counterfeiting as a criminal

---

[17] U. S. Senate, Committee on Armed Services, *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain* (2012), at 7.
[18] Daniel DiMase *et al.*, *Traceability and Risk Analysis Strategies for Addressing Counterfeit Electronics in Supply Chains for Complex Systems* (Society for Risk Analysis 2016), at 4-5.
[19] Dr. Brian Cohen Interview Summary (Appendix 19), at 2.
[20] *Id. See also* Dan Deisz Interview Summary (Appendix 19), at 4, n. 2. Mr. Deisz noted that counterfeiters could potentially insert random failures or data dependent failures into parts. He commented that the worst malicious insertion would be an unpredictable failure.

enterprise that undermined quality control. A different community within DoD is concerned about counterfeits resulting from malicious actions in the supply chain, including nation state actions to taint the supply chain and other bad actors such as disgruntled employees.[21]

Efforts to address these risks through counterfeit mitigation and prevention have included federal legislation imposing heightened requirements on government contractors and criminal penalties for counterfeiters who traffic in counterfeit military goods and services; DoD rules and regulations that require contractors to establish and maintain an acceptable counterfeit electronic part detection and avoidance system, as well as set out a three-tier hierarchy for sourcing electronic parts; and development of industry standards directed to inspection and testing protocols. The result is a complex network of laws, regulations, policies, procedures and standards, sometimes in conflict with one another, that appear to be only moderately successful in addressing the counterfeiting problem.

1. Federal Actions and Legislation

On December 31, 2011, President Barack Obama signed into law the National Defense Authorization Act for Fiscal Year 2012 ("FY 2012 NDAA). Section 818 of the FY 2012 NDAA,[22] entitled "Detection and Avoidance of Counterfeit Electronic Parts," instructed the Secretary of Defense to take numerous actions, including establishing department-wide definitions of "counterfeit electronic parts" and "suspect counterfeit electronic parts"; issuing guidance on implementing a risk-based approach to minimize the impact of counterfeits on the DoD; revising the Defense Federal Acquisition Regulation Supplement ("DFARS") to include several new provisions to address the detection and avoidance of counterfeit electronic parts; and implementing a program to enhance contractor detection and avoidance of counterfeit electronic parts. In addition, Section 818 amended 18 U.S.C. § 2320 ("Trafficking in counterfeit goods or services") to include provisions on trafficking in counterfeit military goods and services.

a. Events Leading Up to Enactment of FY 2012 NDAA

Section 818 was the result of a burst of activity beginning in 2008, including various reports, hearings, briefings and other discussions concerning the severe risks posed by the infiltration of counterfeit electronic parts into the defense supply chain. It is difficult to pinpoint the first incidence of counterfeit electronic parts in the military supply chain. Certainly, the DoD was already experiencing problems with counterfeit materiel and other non-electronic parts as early as the 1980s. An anonymous

[21] *But see,* Robert S. Metzger, *Convergence of Counterfeit and Cyber Threats: Understanding New Rules on Supply Chain Risk*, 101 FEDERAL CONTRACTS REPORT (Feb. 18, 2014).
[22] National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, 125 Stat. 1298 (2011) [hereinafter "FY 2012 NDAA"].

source from the DoD recalled a problem with counterfeit fasteners in the late 1980s,[23] which ultimately led to the enactment of the Fastener Quality Act of 1990.[24] A 1998 report by the Organization for Economic Co-Operation and Development (OECD) on "The Economic Impact of Counterfeiting" did not even recognize electronics or electronic parts as an item of concern, although the report did mention that counterfeit aircraft components were a problem.[25]

By 2001, the counterfeiting problem had expanded to include electronic parts. Richard Smith, Vice President of Business Development at ERAI, Inc. (an information services organization that maintains a database of suspect counterfeit and nonconforming electronic parts and high-risk suppliers), indicated that ERAI received its first report of a suspect counterfeit part at the end of 2001,[26] around the time that China joined the World Trade Organization.[27] According to ERAI's online Awareness Timeline,[28] ERAI received its first nonconforming part complaint on November 29, 2001, against 3A Century (a/k/a "Gold Advanced," a/k/a "JXJ"), a China-based distributor. The complaint described the product nonconformance as follows:

> Parts arrived in Samsung tubes (ordered TI parts [part number TCM3105DW]). Numerous mixed date codes arrived in a single tube. Solder splash present on part leads. There were 'wash marks' and smears on the upper surface of the chip.[29]

ERAI observed that "[w]ithin a few months, Chinese distributors began refurbishing and remarking parts to have consistent date and lot codes in order to pass used parts off as new."[30] By the spring of 2003, reports of counterfeit parts were also being filed with the Government-Industry Data Exchange Program ("GIDEP").[31] Shortly thereafter, the Secretary of Defense issued a memo entitled "Encouraging

---

[23] Interview with Anonymous Source (notes in possession of authors).
[24] *Id.*
[25] Organization for Economic Co-Operation and Development, *The Economic Impact of Counterfeiting* (1998), at 15. The report states that "there have been a number of incidents of aeroplane crashes caused by fake components." However, the term "components" apparently refers to items such as washers, bolts, nuts, and screws, not to electronic components.
[26] Richard Smith Interview Summary (Appendix 19), at 1.
[27] China became a member of the WTO on December 11, 2001. *See* World Trade Organization, *China and the WTO*, available at https://www.wto.org/english/thewto_e/countries_e/china_e.htm#:~:text=China%20has%20been%20a%20member%20of%20WTO%20since%2011%20December%202001.
[28] ERAI's website contains an extensive "Awareness Timeline" chronicling events in the history of counterfeiting, anti-counterfeiting legislation, development of industry standards, and criminal prosecutions for counterfeiting and related offenses. *See* https://www.erai.com/ca_awareness_timeline.
[29] *Id.*
[30] *Id.*
[31] See GIDEP Alert No. CE9-A-03-2 submitted by Texas Instruments, March 31, 2003 ("Texas Instruments has received notice of counterfeit devices bearing the TI trademark and part number being sold through various brokers who are not authorized TI distributors."); GIDEP Alert No. B8-A-03-01

Participation in the Trusted Foundry Pilot Program."[32] The memo recognized that counterfeits are not the only problem and mentioned backdoor threats as well.

i) Industry Took the First Steps to Address the Counterfeiting Problem

The industrial sector apparently took note of the counterfeit problem and started to act before it became a priority for the Government. Dan Deisz, Director of Design Technology at Rochester Electronics, recalled that counterfeiting came to the forefront when semiconductor companies started seeing returns from customers.[33] In 2007, the Semiconductor Industry Association ("SIA") formed an Anti-Counterfeiting Task Force to combat counterfeit chips,[34] and SAE International formed its G-19 Counterfeit Electronic Components Committee to respond to the threat of counterfeit electronic parts.[35] In the spring of 2007, ERAI issued a special report entitled "A Time for Change,"[36] following two investigative trips to China by its representatives in January 2004 and December 2006.[37] Also in 2007, the Organization for Economic Co-Operation and Development released a new report on "The Economic Impact of Counterfeiting and Piracy," which identified electrical components as a type of product subject to counterfeiting, thereby leading to concerns about quality and safety.[38] In 2008, the Aerospace Industries Association ("AIA") created a Counterfeit Parts Integrated Project Team in an effort to engage the government in discussions about policies to avoid introduction of counterfeit parts into aerospace and defense products, and to create a set of standards to "ensure that the risk of introducing counterfeit parts and materials is minimized without sacrificing the benefits of buying commercially available parts."[39]

---

submitted by Textron Systems, April 15, 2003 ("Textron Systems has experienced a high failure rate of parts marked LT1097S8 with a date code of 0103 and a Linear Technology Corp. logo. Four parts were returned to Linear Technology Corp (LTC) for failure analysis. LTC has informed Textron Systems that the parts are counterfeit. Textron Systems had purchased the parts through a distributor that was not franchised by LTC.").

[32] DOD Assured Microelectronics Policy (January 2004).

[33] Dan Deisz Interview Summary (Appendix 19), at 4.

[34] Semiconductor Industry Association, *History*, available at https://www.semiconductors.org/about/history/.

[35] SAE Aerospace, Committee Charter, SAE G-19 Counterfeit Electronic Components Committee (Nov. 2007). Mr. Deisz from Rochester Electronics explained that representatives of Intel, Texas Instruments, Analog Devices, and a few other companies met to compare notes and potentially influence policy. *See* Dan Deisz Interview Summary (Appendix 19), at 4.

[36] Kristal Snider, *A Time for Change: The Not So Hidden Truth*, available at https://www.erai.com/CustomUploads/ca/timeline/A_Time_For_Change.pdf.

[37] ERAI, Inc., *Awareness Timeline*, available at https://www.erai.com/ca_awareness_timeline.

[38] Organization for Economic Co-Operation and Development, *The Economic Impact of Counterfeiting and Piracy*, at 12, 19 (2007).

[39] Aerospace Industries Association, *Counterfeit Parts: Increasing Awareness and Developing Countermeasures,* Appendix (*AIA Counterfeit Parts Integrated Project Team Statement, April 2008)* (2001), at 24.

AIA's Counterfeit Parts Integrated Project Team issued a report in March 2011, in which it proposed a new definition of "counterfeit part": "Counterfeit parts are defined as a product produced or altered to resemble a product without authority or right to do so, with the intent to mislead or defraud by presenting the imitation as original or genuine."[40] AIA made numerous suggestions intended to reduce the risk of counterfeit parts from entering the supply chain, relating to nine different areas of discussion. For example, AIA recommended that industry members adopt SAE's AS5553 standard, and it encouraged industry and government to create an Approved Suppliers List of vetted distributors who have processes in place to mitigate the risk of receiving, storing, and shipping counterfeit devices. It recommended reporting counterfeits into a database such as GIDEP, and it requested the government to develop guidance on proper disposition of known or suspected counterfeit parts. AIA also recommended that industry and government take proactive steps to deal with component obsolescence; that companies develop counterfeit parts control plans to document processes used for avoidance, detection, disposition, and reporting of counterfeit parts; and that government and industry develop best practices for recycling of e-waste.[41]

ii) Government Action Started Later

Although industry became aware of the counterfeiting problem in the mid-2000's, it appears that the Government was slower to respond to the risk. An anonymous source recalled attending a briefing at NASA in 2006 or 2007, where the source learned that NASA was experiencing problems with counterfeit parts coming from China. Although the source reported this to source's DoD component, it was not interested in becoming involved in counterfeiting issues at that point. Nevertheless, the source described the period 2007 to 2010 as the "heyday of counterfeiting," when there was an extreme infiltration of counterfeits into the DoD supply chain.[42]

In June 2007, the U.S. Department of the Navy, Naval Air Systems Command (NAVAIR) asked the Bureau of Industry and Security (BIS) Office of Technology Evaluation (OTE) to conduct a defense industrial base assessment of counterfeit electronics. The resulting report, issued in January 2010, indicates that "NAVAIR suspected that an increasing number of counterfeit/defective electronics were infiltrating the DoD supply chain and affecting weapon system reliability," which could "complicate the

[40] *Id.* at 10.
[41] *Id.* at 12-22. See also, Henry Livingston, *Securing the DOD Supply Chain from the Risks of Counterfeit Electronic Components: Recommendations on Policies and Implementation Strategy,* BAE Systems (2010) (proposing numerous policy and implementation strategy considerations for addressing the infiltration of counterfeit parts into the DoD supply chain).
[42] Interview with Anonymous Source DoD (notes in possession of authors).

Navy's ability to sustain platforms with extended life-cycles and maintain weapons systems in combat operations."[43]

Another source from the DoD reported that in 2009, DoD, the Defense Contract Management Agency, and the Defense Logistics Agency ("DLA") finally began to recognize the severity of the counterfeit electronics problem. By this time, the source believes there was extreme infiltration of counterfeits into DoD supply chain, probably a direct result of China recycling significant quantities of e-waste and knowing that DoD needed to acquire obsolete parts. Nevertheless, the source felt that little happened in DoD from 2009 to 2011, because the Office of the Secretary of Defense did not think this was their problem and they were trying to push responsibility onto DLA and the Services.[44]

In January 2010, the Department of Commerce Bureau of Industry and Security ("BIS") issued its *"Defense Industrial Base Assessment: Counterfeit Electronics"* report.[45] The Introduction to the report stated that its purpose was "to provide statistics on the extent of infiltration of counterfeit electronic components into United States industrial and defense supply chains, to understand how different segments of the supply chain currently address the issue, and to gather best practices from the supply chain on how to handle counterfeits."[46] For purposes of the report, BIS defined a "counterfeit" as "an electronic part that is not genuine because it:

- is an unauthorized copy;
- does not conform to original OCM design, model, and/or performance standards;
- is not produced by the OCM or is produced by unauthorized contractors;
- is an off-specification, defective, or used OCM product sold as "new" or working; or
- has incorrect or false markings and/or documentation."[47]

BIS conducted five surveys of government and industry, on the basis of which it made a number of general findings. The surveys disclosed that no type of company or organization was untouched by counterfeit electronic parts, and even the most reliable sources had counterfeit parts in their inventories.[48]

---

[43] U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, *Defense Industrial Base Assessment: Counterfeit Electronics* (January 2010), at i.
[44] Interview with Anonymous Source (notes in possession of authors).
[45] U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, *Defense Industrial Base Assessment: Counterfeit Electronics,* https://www.bis.doc.gov/index.php/documents/technology-evaluation/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010/file [hereinafter "Defense Industrial Base Assessment"].
[46] *Id.* at 1. The report stated that it was intended to replace anecdotal information within the U.S. Navy and other governmental and industry organizations with concrete data on the impact and pervasiveness of counterfeit electronics within the U.S. supply chain.
[47] *Id.* at 3. The report noted that the definition of counterfeit parts used was specific to the study and was broader than definitions typically used by industry. *Id.*, n.2.
[48] *Id.* at 7.

Nevertheless, there was a lack of dialogue about counterfeits between all organizations in the U.S. defense supply chain.[49] Most organizations assumed that other parties in the supply chain were testing parts, and therefore they conducted little testing themselves.[50] There was a lack of traceability in the supply chain, as well as insufficient accountability within organizations and limited record keeping on counterfeit incidents.[51] Further, few organizations understood legal requirements and liabilities relating to counterfeits, and few knew what legal or other authorities to contact about counterfeit parts.[52] The report determined that stricter testing protocols and quality controls were needed by contractors and suppliers, and DoD organizations needed additional procurement and testing protocols to prevent counterfeit parts from entering their supply chain.[53] A number of best practices were recommended, including buying parts directly from OCMs and authorized distributors, not from brokers, independent distributors, or the gray market.[54]

BIS's Defense Industrial Base Assessment survey asked DoD organizations a series of questions about the DFARS and what changes should be made to address infiltration of counterfeit parts. The responses indicated that existing DFARS provisions promoted "a procurement system that favors the lowest price items rather than the best overall value."[55] The report observed that, "[w]hile such a system can be very cost effective, it can also allow price to dictate suppliers and increase the risk of counterfeit incidents."[56] DoD organizations felt the DFARS should be modified to reduce the emphasis on small business considerations and lowest bidder, and instead allow organizations to select suppliers based on "best value."[57] According to the report, many DoD organizations felt the DFARS "forces those who are responsible for procuring piece parts to buy from unauthorized distributors or independent sources."[58]

Most DoD organizations felt the DFARS was inadequate to address the counterfeit problem because it did not specifically discuss counterfeit electronics.[59] At that time, counterfeit parts were simply treated as nonconforming items, and the terms "counterfeit" and "nonconforming" were often used

[49] *Id.* at 5.
[50] *Id.* at 6.
[51] *Id.* at 6.
[52] *Id.* at 6-7.
[53] *Id.* at 7.
[54] *Id.* at 198. Other recommendations included establishing a list of trusted suppliers, visual inspection and component testing of parts, and requiring suspect and confirmed counterfeit parts to be quarantined to prevent accidental sale or use. *See id.* at 200-206.
[55] *Id.* at 157.
[56] *Id.* at 157.
[57] *Id.* at 157.
[58] *Id.* at 157.
[59] *Id. at 157.*

interchangeably. The FAR defined three specific types of nonconformance: critical, major, and minor.[60] A "critical nonconformance" refers to "a nonconformance that is likely to result in hazardous or unsafe conditions for individuals using, maintaining, or depending upon the supplies or services; or is likely to prevent performance of a vital agency mission." A "major nonconformance" means "a nonconformance, other than critical, that is likely to result in failure of the supplies or services, or to materially reduce the usability of the supplies or services for their intended purpose." A "minor nonconformance," on the other hand, means "a nonconformance that is not likely to materially reduce the usability of the supplies or services for their intended purpose, or is a departure from established standards having little bearing on the effective use or operation of the services or supplies."[61] The seriousness of the nonconformance determined DoD's response. If a nonconformance was critical or major, the contracting officer would ordinarily reject the supplies; if a nonconformance was minor, the contract administration office could determine whether to accept or reject.[62] Neither the FAR nor DFARS contained any provisions addressing "nonconforming" electronic parts or requiring specific inspection, testing, or traceability.

The BIS report concluded with a number of specific recommendations for the U.S. Government, including the following:

- Establish a centralized federal reporting mechanism and database for collecting information on suspect and confirmed counterfeit electronic parts;
- Clarify the criteria in the FAR and DFARS "to promote the ability to award electronic parts contracts on the basis of "best value" rather than on the basis of "lowest price" or "low bid";
- Issue clear legal guidance on various issues, including civil and criminal liabilities for selling or dealing in counterfeit electronic parts, requirements for quarantining suspect and confirmed counterfeit parts, and appropriate contacts at the FBI for reporting suspected criminal activity relating to counterfeiting;
- Establish a dialogue with law enforcement on the potential need to increase prosecution of counterfeiters;
- Establish a government data repository of electronic parts information and for disseminating best practices for counterfeit mitigation, including identifying industry or federal standards for parts procurement and testing;
- Develop appropriate international agreements; and

[60] 48 C.F.R. § 101 (eff. June 4, 1996).
[61] *Id.*
[62] 48 C.F.R. § 407(c)(1), (d) (eff. June 4, 1996).

- Address issues relating to procurement of obsolete parts, such as improved forecasting of future requirements and timely end-of-life notices when manufacturers planned to cease production of parts.[63]

Also in 2010, the Government Accountability Office ("GAO") published two reports relating to the risks posed by counterfeiting. In its report on the Defense Supplier Base, GAO observed, "DOD is limited in its ability to determine the extent to which counterfeit parts exist in its supply chain because it does not have a department wide definition of the term "counterfeit" and a consistent means to identify instances of suspected counterfeit parts."[64]

iii) Senate Armed Services Committee Investigation

In March 2011, the Senate Armed Services Committee initiated an investigation into counterfeit electronic parts in the DoD supply chain. The investigation:

> uncovered overwhelming evidence of large numbers of counterfeit parts making their way into critical defense systems. It revealed failures by defense contractors and DOD to report counterfeit parts and gaps in DOD's knowledge of the scope and impact of such parts on defense systems. The investigation exposed a defense supply chain that relies on hundreds of unvetted independent distributors to supply electronic parts to some of our most sensitive defense systems. And, it found overwhelming evidence that companies in China are the primary source of counterfeit electronic parts in the supply chain.[65]

The Committee's report reached several conclusions, including (a) reliance on unvetted independent distributors created unacceptable risks to national security and to the safety of military personnel; (b) weaknesses in the testing regime and wide disparities in testing for electronic parts create vulnerabilities that are exploited by counterfeiters; (c) suspected counterfeit parts were not being reported to the DoD or criminal authorities; and (d) permitting contractors to recover costs incurred as a result of their own failure to detect counterfeits does not encourage the adoption of aggressive counterfeit avoidance and detection programs.[66]

The Senate Armed Services Committee reported that "[m]uch of the material used to make counterfeit electronic parts is electronic waste or "e-waste" shipped from the United States and the rest of the world to China."[67] E-waste was being disassembled by hand, washed in dirty rivers, and then dried on

---

[63] *Id.* at 209-11.
[64] U.S. Government Accountability Office, *Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts*, GAO-10-389 (2010) , at i.
[65] Committee on Armed Services, United States Senate, *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain* (Report 112-167) (2012) , at i [hereinafter "Senate Armed Services Committee Report"].
[66] *Id.* at vi-vii.
[67] *Id.* at 5.

city sidewalks. Date codes on the parts were frequently changed to make them appear new, and other false markings were also placed on the parts.[68] In other instances, blank chips were being manufactured, and counterfeit markings were later added as needed.

However, the Committee learned that did not mean that counterfeiters were unsophisticated or that counterfeit parts were easily identified. At a public hearing on November 8, 2011, Thomas Sharpe of SMT Corporation testified that "[m]any of the current counterfeiting techniques are already beyond the in-house detection capabilities of most open-market suppliers."[69] Similarly, Vivek Kamath, Raytheon's Vice President of Supply Chain Operations, stated:

> [W]hat keeps us up at night is the dynamic nature of this threat because by the time we've figured out how to test for these counterfeits, they've figured out how to get around it. And it's literally on almost a daily basis they change and the sophistication of the counterfeiting is amazing to us. We're finding out that you have to go down to the microns to be able to figure out that it's actually a counterfeit.[70]

While the Senate Armed Services Committee investigation was ongoing, Committee Chairman Carl Levin and Ranking Member John McCain proposed an amendment to the FY 2012 NDAA to address the problem of counterfeit electronic parts in the defense supply chain.[71] The proposed amendment was intended "to address weaknesses in the defense supply chain and to promote the adoption of aggressive counterfeit avoidance practices by DOD and the defense industry."[72] The amendment had several objectives, including reducing the risk of acquiring counterfeit parts by ensuring that, whenever possible, parts were purchased only from manufacturers, authorized distributors, and trusted suppliers; establishing policies and procedures for inspection and testing of electronic parts; requiring reporting of counterfeit parts to the government; and strengthening the incentive to avoid and detect counterfeit electronic parts by disallowing the recovery of costs of counterfeit parts and any repair or remediation required as a result of their use.[73] The committee's written report was published on May 21, 2012, shortly after the enactment of the FY 2012 NDAA, and it contained detailed explanations of what Congress hoped to achieve through that legislation.[74]

---

[68] *Id.* at 6.
[69] *Id.* at 7, *citing* Senate Armed Services Committee Hearing at 17.
[70] Senate Armed Services Committee Report, at 7, *citing* Committee Staff interview with Vivek Kamath, at 11 (October 6, 2011).
[71] *Id.* at 66. The proposed amendment became Section 818 of the FY 2012 NDAA, discussed *infra*. At approximately the same time, DoD Instruction 4140.01: DoD Supply Chain Materiel Management Policy issued.
[72] U.S. Senate Committee on Armed Services, Press Release: *Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts*, at 2 (May 21, 2012).
[73] Senate Armed Services Committee Report, at 66.
[74] *See id. at* 66-72.

b. FY 2012 NDAA Section 818

In December 2011, Congress passed the FY 2012 NDAA, and it was signed into law by President Barack Obama on December 31, 2011.[75] In addition to authorizing $662 billion in funding, the FY 2012 NDAA included Section 818, an effort at providing comprehensive legislation to address weaknesses in the DoD supply chain and prevent continued infiltration of counterfeit electronic parts.[76] Section 818 instructed the Secretary of Defense to conduct an assessment of DoD acquisition policies and systems for the detection and avoidance of counterfeit electronic parts[77] and, within 180 days after enactment of the Act, to take certain actions within the DoD. Specifically, the Secretary was required to establish Department-wide definitions of "counterfeit electronic parts" and "suspect counterfeit electronic parts,"[78] and those definitions were required to include "previously used parts represented as new."[79] The Secretary was also instructed to issue or revise guidance on two major topics: (1) implementing a risk-based approach to minimize the impact of counterfeits on the DoD, including requirements for training personnel, making sourcing decisions, ensuring traceability of parts, inspecting and testing parts, reporting and quarantining counterfeits, and taking corrective actions;[80] and (2) remedial actions to be taken where a supplier has repeatedly failed to detect and avoid counterfeit electronic parts or failed to exercise due diligence in detecting and avoiding counterfeits, including consideration of whether the supplier should be suspended or debarred until it has effectively addressed the issues leading to those failures.[81] In addition, the Secretary was instructed to establish processes for ensuring that DoD personnel submit a report to GIDEP within 60 days after becoming aware of (or having reason to suspect) that any end item, component, part or materiel contained in supplies purchased by or for the DoD contains

---

[75] National Defense Authorization Act for Fiscal Year 2012, Public Law 112-81, 125 Stat. 1298 (December 31, 2011).
[76] The Act defined an "electronic part" as "an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly. *See* FY 2012 NDAA § 818(f)(2). However, developing definitions of "counterfeit electronic part" and "suspect counterfeit electronic part" was delegated to the Secretary of Defense. *See* FY 2012 NDAA § 818(b)(1).
[77] FY 2012 NDAA § 818(a).
[78] The Senate Armed Services Committee Report noted that on December 14, 2011, while the 2012 NDAA conference report was being debated in Congress, the DoD issued Department of Defense Instruction 4140.01 (Supply Chain Materiel Management Policy). DODI 4140.01 defined "counterfeit materiel" as "materiel whose identity or characteristics have been deliberately misrepresented, falsified, or altered without the legal right to do so." Committee on Armed Services, U.S. Senate, *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain,* at 66 n. 496 (2012), *citing* Department of Defense, *Instruction 4140.01: DOD Supply Chain Materiel Management Policy,* at 17 (2011).
[79] FY 2012 NDAA § 818(b)(1).
[80] *Id.* at § 818(b)(2).
[81] *Id.* at § 818(b)(3).

counterfeit electronic parts or suspect counterfeit electronic parts.[82] Finally, the Secretary was required to establish a process for analyzing, assessing, and acting on reports of counterfeit electronic parts and suspect electronic parts submitted to GIDEP.[83]

In addition to actions internal to the DoD, the Secretary was also ordered to make substantial revisions to the DFARS to address the detection and avoidance of counterfeit electronic parts, including contractor responsibilities, use of trusted suppliers, and creation of a reporting requirement.[84] Under these new regulations, covered contractors[85] who supply electronic parts or products that include electronic parts would be responsible for detecting and avoiding the use or inclusion of counterfeit electronic parts or suspect counterfeit electronic parts in those products, as well as any rework or corrective action that may be required to remedy the use or inclusion of those parts.[86] Further, the regulations were to provide that the cost of counterfeit electronic parts and suspect counterfeit electronic parts, as well as the cost of rework or corrective action that may be required to remedy the use or inclusion of those parts, would not be allowable costs under DoD contracts.[87]

The revised regulations envisioned by Section 818 were also expected to contain provisions requiring the use of "trusted suppliers."[88] That is, the regulations were to require that, whenever possible, the DoD and its contractors and subcontractors at all tiers should:

> (i) obtain electronic parts that are in production or currently available in stock from the original manufacturers of the parts or their authorized suppliers, or from trusted suppliers who obtain such parts exclusively from the original manufacturers of the parts or their authorized dealers; and

---

[82] *Id.* at § 818(b)(4).
[83] *Id.* at § 818(b)(5).
[84] *Id.* at § 818(c).
[85] A "covered contractor" has the meaning given that term in § 893(f)(2) of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011. *See id.* at § 818(f)(1). That is, a "covered contractor" is 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 contractors are sometimes referred to as "CAS" contractors.
[86] *Id.* at § 818(c)(2)(a).
[87] *Id.* at § 818(c)(2)(b).
[88] In its Report, the Senate Armed Services Committee clearly stated that these provisions were "aimed at eliminating DOD and defense industry purchases of electronic parts from unknown or suspect suppliers." The Committee's investigation determined that the risk of obtaining counterfeit parts in the independent distribution market is significantly higher than from an OCM or authorized distributor, and that conclusion held true for both parts in production and parts that were either out of production or not readily available in stock. As a result, the FY 2012 NDAA was written to require the Secretary to issue regulations requiring DOD, defense contractors and subcontractors to buy from "trusted suppliers" that can be reviewed and audited by DOD. DOD was to have responsibility for establishing qualification requirements for trusted suppliers that ensure they have appropriate policies and procedures in place to detect and avoid counterfeit electronic parts. *See* Senate Armed Services Committee Report at 68-69.

(ii) obtain electronic parts that are not in production or currently available in stock from trusted suppliers.[89]

The regulations would also establish requirements for notification of the DoD, as well as inspection, testing, and authentication, if electronic parts were obtained from any other source.[90] Although the term "trusted suppliers" was not defined in the Act, the new DFARS provisions were to include qualification requirements pursuant to which the DoD would identify trusted suppliers that have appropriate policies and procedures in place to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts.[91] DoD contractors and subcontractors could also identify and use additional trusted suppliers, provided that their standards and processes for identifying additional trusted suppliers comply with established industry standards, and the contractor or subcontractor assumed responsibility for the authenticity of parts provided by those suppliers.[92] The DoD would also have the right to review and audit the selection of additional trusted suppliers by its contractors and subcontractors.[93]

A third area to be addressed by the new DFARS regulations would impose GIDEP reporting requirements on contractors.[94] Specifically, Congress instructed that the regulations should require that any DoD contractor or subcontractor must report in writing to GIDEP within 60 days if they became aware (or had reason to suspect) that any end item, component, part, or material contained in supplies purchased by the DoD, or purchased by a contractor or subcontractor for delivery to the DoD, contained counterfeit electronic parts or suspect counterfeit electronic parts.[95] In order to address concerns raised by contractors, the Act stated that a contractor or subcontractor that provides a GIDEP report would not be subject to civil liability on the basis of such reporting, provided that 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.[96]

Finally, Section 818 instructed the Secretary of Defense to implement a program to enhance contractor detection and avoidance of counterfeit parts, not later than 270 days after enactment of the

[89] FY 2012 NDAA § 818(c)(3)(A).
[90] *Id.* at § 818(c)(3)(B).
[91] *Id.* at § 818(c)(3)(C).
[92] *Id.* at § 818(c)(3)(D).
[93] *Id.* at § 818(c)(3)(D)(iii).
[94] These provisions reflect the Senate Armed Services Committee's conclusion that the defense industry routinely failed to report cases of suspect counterfeit parts, thereby putting the integrity of the defense supply chain at risk. *See* Senate Armed Services Committee Report at vii, 70-71.
[95] FY 2012 NDAA § 818(c)(4).
[96] *Id.* at § 818(c)(5).

Act.[97] The new program was required to include several elements at the contractor level.[98] Section 818 stated that the program shall require covered contractors[99] that supply electronic parts or systems containing electronic parts to establish policies and procedures to eliminate counterfeit parts from the defense supply chain, which must address the following:

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;
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.[100]

The program was further required to establish processes for review and approval of those contractor systems, and the Act instructed that the review processes should be comparable to those established for contractor business systems under Section 893 of the FY 2011 NDAA.[101]

In addition, Section 818 called for creation of an inspection program by the Secretary of Homeland Security,[102] intended to provide enhanced targeting of electronic parts imported from another country, and the sharing of information appearing on imported goods with trademark owners by the Treasury Department.[103] Finally, Congress amended 18 U.S. Code § 2320 to include provisions on trafficking in counterfeit military goods or services.[104]

---

[97] *Id.* at § 818(e).
[98] The provisions on testing were apparently included to address the Senate Armed Services Committee's investigation, which "identified wide disparities in testing protocols used by DLA and companies in the defense supply chain." The Report noted that while some companies require a wide range of testing to determine authenticity of parts, others were willing to accept parts that were only subjected to basic testing. *See* Senate Armed Services Committee Report at 69.
[99] Note that the program requirements were only directed at contractors, not subcontractors. *See* FY 2012 NDAA § 818(e)(2)(A).
[100] *Id.* at § 818(e)(2)(A)(i)-(ix).
[101] *Id.* at § 818(e)(2)(b), referencing the Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Public Law 111-383, § 893, 124 Stat. 4311 (2010).
[102] *See* FY 2012 NDAA § 818(d).
[103] *See id.* at § 818(g).
[104] *See id.* at § 818(h).

c. Reactions to FY 2012 NDAA

Numerous organizations expressed reactions to Section 818, including contractors and subcontractors, industry associations, and the legal community. The American Bar Association's Section of Public and Contract Law released a white paper in October 2012 that provided extensive comments about Section 818 and its implementation in new regulations. The ABA highlighted the lack of a uniform legal definition of the terms "counterfeit part" and "suspect counterfeit part," and it noted that the terms vary depending upon the parties involved.[105] For example, although the DoD had issued guidance that included a definition of "counterfeit materiel," it was unclear whether gray market items were included within that definition.[106]

The ABA also expressed concern about how onerous some of Section 818's requirements might be for suppliers and contractors. For example, Section 818 required the use of "trusted suppliers," but there was a lack of clarity about how trusted suppliers were to be identified. The white paper suggested that DoD must define what would constitute a "trusted supplier" and identify the standards and processes that contractors needed to follow in order to qualify suppliers as trusted suppliers. It stated:

> If these requirements are too onerous, needed suppliers might refuse to participate, making certain parts potentially inaccessible to DoD. If trusted suppliers will be expected to assume full responsibility for the costs of parts they supply and the unknowable costs of any rework or corrective action, there will be few companies, and likely no responsible small businesses willing to accept liability that exceeds so substantially the costs of the parts they are supplying. In engaging in the development of this guidance, DoD should undertake a risk-based assessment with input from Industry, identifying where the critical issues arise and what is needed to address them effectively and efficiently.[107]

The ABA raised additional concerns about the potential burden imposed by requiring contractors and subcontractors to notify DoD when they source electronic parts from an entity other than the OCM, an authorized dealer, or a trusted supplier. They observed:

> Requirements that are too onerous likely will prompt commercial and other suppliers to re-evaluate their continued participation in the government supply chain. Loss of these suppliers and contractors could negatively impact the defense industrial base, drive up

[105] American Bar Association Section of Public Contract Law, Committee on Acquisition Reform and Emerging Issues, Task Force on Counterfeit Parts, *A White Paper Regarding Department of Defense Implementation of Section 818 of the National Defense Authorization Act for Fiscal Year 2012* (2012), at 14.
[106] *Id.* at 14-15.
[107] *Id.* at 18.

> costs of obtaining the supplies, and potentially render it difficult or impossible to obtain needed supplies on a timely basis.[108]

Questions were also raised about the requirement for traceability of parts. The white paper observed that it is "probably not feasible to expect every electronic component in every item of supply to be traceable back to its original source." As a result, "[i]t is important to identify which items need to be traced before they are purchased. A risk-based approach to this issue makes the most sense."[109]

Another area commented on by the ABA related to the reporting requirements contained in Section 818, including reporting to "appropriate Government authorities" and GIDEP. The white paper suggested that it was important to consider "what information a party is to report, to whom a party is to report, the method by which the report is to be made, and what is to be contained in the report."[110] For instance, mandatory reporting to GIDEP could be problematic because not all contractors or subcontractors were able to participate, and the GIDEP system contained export-controlled data that could not be shared with companies outside the U.S. or Canada. These factors could "undermine a legislative aim to abolish counterfeits by depriving contractors and subcontractors who cannot access GIDEP from access to data that would help them avoid purchasing counterfeit parts from known or unknowable sources."[111] The white paper also suggested that, although Section 818 provided that contractors which reported to GIDEP would be immune from civil liability, "the entire procurement community would benefit from clarification as to both the degree of investigation needed to trigger the reporting obligation and the associated immunity."[112]

Other commentators voiced similar concerns about the burdens imposed by Section 818 and whether they would force small businesses to exit the DoD supply chain. One observed:

> Costs of detection, avoidance and elimination of counterfeits will impose both non-recurring and recurring expense. Customers rarely will volunteer to pay higher prices to cover those costs. More likely, higher tier customers will flow down new demands and controls, and insist that suppliers absorb costs and risks. This will cause considerable hardship on middle and lower tiers of the supply chain, and may cause some number of firms to exit the defense market rather than absorb unrecoverable new costs or assume enterprise risks.[113]

---

[108] *Id.* at 19.
[109] *Id.* at 31.
[110] *Id.* at 24.
[111] *Id.* at 25.
[112] *Id.*
[113] Robert S. Metzger, *Counterfeit Parts: What to do Before the Regulations (and Regulators) Come? Practical Steps Industry Can Take Now,* 98 FEDERAL CONTRACTS REPORT 246 (2012), at 7. Metzger also suggested that commercial device suppliers may decide that "the hazards and costs of compliance

Other considerations related to a lack of instruction about what a contractor should do (and at whose expense) when no genuine part was available from an OCM, authorized distributor, or trusted supplier. Would the government assume financial responsibility if a redesign was required or if a limited production of surrogate parts had to be obtained from a contract manufacturer?[114]

Others apparently questioned the overall fairness of Section 818: "Section 818 places the entire burden of eliminating counterfeit electronic parts on industry. . . . [T]he costs of counterfeit parts and the costs of rework and corrective action are unallowable, even if the contractor conducted adequate testing of the parts and was unaware that the parts were counterfeit when they were installed in the product."[115] It was noted that such costs were unallowable even when the contractor obtained the parts from the Government itself.[116]

d. DLA's DNA Marking Program

Shortly after the enactment of the FY 2012 NDAA, DLA introduced a new authentication marking requirement for electronic microcircuits in FSC 5962.[117] On October 31, 2012, DLA announced that all suppliers that provide electronic microcircuits to DLA would be required to provide items marked with a botanical DNA taggant.[118] An anonymous source indicated that the DNA marking program started as a research project with Applied DNA Sciences,[119] but it was quickly implemented even though it was still in the research phase. However, OCMs objected to the program and claimed that use of the DNA taggant would void the manufacturer's warranty on the electronic parts. The source observed that in order for the program to be successful, acceptance by all manufacturers would be critical. Ideally, each

---

with Section 818 do not justify continuing to do business with companies in the U.S. defense supply chain."

[114] Robert S. Metzger, *Counterfeit Electronic Parts: What to do Before the Regulations (and Regulators) Come? Part 1: New Requirements,* 98 FEDERAL CONTRACTS REPORT (June 21, 2012), at 7.

[115] Shawn Cheadle, Christopher W. Myers, and Kelly P. Garehime, *Counterfeit Parts and the New Law: Are We All DoD Contractors?,* 32 ACC DOCKET 42, 44 (2014).

[116] Robert S. Metzger, *Counterfeit Parts: What to do Before the Regulations (and Regulators) Come? Practical Steps Industry Can Take Now,* 98 FEDERAL CONTRACTS REPORT 246 (August 21, 2012), at 7.

[117] FSC 5962 refers to Federal Supply Class 5962 (Microcircuits, Electronic). The Federal Supply Classification system is a commodity classification system designed to serve the functions of supply and management and claims to be sufficiently comprehensive in scope to permit the classification of all items of personal property. *See* https://www.dla.mil/Portals/104/Documents/DispositionServices/Receiving/Usable/DISP_h2book[1].pdf.

[118] CISION PR Newswire, *Defense Logistics Agency requires DNA marking to combat counterfeit parts* (October 31, 2012), available at https://www.prnewswire.com/news-releases/defense-logistics-agency-requires-dna-marking-to-combat-counterfeit-parts-176623411.html.

[119] *See* Applied DNA Sciences, *DNA Marking and Authentication: A unique, secure anti-counterfeiting program for the electronics industry* (November 2011), available at https://www.dla.mil/Portals/104/Documents/LandAndMaritime/V/VA/PSMC/Nov11/LM_DNAMarkingAndAuthentication_151030.pdf.

manufacturer would have its own DNA mark, which should be applied in-house at the end of the manufacturing process.[120]

The source indicated that DNA tagging is still practiced today by DLA, and DNA taggants are applied to all parts in FSC 5962 that are tested by the DLA Electronics Test Lab (Columbus, Ohio). The DNA taggant means the part has been tested and has been determined to be authentic. It is not a source indicator, and it does not contain DNA specific to each distributor. Although the program originally envisioned that each manufacturer would have its own unique mark, only one DNA tag is used by DLA. The source also noted many of the counterfeit parts that are currently being encountered are diodes and transistors, which fall into FSC 5961 (Semiconductor Devices and Associated Hardware). However, parts in FSC 5961 were never included in the DNA tagging program.[121]

e. Subsequent NDAAs and Revisions to Section 818

In subsequent years, the National Defense Authorization Acts made several substantive changes to Section 818's multi-faceted approach to detection and avoidance of counterfeit electronic parts. Section 833 of the NDAA for Fiscal Year 2013 ("FY 2013 NDAA") amended Section 818(c)(2)(B), relating to allowable costs. While the original provision stated that the cost of counterfeit electronic parts and suspect counterfeit electronic parts, along with the cost of rework or corrective action required to remedy the use or inclusion of such parts, were not allowable costs under DoD contracts, the amendment created a three-pronged exception to address situations where the contractor obtained the counterfeit or suspect counterfeit parts from the Government. Under Section 833, such costs would be allowable if (1) the contractor had an operational system to detect and avoid counterfeit parts that was reviewed and approved by the DoD; (2) the counterfeit parts were provided to the contractor as Government property; and (3) the contractor provided timely notice to the Government.[122] Section 885 of the FY 2016 NDAA made additional amendments to Section 818(c)(2)(B), extending to situations where the parts were obtained by a contractor "in accordance with regulations described in paragraph (3)," relating to trusted suppliers.[123]

The NDAA for Fiscal Year 2015 amended the sourcing requirements in Section 818(c)(3). First, it eliminated the phrase "whenever possible" from Section 818(c)(3)(A), with the result that the DoD and its contractors and subcontractors must always obtain electronic parts from the sources indicated (i.e,

[120] Interview with Anonymous Source (notes in possession of authors).
[121] *Id.*
[122] National Defense Authorization Act for Fiscal Year 2013, Public Law 112-239, § 833, 126 Stat. 1844-1845 (2013).
[123] National Defense Authorization Act for Fiscal Year 2016, Public Law 114-92, § 885, 129 Stat. 726, 948 (2015).

parts in production or available in stock must be obtained from the original manufacturers, their authorized dealers, or from trusted suppliers who obtain such parts exclusively from the original manufacturers of the parts or their authorized dealers; parts not in production or available in stock must be obtained from trusted suppliers).[124] The amendment also added a third tier, where the DoD and contractors were instructed to "obtain electronic parts from alternate suppliers if such parts are not available from original manufacturers, their authorized dealers, or suppliers identified as trusted suppliers in accordance with regulations prescribed pursuant to subparagraph (C) or (D)."[125]

The NDAA for Fiscal Year 2017 eliminated all uses of the term "trusted supplier" in Section 818 and replaced it with the phrase "suppliers that meet anticounterfeiting requirements."[126] This change was made in response to concerns expressed by the public that the term "trusted supplier" could be confused with other DoD programs already in place. A "supplier that meets anticounterfeiting requirements" was one that complied with the requirements in Section 818(c)(3)(C) and (D) for DoD-approved suppliers and suppliers identified by contractors and subcontractors. The amendment also changed the heading of Section 818(c)(3) to "Suppliers Meeting Anticounterfeiting Requirements."[127]

More recently, Congress' attention has shifted to state-of-the-art microelectronics and trusted supply chain issues. In the NDAA for Fiscal Year 2020, Section 224 required that, no later than January 1, 2021, the Secretary of Defense must establish trusted supply chain and operational security standards for the purchase of microelectronics products and services by the DoD.[128] The Secretary is further instructed to ensure that, by January 1, 2023, microelectronics products and services purchased by the DoD meet applicable trusted supply chain and operational security standards, unless no such product or service is available for purchase that meets such standards.[129] The pending NDAA for Fiscal Year 2021 contains a Section 807, entitled "Microelectronics Manufacturing Strategy," which would require the DoD to develop a strategy to manufacture state-of-the-art integrated circuits in the U.S. within a period of three to five years. In addition, DoD is to include a plan to explore and evaluate options for re-

[124] National Defense Authorization Act for Fiscal Year 2015, Public Law 113-291, § 817(1)(A), 128 Stat. 3292, 3432 (2014).
[125] *Id.,* §817(1)(D).
[126] National Defense Authorization Act for Fiscal Year 2017, Public Law 114-328, § 815, 130 Stat. 2000, 2271-2272 (2016).
[127] *Id.*
[128] National Defense Authorization Act for Fiscal Year 2020, Public Law 116-92, § 224, 133 Stat. 1266 (2019).
[129] *Id.*

establishing microelectronics foundry services and the industrial capabilities associated with those services.[130]

2) Federal Regulations and Rulemaking Activities

In the FY 2012 NDAA and the National Defense Authorization Acts for subsequent years, the Secretary of Defense was instructed to make substantial revisions to the Defense Federal Acquisition Regulation Supplement ("DFARS") to address the detection and avoidance of counterfeit electronic parts, including contractor responsibilities, use of trusted suppliers, and creation of a GIDEP reporting requirement.[131] The DFARS implements and supplements the provisions of the Federal Acquisition Regulation ("FAR") and is issued under the authorization of the Secretary of Defense.[132] It contains requirements of law, DoD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies and procedures that have a significant effect beyond the internal operating procedures of the DoD or a significant cost or administrative impact on contractors or offerors.[133]

The FAR and DFARS are issued under statutory authority and are published in conformance with required statutory and regulatory procedures. As a result, the FAR and DFARS have the force and effect of law.[134] They are not merely internal agency procedures or interpretative guidance.[135]

The FAR contains specific requirements that agencies such as DoD must follow when issuing agency-specific acquisition regulations (e.g., the DFARS).[136] The views of nongovernmental parties and organizations, as well as other agencies, must be considered in formulating acquisition policies and procedures.[137] A notice of the proposed regulation must be published in the Federal Register, and interested persons then have a minimum of 30 days to submit written comments on the proposed revision.[138] Public meetings may also be held when a decision is likely to benefit from significant

---

[130] National Defense Authorization Act for Fiscal Year 2021, S. 4049 § 807, 116th Cong. (2020). The report accompanying S. 4049 indicates that the Senate Armed Services Committee is concerned about the U.S.'s current near-total dependence on overseas foundries for the manufacture and assembly of state-of-the-art microelectronics. However, the committee also noted that microelectronics supply chain problems are not limited to state-of-the-art devices, and that other essential computing and networking equipment is also dominated by foreign suppliers in at-risk locations. *See* National Defense Authorization Act for Fiscal Year 2021, Report to Accompany S. 4049, at 242, 116th Cong. (2020).
[131] FY 2012 NDAA § 818(c).
[132] 48 C.F.R. § 201.301(a)(1).
[133] *Id.*
[134] Davies Precision Machining, Inc. v. U.S., 35 Fed. Cl. 651, 657 (1996).
[135] *Id.*
[136] 48 C.F.R. § 1.301(b).
[137] 48 C.F.R. § 1.501-2(a).
[138] 48 C.F.R. § 1.501-2(b), (c). Normally, at least 60 days will be given for receipt of comments. *Id.*

additional views and discussions.[139] The final rule, which is also published in the Federal Register, must incorporate a general description of and response to the comments received. The final rule may be published with no changes from the proposed rule, or minor changes may be made based on the comments received. Alternatively, DoD could publish a new proposed rule for comment or an interim rule. Each notice, comment, and issuance of a new rule is referred to as a "DFARS Case." The DFARS Cases are numbered sequentially, based on the order in which they were opened.

From 2012 through 2019, Congress' instructions in Section 818 of FY 2012 NDAA and subsequent NDAAs were implemented in a piecemeal fashion through several such DFARS Cases.[140] Although Congress instructed the Secretary of Defense to issue regulations "not later than 270 days after the date of the enactment" of the FY 2012 NDAA (i.e., by September 26, 2012),[141] the first set of regulations did not take effect until May 6, 2014, almost two and one-half years after enactment of the law. Largely in response to opposition from contractors and industry members, the aggressive plan initially passed by Congress, requiring contractors to eliminate counterfeit electronic parts from the defense supply chain, was gradually diluted to allow contractors to make purchases outside the authorized supply chain and then utilize risk-based inspection and testing procedures to determine whether the parts could be accepted and used or supplied to the Government. In addition, Congress' prohibition on allowing contractors to be reimbursed for the cost of counterfeit electronic parts and suspect counterfeit electronic parts, as well as the cost of rework or corrective action required to remedy the use or inclusion of such parts, was weakened to create a safe harbor for contractors which have an operational system to detect and avoid counterfeit parts and provide timely notice to the Government if the contractor becomes aware of the use or inclusion of counterfeit or suspect counterfeit parts. Finally, the reporting requirement created by Congress in Section 818 did not take effect until December 23, 2019, and it is limited to high value and critical items.

a. DFARS Case 2012-D055: Detection and Avoidance of Counterfeit Electronic Parts

Shortly after the passage of FY 2012 NDAA, DFARS Case 2012-D055 was opened in order to begin implementation of the regulations required by Section 818, as well as the amendments of Section

[139] 48 C.F.R. § 1.503.
[140] Henry Livingston, a Technical Director and Engineering Fellow at BAE Systems, maintains a blog entitled *Counterfeit Parts: Discussions from a defense and aerospace community perspective*. Mr. Livingston tracks and comments on the FAR and DFARS cases relating to the counterfeit parts problem and related issues. *See* https://counterfeitparts.wordpress.com/.
[141] FY 2012 NDAA § 818(c)(1). The FY 2012 NDAA was signed by President Obama on December 31, 2011.

833 of the FY 2013 NDAA.[142] A proposed rule was published on May 16, 2013,[143] which provided definitions of "counterfeit part" and "suspect counterfeit part"; contained provisions making CAS contractors responsible for detecting and avoiding the use or inclusion of counterfeit electronic parts; disallowed the recovery of costs of counterfeit electronic parts or suspect counterfeit electronic parts and the cost of rework or corrective action required to remedy the use or inclusion of such parts, unless the contractor has an approved system to detect and avoid counterfeit parts and suspect counterfeit parts, the parts are Government-furnished property, and the contractor provides timely notice to the Government; and prescribed policy and procedures for preventing counterfeit parts and suspect counterfeit parts from entering the supply chain.[144] The proposed rule also included a new contract clause at DFARS 252.246.7007, entitled "Contractor Counterfeit Electronic Part Avoidance and Detection System.[145]

Following publication of the proposed rule, 50 respondents submitted public comments.[146] In addition, the DoD hosted a public meeting on June 28, 2013, which was attended by members of private-sector firms, industry associations, and government agencies, 12 of whom made presentations.[147] Nokomis, Inc. presented its Advanced Detection of Electronic Counterfeits ("ADEC") Sensor System, which it described as a government funded development to mitigate counterfeit threats. Nokomis suggested that the FY 2012 NDAA "[r]equires the development of technologies to test parts[,] especially those parts the DOD buys itself,"[148] and it contended that "ADEC should be a requirement for a DOD-approved operational system to detect and avoid counterfeit parts."[149] Nokomis further proposed that "ADEC is critical to functionally meeting the proposed DFARS regulations."[150] Other presentations focused on the need for consistent definitions (e.g., proposed use of SAE's definition of "counterfeit part" from AS5553A) and the need to define the term "trusted supplier."[151]

---

[142] National Defense Authorization Act for Fiscal Year 2013 § 833 ("Contractor Responsibilities in Regulations Relating to Detection and Avoidance of Counterfeit Electronic Parts"), Public Law 112-239 (2013), amended FY 2012 NDAA § 818 to provide an exception in limited circumstances to the prohibition on recovery of the costs of counterfeit and suspected counterfeit electronic parts and rework or corrective action with respect to such parts.
[143] 78 Fed. Reg. 28780 (May 16, 2013).
[144] *Id.* at 28780-28785.
[145] *Id.* at 28785.
[146] *See* 79 Fed. Reg. 28092 (May 6, 2014).
[147] *Id. See also*, Notice of Meeting, 78 Fed. Reg. 35262 (June 12, 2013).
[148] Nokomis, Inc., *Advanced Detection of Electronic Counterfeits*, at 2 (June 28, 2013), available at https://www.acq.osd.mil/dpap/dars/publicmeeting/presentations/Nokomis_Presentation.pdf.
[149] *Id.* at 5.
[150] *Id*. at 7.
[151] *See, e.g.,* TTI, Inc., *Proposed DFAR* Comments (June 28, 2013), available at https://www.acq.osd.mil/dpap/dars/publicmeeting/presentations/TTI_Inc_Presentation.pdf; Aerospace Industries Association of America, Inc., *AIA Counterfeit Parts Testimony Detection and Avoidance of*

On May 6, 2014, a final rule was issued which made significant changes to the proposed rule.[152] It contained a definition of "electronic part" that differed from the definition in Section 818(f)(2) and the proposed rule. The final rule defined an "electronic part" as "an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly." It further stated that the term "electronic part" "includes any embedded software or firmware."[153] The definitions of "counterfeit electronic part" and "suspect counterfeit electronic part" were substantially different from the definitions originally proposed, and definition of "obsolete electronic part" was added. Under the new definitions incorporated into DFARS § 202.101,

> *Counterfeit electronic part* means an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.[154]

In its comments, DoD acknowledged that some respondents preferred the definition of counterfeit electronic part from SAE AS5553A.[155] However, DoD declined to adopt that definition due to the "continually evolving nature of the definitions in industry standards and the inconsistencies among the definitions in the standards."[156]

The new regulation defined a "suspect counterfeit electronic part" as "an electronic part for which credible evidence (including, but not limited to, visual inspection or testing) provides reasonable doubt that the electronic part is authentic."[157] The regulation also supplied a definition of "obsolete electronic part," to wit, "an electronic part that is no longer in production by the original manufacturer or an aftermarket manufacturer that has been provided express written authorization from the current design activity or original manufacturer."[158]

Counterfeit Parts (June 28, 2013), available at https://www.acq.osd.mil/dpap/dars/publicmeeting/presentations/AIA_Presentation.pdf.

[152] 79 Fed. Reg. 26092 (May 6, 2014).

[153] *Id.* at 26108 (codified at 48 C.F.R. § 252.246-7007, eff. May 6, 2014).

[154] *Id.* at 26106 (codified at 48 C.F.R. § 202.101, eff. May 6, 2014).

[155] SAE AS5553A defined a counterfeit as "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." *See* 79 Fed. Reg. at 26093.

[156] *Id.* at 26093.

[157] *Id.* at 26106 (codified at 48 CFR § 202.101, eff. May 6, 2014).

[158] *Id.*

Despite the fact that 19 respondents requested that a definition of "trusted supplier" be included in the new DFARS provisions, DoD declined to provide such a definition. DoD noted the expressed concern that defining and using the term "trusted supplier" would create confusion with other current DoD and industry initiatives that used the term.[159] Instead, DoD revised the system criteria in DFARS § 246.807-2(a)(5) and the prescribed contract language in DFARS § 252.246-7007(c)(5) to "express what is intended by 'trusted supplier' without directly using that term."[160] The new provisions required use of "suppliers that meet applicable counterfeit detection and avoidance system criteria."[161]

The regulations also incorporated a new Section 231.205-71, entitled "Cost of remedy for use or inclusion of counterfeit parts and suspect counterfeit parts."[162] The provision recognized limited exceptions to FY 2012 NDAA Section 818(c)(2)(B)'s ban on the cost of counterfeit electronic parts and the cost of rework or corrective action as allowable costs under DoD contracts.[163] The new DFARS provision stated that the costs of counterfeit electronic parts or suspect electronic parts and the cost of rework or corrective action that may be required to remedy the use or inclusion of such parts are unallowable unless –

> (1) The contractor has an operational system to detect and avoid counterfeit parts and suspect counterfeit electronic parts that has been reviewed and approved by DoD pursuant to 244.303;
>
> (2) The counterfeit electronic parts or suspect counterfeit electronic parts are Government-furnished property as defined in FAR 45.101; and
>
> (3) The contractor provides timely (i.e., within 60 days after the contractor becomes aware) notice to the Government.[164]

---

[159] *Id.* at 26095. The proposed confusion was with DoD's Trusted Foundry Program, co-administered by DMEA and the National Security Agency ("NSA"). DMEA has recognized over 70 facilities as "Trusted Accredited Suppliers" of microelectronic devices and services. Those companies then formed a Trusted Supplier Steering Group, and the companies are routinely referred to as "Trusted Suppliers." *See* Trusted Supplier Steering Group, *The Guidebook on Trust: How to Procure Trusted ASICS from Accredited Sources*, available at https://www.intrinsix.com/hubfs/Premium_Content/trusted-asic-design/The_Guidebook_on_Trust.pdf.

[160] *Id.*

[161] *Id.* at 26108 (codified at 48 C.F.R. § 252.246-7007(c)(5), eff. May 6, 2014).

[162] *Id.* at 26106 (codified at 48 C.F.R. § 231.205-71, eff. May 6, 2014).

[163] FY 2012 NDAA § 818(c)(2)(B). In Section 833 of the National Defense Authorization Act of 2013, Congress amended Section 818(c)(2)(B) and created limited exceptions to the blanket prohibition on the cost of counterfeit electronic parts and suspect counterfeit electronic parts and for the cost of rework or corrective action that may be required. National Defense Authorization Act of 2013, Pub. L. No. 112-239 § 833, 126 Stat. 1827 (2013).

[164] 79 Fed. Reg. 26106 (codified at 48 C.F.R. § 231.205-71(b), eff. May 6, 2014). *See* discussion of further amendment implemented in DFARS Case No. 2016-D010, below.

However, the final rule deleted proposed language limiting that provision to contractors that are subject to Cost Accounting Standards ("CAS"), and providing that such contractors are affirmatively responsible for detecting and avoiding the use of counterfeit electronic parts or suspect counterfeit electronic parts provided under CAS-covered contracts.[165] DoD explained that because the new cost principle was located in DFARS subpart 231.2 ("Contracts with Commercial Organizations"), it was applicable to any contract with a commercial organization and was not limited to CAS-covered contracts.[166]

The other significant provisions in the final rule were adoption of Subpart 246.8, including Section 246.870 ("Contractors' counterfeit electronic part detection and avoidance systems")[167] and the corresponding contract clauses in Section 252.244-7007 (sometimes referred to herein as "Contract Clause 7007").[168] Unlike Section 231, these provisions are limited to CAS-covered contractors. The regulation states that CAS-covered contractors and their subcontractors that supply electronic parts or products that include electronic parts are required to establish and maintain "an acceptable counterfeit electronic part detection and avoidance system."[169] The system is required to include risk-based policies and procedures that address at least the 12 criteria set out in detail in Contract Clause 7007(c), including training of personnel, inspection and testing of electronic parts, processes to abolish counterfeit parts proliferation, processes for maintaining traceability, use of authorized suppliers, reporting and quarantining of counterfeits, and methodologies to identify suspect counterfeit parts.[170] As requested by many respondents, the new regulations did not merely repeat the system criteria from Section 818 without elaboration, but instead attempted to expand and clarify the intent of the criteria, and it authorized contractors to make risk-based decisions relating to counterfeit detection and avoidance. Testing and inspection is to be performed in accordance with Government- and industry-recognized techniques, and the contractor is instructed to select tests and inspections with the goal of minimizing risk to the Government.[171] Further, the new regulation expressly stated that counterfeit detection and avoidance requirements, including system criteria, must be flowed down to subcontractors at all levels in the supply chain that are responsible for buying or selling electronic parts or assemblies, or for performing authentication testing.[172]

---

[165] *Compare* 78 Fed. Reg. at 28783.
[166] 79 Fed. Reg. at 26101.
[167] *Id*. at 26106-26107 (codified at 48 C.F.R. § 246.870, eff. May 6, 2014).
[168] *Id*. at 26108 (codified at 48 C.F.R. § 252.244-7007, eff. May 6, 2014).
[169] 48 C.F.R. § 246.870-2(a) (eff. May 6, 2014).
[170] 48 C.F.R. § 252.246-7007(c) (eff. May 6, 2014).
[171] 79 Fed. Reg. at 26096.
[172] 48 C.F.R. § 252.246-7007(c)(9), (e) (eff. May 6, 2014).

b. DFARS Case 2014-D005: Detection and Avoidance of Counterfeit Electronic Parts—Further Implementation

DFARS Case 2014-D005 amended the DFARS to provide further implementation of Section 818 of the FY 2012 NDAA, as well as modifications contained in Section 817 of the NDAA for FY 2015.[173] DoD described the rule as taking a "risk-based approach to counterfeit management."[174] It stated that the rule "allows contractors to make risk-based decisions (such as testing and inspection) based on supply chain assurance measures (such as the source of the electronic part), which is all subject to review and audit by the contracting officer."[175]

The case resulted in several significant changes to the DFARS. First, it added a number of new definitions to DFARS § 202.101, including a definition for the term "contractor-approved supplier," which replaced the controversial term "trusted supplier" that was originally used in Section 818 of the 2012 NDAA.[176] A "contractor-approved supplier" means a supplier that "does not have a contractual agreement with the original component manufacturer for a transaction, but has been identified as trustworthy by a contractor or subcontractor."[177] The definition of "electronic part" in Contract Clause 7007 was also revised to delete the sentence "The term 'electronic part' includes any embedded software or firmware.'"[178]

More importantly, the rule implemented a three-tier approach to selecting suppliers of electronic parts. The revised policy section[179] and the corresponding new contract clause at DFARS § 252.246-7008 (sometimes referred to herein as "Contract Clause 7008)[180] both address three distinct situations. In the first category ("Tier One"), the government requires contractors and subcontractors at all levels of the supply chain to obtain electronic parts that are in production by the original manufacturer or an authorized aftermarket manufacturer, or currently available in stock, from (a) the original manufacturers of the parts,

---

[173] National Defense Authorization Act of 2015, Pub. L. No. 113-291, § 817, 128 Stat. 3432 (2014).
[174] 81 Fed. Reg. 50635, at 50640 (August 2, 2016).
[175] *Id.* at 50640. It noted that DoD uses the Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs.
[176] *Id*. at 50647 (codified at 48 C.F.R. § 202.101, eff. Aug. 2, 2016).
[177] *Id.*
[178] The proposed rule explained that, although electronic parts may include embedded software or firmware, the requirements of the regulation were more applicable to hardware. Further, it noted that industry standards were still under development to address testing of embedded software or firmware in electronic parts. *See* 80 Fed. Reg. at 56941.
[179] 48 C.F.R. § 246.870-2 (eff. Aug. 2, 2016).
[180] 48 C.F.R. § 252.246-7008 (eff. Aug. 2, 2016).

(b) their authorized suppliers, or (c) suppliers that obtain such parts exclusively from the original manufacturers of their parts or their authorized suppliers.[181]

The second tier ("Tier Two) addresses situations where electronic parts are not in production by the original manufacturer or an authorized aftermarket manufacturer, and they are not currently available in stock from a Tier One source. In those situations, contractors must obtain electronic parts from "suppliers identified by the Contractor as contractor-approved suppliers,"[182] provided that three conditions are met. First, the contractor must use established counterfeit prevention industry standards and processes (including inspection, testing, and authentication) for identifying and approving contractor-approved suppliers.[183] Next, the contractor is required to assume responsibility for the authenticity of parts provided by the contractor-approved supplier.[184] Finally, the rule makes the selection of contractor-approved suppliers subject to review and audit by the contracting officer.[185]

The third category ("Tier Three") addresses a variety of problematic situations, where contractors and subcontractors are required to comply with certain notification, inspection, testing, and authentication requirements.[186] These include situations where a contractor obtains an electronic part from a source other than a Tier One source, because the parts were not available from a Tier One source; and where a contactor obtains an electronic part from a subcontractor (other than the original manufacturer) who refused to accept flow down of the sourcing provisions.[187] The notification, inspection, testing, and authentication requirements also apply where a contractor cannot confirm that an electronic part was new (or not previously used) and that it had not been comingled with used, refurbished, reclaimed, or returned parts.[188]

---

[181] 48 C.F.R. § 246.870-2(a)(i); 48 C.F.R. § 252.246-7008(b)(1).
[182] 48 C.F.R. § 246.870-2(a)(ii); 48 C.F.R. § 252.246-7008(b)(2).
[183] 48 C.F.R. § 246.870-2(a)(ii)(A); 48 C.F.R. § 252.246-7008(b)(2)(i). Both the policy language and the corresponding contract provision direct contractors to the list of DoD-adopted standards at https://assist.dla.mil.
[184] 48 C.F.R. § 246.870-2(a)(ii)(B); 48 C.F.R. § 252.246-7008(b)(2)(ii).
[185] 48 C.F.R. § 246.870-2(a)(ii)(C); 48 C.F.R. § 252.246-7008(b)(2)(iii). Subsequently, in DFARS Case 2016-D013, the subsection was further amended to clarify that such review, audit and approval would generally be conducted in conjunction with a contractor purchasing system review (CPSR) or other surveillance of purchasing practices by the contract administration office, unless the government has credible evidence that a contractor-approved supplier has provided counterfeit parts. Apparently in an effort to avoid delay, the amendment provided that the contractor may proceed with the acquisition of electronic parts from a contractor-approved supplier unless otherwise notified by DoD. *See* 83 F.R. 19641, at 19645 (codified at 48 C.F.R. § 246.870-2(a)(1)(ii)(C) and 48 C.F.R. § 252.246-7008(b)(2)(iii), eff. May 4, 2018).
[186] 48 C.F.R. § 246.870-2(a)(ii)(C)(2); 48 C.F.R. § 252.246-7008(b)(3).
[187]48 C.F.R. § 246.870-2(a)(ii)(C)(2)(i); 48 C.F.R. § 252.246-7008(b)(3)(i)(A).
[188] 48 C.F.R. § 246.870-2(a)(ii)(C)(2)(ii); 48 C.F.R. § 252.246-7008(b)(3)(i)(B).

Finally, the new rule amended DFARS Contract Clause 7007, which already required CAS-covered contractors to establish and maintain an acceptable counterfeit electronic part detection and avoidance system.[189] The amendment made clear that the system must include risk-based policies and procedures, including a revised list of system criteria that includes use of suppliers in accordance with the three-tier approach in Contract Clause 7008.[190] The amendments also added a subsection (e), requiring that contractors flow down the substance of Contract Clause 7008 in all subcontracts, including subcontracts for commercial items that are electronic parts or assemblies containing electronic parts, unless the subcontractor is the original manufacturer.[191]

c. DFARS Case 2016-D010: Cost of Remedy for Use or Inclusion of Counterfeit Electronic Parts

In 2014, DFARS Case 2012-D055 added Section 231.205-71, entitled "Cost of remedy for use or inclusion of counterfeit electronic parts and suspect counterfeit electronic parts."[192] That section provided that the costs of counterfeit electronic parts or suspect counterfeit electronic parts, and the cost of rework or corrective action that may be required to remedy the use or inclusion of such were unallowable unless, *inter* alia, the contractor provided timely notice to the Government.[193]

The exception was subsequently refined through DFARS Case 2016-D010. First, the amendment limited the safe harbor to those instances where the contractor becomes aware of the counterfeit electronic parts or suspect counterfeit electronic parts through inspection, testing, and authentication efforts of the contractor or its subcontractors; through a GIDEP alert; or by some other means.[194] In addition, the contractor must provide timely written notice (i.e., within 60 days after the contractor becomes aware) to both the contracting officer and GIDEP.[195] The only instances in which the contractor is not required to report to GIDEP are where the contractor is a foreign business entity without a physical presence in the United States, or where the part is the subject of an ongoing criminal investigation.[196]

[189] 48 C.F.R. § 252.246-7007 (eff. May 6, 2014).
[190] 81 Fed. Reg. 50635, at 50640 (codified at 48 C.F.R. § 252.246-7007(c)(5), eff. May 6, 2014).
[191] *Id.* at 50640 (codified at 48 C.F.R. § 252.246-7007(e), eff. May 6, 2014).
[192] 48 C.F.R. § 231.205-71 (eff. May 6, 2014).
[193] 48 C.F.R. § 231.205-71(b)(3) (eff. May 6, 2014).
[194] 81 Fed. Reg. 59510, at 59515 (codified at 48 C.F.R. § 231.205-71(b)(3)(i), eff. Aug. 30, 2016).
[195] *Id.* (codified at 48 C.F.R. § 231.205-71(b)(3)(ii), eff. Aug. 30, 2016).
[196] *Id.*

d. DFARS Case 2015-D020: DoD Use of Trusted Suppliers for Electronic Parts and DFARS Case 2017-D023: Suppliers that Meet Anti-Counterfeiting Requirements

DFARS Case 2015-D020 ("DoD Use of Trusted Suppliers for Electronic Parts") was opened in order to implement Section 818(c)(3) of the FY 2012 NDAA, as amended by Section 817 of the FY 2015 NDAA.[197] Following the 2015 amendments, Section 818(c)(3) provided:

> (3) TRUSTED SUPPLIERS.—The revised regulations issued pursuant to paragraph (1) shall—
>
> (A) require that 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 suppliers identified as trusted suppliers in accordance with regulations issued pursuant to subparagraph (C) or (D);
>
> (ii) obtain electronic parts that are not in production or currently available in stock from suppliers identified as trusted suppliers in accordance with regulations issued pursuant to subparagraph (C) or (D); and
>
> (iii) obtain electronic parts from alternate suppliers if such parts are not available from original manufacturers, their authorized dealers, or suppliers identified as trusted suppliers in accordance with regulations issued pursuant to subparagraph (C) or (D);
>
> (B) establish requirements for notification of the Department, and for 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 clause (i) or (ii) of subpargraph (A), if obtaining the electronic parts in accordance with such clauses is not possible;
>
> (C) establish qualification requirements, consistent with the requirements of section 2319 of title 10, United States Code, pursuant to which the Department may identify as trusted suppliers those 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.

[197] Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, Public Law 113-291 § 817, 128 Stat. 3292 (Dec. 2, 2014).

Thus, the amendment retained the concept of "trusted suppliers," but it introduced the three-tiered sourcing system for obtaining electronic parts that had already been incorporated into the DFARS by DFARS Case 2014-D005. The amended language also retained the instruction for DoD to establish qualification requirements for identifying trusted suppliers, and it continued to allow DoD contractors and subcontractors to identify and use additional trusted suppliers, subject to review and audit by DoD officials.

DFARS Case 2015-D020 was closed in 2017 before revised DFARS regulations were issued. The case was then folded into new DFARS Case 2017-D023, in order to implement Section 815 of the National Defense Authorization Act for Fiscal Year 2017.[198] Section 815 of the FY 2017 NDAA deleted the term "trusted suppliers" and inserted "suppliers meeting anticounterfeiting requirements" throughout Section 818(c)(3).[199] However, the amendment did not define the term "suppliers meeting anticounterfeiting requirements."

Shortly after it was opened, DFARS Case 2017-Do23 was placed on hold at the direction of the director of the Defense Acquisition Regulation Council ("DARC").[200] No additional information about DFARS Case 2017-D023 has been located, and its status today remains unclear.

If the requirements of Section 817 of the FY 2015 NDAA and Section 815 of the FY 2017 NDAA were implemented, however, it would require significant changes to the DFARS as they exist today. DFARS Section 246.870-2 and corresponding Contract Clause 7008 provide for a three-tiered sourcing system for obtaining electronic parts, but in Tier One contractors and subcontractors are authorized to obtain parts from "Suppliers that obtain such parts exclusively from the original manufacturers of the parts or their authorized suppliers."[201] It is at best unclear whether "suppliers that obtain such parts exclusively from the original manufacturers of the parts or their authorized suppliers" is equivalent to "suppliers that meet anticounterfeiting requirements," although it seems questionable. Further, the amended version of Section 818(c)(3)(C) requires the DoD to establish qualification requirements pursuant to which it can identify "suppliers that meet anticounterfeiting requirements that have appropriate policies and procedures in place to detect and avoid counterfeit electronic parts and

---

[198] National Defense Authorization Act for Fiscal Year 2017, Public Law 114-328, 130 Stat. 2000 (Dec. 23, 2016).
[199] *Id.* at § 815.
[200] The *Counterfeit Parts* blog authored by Henry Livingston contains the following notes:

> 01/11/2017 Case on hold at the direction of DARC Director, pending input from PDI.
> 02/02/2017 Case closed into Holding File 2017-H011, pending further input from PDI.

See https://counterfeitparts.wordpress.com/2017/11/28/far-dfars-case-update-27-nov-2017/.
[201] 48 C.F.R. § 246.870-2(a)(1)(i)(C) (eff. May 4, 2018); 48 C.F.R. §252.246-7008(b)(1)(iii) (eff. May 4, 2018).

suspect counterfeit electronic parts."[202] Those qualification requirements have yet to be implemented. Instead, the DFARS authorizes the use of contractor-approved suppliers, as contemplated by Section 818(c)(3)(D).[203]

e. FAR Case 2013-002: Reporting of Nonconforming Items to the Government-Industry Data Exchange Program

In 2013, the DoD, the General Services Administration, and NASA began working together on an amendment to the Federal Acquisition Regulation ("FAR") to require contractors and subcontractors to report counterfeit and suspect counterfeit items, as well as major and critical nonconformances, to GIDEP. These amendments were intended to implement Sections 818(c)(4) and 818(c)(5) of the FY 2012 NDAA, which were limited to DoD contractors and subcontractors which encountered counterfeit electronic parts and suspect counterfeit electronic parts.[204] However, the FAR Council extended coverage to include other Government agencies, a much broader group of items than just electronic parts, and nonconformances as well as counterfeits.[205] After the FAR case was opened in 2013, a proposed rule was published on June 10, 2014,[206] and a public meeting was held on June 16, 2014.[207] However, a final rule did not issue until November 2019, with the amendments finally taking effect on December 23, 2019.[208]

The new regulation created reporting requirements applicable to an acquisition by any federal agency, including DoD, of any items subject to higher-level quality standards[209] and any items that the contracting officer determines to be critical items[210] for which the reporting requirements would be appropriate.[211] In addition, the requirements apply to acquisitions that exceed the simplified acquisition threshold and are by or for the DoD of electronic parts or end items, components, parts, or materials containing electronic parts, and for acquisitions of services, where the contractor will furnish such items

---

[202] FY 2012 NDAA § 818(c)(3)(C) (as amended Dec. 23, 2016).
[203] *See* 48 C.F.R. § 246.870-2(a)(1)(ii) (eff. May 4, 2018); 48 C.F.R. § 252.246-7008(b)(2) (eff. May 4, 2018).
[204] FY 2012 NDAA § 818(c)(4), (5).
[205] 84 Fed. Reg. 64680 (November 22, 2019).
[206] 79 Fed. Reg. 33164 (June 10, 2014).
[207] 84 Fed. Reg. 64680, at 64682.
[208] 84 Fed. Reg. 64680.
[209] *See* 48 C.F.R. 52.246-11 Higher-Level Contract Quality Requirement.
[210] A "critical item" means "an item, the failure of which is likely to result in hazardous or unsafe conditions for individuals using, maintaining, or depending upon the item; or is likely to prevent performance of a vital agency mission." 84 Fed. Reg. 64680, at 64694 (codified at 48 C.F.R. § 46.101, eff. Dec. 23, 2019).
[211] *Id.* (codified at 48 C.F.R. § 46.317(a)(1), eff. Dec. 23, 2019).

as part of the service being provided.[212] The reporting requirements do not apply to acquisitions of commercial items, including commercially available off-the-shelf ("COTS") items.[213]

The new contract language requires contractors to submit a report to GIDEP within 60 days of becoming aware or having reason to suspect that an item purchased by the contractor for delivery to, or for, the Government is either a counterfeit or suspect counterfeit item or a common item that has a major or critical nonconformance.[214] That awareness could arise from inspection, testing, record review, or notification from another source, such as a seller, customer, or third party.[215] Reporting is not required in only very limited circumstances: where the contractor is a foreign business entity that does not have a physical presence in the U.S.; where the contractor is aware that the counterfeit, suspect counterfeit, or nonconforming item is the subject of an ongoing criminal investigation; or for nonconforming items, where the manufacturer or distributor has not released the item to more than one customer.[216] Consistent with FY 2012 NDAA § 818(c)(5), the rule created a safe harbor for contractors and subcontractors that submit GIDEP reports: the contractor or subcontractor will not be subject to civil liability for reporting, provided that the contractor or subcontractor made a reasonable effort to determine that the report was factual.[217]

The contract clause also imposes three additional obligations on contractors. First, contractors must screen GIDEP reports as a part of the contractor's inspection system or quality control program, in order to avoid the use and delivery of counterfeit or suspect counterfeit items or delivery of items that contain a major or critical nonconformance.[218] Contractors are also required to notify the contracting officer within 60 days of becoming aware of or having reason to suspect that any end item, component, subassembly, part, or material contained in supplies purchased by the contractor for delivery to, or for, the government is counterfeit or suspect counterfeit.[219] Finally, the contractor is required to retain counterfeit or suspect counterfeit items in its possession until it receives disposition instructions from the contracting

---

[212] *Id.* The simplified acquisition threshold (the "SAT") at that time was $150,000. It was increased to $250,000 effective August 31, 2020. *See* 85 Fed. Reg. 40064, 40067 (July 2, 2020), *amending* 48 C.F.R. § 2.101.
[213] *See id.* at 64682. The Summary of Significant Changes from the Proposed Rule states that the final rule has been significantly descoped to exclude contracts and subcontracts at or below the simplified acquisition threshold (SAT), as well as contracts and subcontracts for the acquisition of commercial items, including COTS items. Instead, the rule focuses on supplies that require higher-level quality standards or are determined to be critical items.
[214] *Id.* at 64695 (codified at 48 C.F.R. § 52.246-26(b)(4), eff. Dec. 23, 2019).
[215] *Id.*
[216] *Id.* (codified at 48 C.F.R. § 52.246-26(c), eff. Dec. 23, 2019).
[217] *Id.* (codified at 48 C.F.R. § 52.246-26(f), eff. Dec. 23, 2019).
[218] *Id.* (codified at 48 C.F.R. § 52.246-26(b)(1), eff. Dec. 23, 2019).
[219] *Id.* (codified at 48 C.F.R. § 52.246-26(b)(2), eff. Dec. 23, 2019).

officer.[220] All four requirements (screening GIDEP reports, notifying the contracting officer, retaining counterfeit items, and reporting to GIDEP) must be flowed down in subcontracts for electronic parts or end items, components, parts, or materials containing electronic parts.[221]

In one respect, the final rule was much broader than the regulations authorized by Section 818(c)(4) of the FY 2012 NDAA, because it includes solicitations and contracts by any agency and is not limited to DoD contractors or subcontractors, and because the reporting requirement is extended to include common items that have a major or critical nonconformance. Conversely, the final rule was narrower than required by Congress since it does not apply to contracts for commercial items (including COTS items) or to contracts at or below the SAT; Section 818(c)(4) instructed that the regulation must require any DoD contractor or subcontractor to report counterfeit and suspect counterfeit electronic parts.

f. FAR Case 2012-032: Higher-Level Contract Quality Requirements

In addition to the FAR and DFARS cases that directly implemented the provisions in Section 818 of the FY 2012 NDAA, several additional cases created or amended regulations that directly or indirectly relate to anti-counterfeiting efforts. These include FAR Case 2012-032, relating to Higher-Level Contract Quality Requirements. The rule clarified when to use higher-level quality standards in solicitations and contracts, and it updated the examples of higher-level quality standards by adding new industry standards that pertain to avoidance of counterfeit parts and other items.[222] The examples included overarching quality management system standards such as ISO 9001, ANSI/ASQC E4, ASME NQA-1, SAE AS9100, SAE AS9003, and ISO/TS 16949, as well as product or process specific standards such as SAE AS5553.[223]

g. DFARS Case 2019-D009: Use of Supplier Performance Risk System (SPRS) Assessments

Currently, DoD is proposing to amend the DFARS to update the policy and procedures for use of the Supplier Performance Risk System ("SPRS"). In a proposed rule published on August 31, 2020, DoD indicated that the SPRS is an application that uses quality and delivery data from Government systems to

[220] 84 Fed. Reg. 64680, at 64695 (codified at 48 C.F.R. § 52.246-26(b)(3), eff. Dec. 23, 2019). Previously, many contractors raised questions about how long they were required to quarantine counterfeit or suspect counterfeit electronic parts. Here, the rule clearly states that counterfeit and suspect counterfeit items must be retained until the contractor receives disposition instructions from the contracting officer. *See also* 48 C.F.R. § 46.407(h).
[221] 84 Fed. Reg. 64680, at 64695 (codified at 48 C.F.R. § 52.246-26(g)(1)(iii), eff. Dec. 23, 2019).
[222] 79 Fed. Reg. 70344 (Nov. 25, 2014).
[223] *Id.*, codified at 48 C.F.R. 46.202-4(b) (eff. Dec. 26, 2014).

calculate "on time" delivery scores and quality classifications. The system generates three risk assessments:

- *Item Risk.* The probability that a product or service will introduce counterfeit or nonconforming material into the DoD supply chain, which can result in significant personnel safety issues, mission degradation, or monetary loss.
- *Price Risk.* Determines whether pricing is fair and reasonable, based on historical pricing data.
- *Supplier Risk.* SPRS calculates a supplier risk score based on three years of relevant supplier performance information, so that contracting officers can compare competing suppliers.

Contracting officers are expected to use the risk assessments in performance evaluations for acquisitions.

3. What is a "Risk Based Approach" to Counterfeit Prevention?

FY 2012 NDAA Section 818 directed the Secretary of Defense to issue or revise guidance applicable to DoD 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."[224] Such guidance was to 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.[225]

Section 818 did not instruct the Secretary of Defense to enact regulations requiring contractors to utilize risk-based policies and procedures for counterfeit avoidance; only the DoD was required to use a risk-based approach for its own purchasing decisions.[226] Instead, Section 818 instructed the Secretary issue regulations providing that "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 electronic parts in such products," as well as any rework or corrective action required to remedy the use or inclusion of counterfeit parts.[227] The Secretary was also instructed to implement a program to enhance contractor detection and avoidance of counterfeit electronic parts, which program shall "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*

[224] FY 2012 NDAA § 818(b)(2).
[225] *Id.*
[226] *Id.* In addition, the Secretary of Homeland Security was instructed to "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." *See id.* at § 818(d).
[227] *Id.* at § 818(c)(2)(A).

chain."[228] Contractors were required to eliminate counterfeit parts, not use risk-based policies and procedures in implementing a counterfeit part detection and avoidance system.

The concept of a risk-based approach to counterfeit detection and prevention for contractors was first introduced as part of DFARS Case 2012-D055. The proposed rule published on May 16, 2013 made no mention of a risk-based approach for contractors, but many respondents objected that the proposed rule did not correctly implement Section 818. Specifically, the respondents argued that Section 818(b)(2) contained a requirement "to implement a risk-based approach to minimize the impact of counterfeit electronic parts or suspect counterfeit electronic parts on DoD."[229] They believed that the proposed rule "would impose unreasonable strict liability standards on industry, regardless of significant and good-faith efforts to address the issue."[230] The DoD reported other respondents stated that:

> considering the potentially unaffordable costs of treating all acquisitions of electronic parts equally, the final rule should provide for weighing the odds of occurrence and the potential consequences in responding to potential threats of counterfeit parts, which can vary from serious impact to negligible impact. One of these respondents recommended that DoD enable its largest contractors to take the lead in detection and avoidance of counterfeit electronic parts by allowing those contractors to make risk-based decisions on how best to implement supply chain assurance measures.[231]

The DoD relented and, rather than requiring 100 percent detection and elimination of counterfeit parts, it allowed covered contractors to establish risk-based counterfeit detection and avoidance systems.[232] Subsequently, in DFARS Case 2014-D005, the use of risk-based processes was extended to traceability, where the contractor is not the original manufacturer of, or authorized supplier for, an electronic part. In that situation, the contractor is required to have "risk-based processes (taking into consideration the consequences of failure of an electronic part) that enable tracking of electronic parts from the original manufacturer to product acceptance by the Government."[233]

DFARS § 246.870-2 and Contract Clause 7007 require contractors to establish and maintain a counterfeit electronic part detection and avoidance system, which must include risk-based policies and procedures that address a minimum of 12 areas.[234] However, aside from setting out the list of minimum considerations, neither the statute nor the regulations defines a "risk-based system" of counterfeit part

---

[228] *Id.* at § 818(e)(2)(A) (emphasis added).
[229] 79 Fed. Reg. at 26096. A close examination of Section 818(b)(2) reveals that it only applies to DoD's internal purchasing decisions and does not apply to contractors.
[230] *Id.*
[231] *Id.*
[232] *Id.* The comments state that "[t]his change confirms the final rule with DoDI 4140.67."
[233] 48 C.F.R. § 252.246-7008(c)(1)."
[234] 48 C.F.R. § 246.870-2(b); 48 C.F.R. § 252.246-7007(b), (c).

detection and prevention, and contractors are not provided with any guidance about how to balance the relevant risks against the time and costs involved in testing. Contract Clause 7007 states:

> Tests and inspections shall be performed in accordance with accepted Government- and industry-recognized techniques. *Selection of tests and inspections shall be based on minimizing the risk to the Government.* Determination of risk shall be based on the assessed probability of receiving a counterfeit electronic part; the probability that the inspection or test selected will detect a counterfeit electronic part; and the potential negative consequences of a counterfeit electronic part being installed (e.g., human safety, mission success) where such consequences are made known to the Contractor.[235]

The goal of minimizing the risk to the Government suggests that any and all possible counterfeit detection and prevention measures are called for, and it effectively negates the benefits of a risk-based approach.[236] It is also inconsistent with DoD Instruction 4140.67, which instructs DoD Component heads to integrate DoD anti-counterfeiting policy into all relevant regulations and contract requirements.[237] DoD Instruction 4140.67 further requires the DoD Component heads to "[i]mplement anti-counterfeiting measures, strategies, plans, and programs that balance the risks caused by [critical materiel and materiel that is susceptible to counterfeiting] with the impact to readiness and cost of the measures."[238]

Risk-based methodologies are discussed in the academic literature, and a risk-based approach has been adopted for testing of electrical, electronic, and electromechanical (EEE) parts by the SAE AS6171 set of standards. DiMase *et al.* have suggested that when electronic parts are not available from authorized sources, a risk-based policy should require an assessment "that may require more stringent test and inspection requirements on material acquired from independent distributors and brokers, where the likelihood of receiving a counterfeit part is more probable than from other trusted sources, and the traceability to the original manufacturer is limited or impossible to achieve."[239] High-risk parts should be prioritized, and parts that could impact mission criticality and safety should be subjected to more testing in order to increase confidence for those applications.[240]

---

[235] 48 C.F.R. § 252.246-7007(c)(2) (emphasis added).
[236] Michael H. Azarian, *An Overview of Risk-Based EEE Counterfeit Part Detection Based on SAE AS6171*, PROCEEDINGS OF THE 44TH INTERNATIONAL SYMPOSIUM FOR TESTING AND FAILURE ANALYSIS (2018), at 1.
[237] U.S. Department of Defense, Instruction No. 4140.67, *DoD Counterfeit Prevention Policy* (2013), at 9.
[238] *Id.* at 10.
[239] Daniel DiMase, Zachary Collier, Jinae Carlson, Robin Gray, and Igor Linkov, *Traceability and Risk Analysis Strategies for Addressing Counterfeit Electronics in Supply Chains for Complex Systems*, SOCIETY FOR RISK ANALYSIS (2016), at 7.
[240] *Id.* at 7. However, the authors warn that "no amount of testing can truly authenticate an electronic part. The best testing can do is increase the confidence that parts do not show evidence of counterfeiting based on testing performed." *Id.*

Azarian argues that a risk-based methodology is advantageous to ensure that the time and money invested in counterfeit detection are commensurate with the potential negative effects and likelihood of counterfeit part usage in a particular application.[241] He explains that the SAE AS6171 family of standards adopted a risk-based methodology to determine the level of testing that should be utilized to manage the risk associated with use of an EEE. *See* detailed discussion of the SAE AS6171 standards, *infra*. The standard fills a need by providing contractors with instruction on how to develop a test plan for a particular application and part by assigning a risk level to the part and then prescribing a specific sequence of tests intended to mitigate the assigned risk.[242]

The U.S. Defense Logistics Agency ("DLA") Land and Maritime has adopted the SAE AS6171 set of standards for use by the DoD,[243] but it is still being called out only infrequently in DoD contracts. Test labs must be accredited to conduct the suite of tests specified by AS6171, but to date, only a small number of labs have been accredited under SAE AS6171. DLA lists over 130 labs on its list of Commercial Labs,[244] but the ANSI National Accreditation Board, an accreditation body, lists only four labs that are accredited under SAE AS6171. [245]

4. DoD Issuances

The DoD issues a variety of documents that prescribe or implement policy on a specific subject, including directives, memoranda, instructions, and manuals.[246] A DoD directive establishes policy and may also assign responsibilities for specific components of DoD, but it does not contain any procedures for carrying out those policies. A DoD Instruction is a DoD issuance that establishes policy and may also contain high level procedures for implementing the policy.[247] DoD Manuals implement the policies contained in DoD Directives and Instructions and may be published in several volumes if they are lengthy.[248] Several DoD Issuances relate in some way to counterfeit prevention and mitigation.

---

[241] Michael H. Azarian, *An Overview of Risk-Based EEE Counterfeit Part Detection Based on SAE AS6171*, *supra* note 236, at 1.
[242] *Id.* at 2.
[243] Defense Logistics Agency, *Adoption Notice*, SAE AS6171 (March 28, 2017), available at https://landandmaritimeapps.dla.mil/Downloads/MilSpec/Docs/SAE/saeas6171.pdf.
[244] Defense Logistics Agency, *List of Commercial Laboratories Suitable for Testing Military Devices*, available at https://landandmaritimeapps.dla.mil/offices/sourcing_and_qualification/labsuit.aspx.
[245] One of those labs is located outside the U.S., in Israel. *See* ANAB, ANSI National Accreditation Board, https://anab.ansi.org/latest-news/anab-offers-lab-accreditation-to-as6171-for-detection-of-counterfeit-parts.
[246] *See Overview of Department of Defense Issuances*, available at https://www.esd.whs.mil/Portals/54/Documents/DD/iss_process/DoD_Issuances.pdf.
[247] *Id.*
[248] *Id.*

a. DoD Instruction 4140.01

In December 2011, DOD Instruction 4140.01 issued, establishing policy and assigning responsibilities for management of materiel across the DoD supply chain.[249] For the first time, the Instruction explicitly recognized the need to prevent counterfeit materiel from entering the defense supply chain.[250] The current version of DoD Instruction 4140.01, adopted March 6, 2019, applies broadly and defines "materiel" as "[a]ll items necessary to equip, operate, maintain, and support military activities without distinction as to their application for administrative or combat purposes, excluding real property, installations, and utilities."[251] "Counterfeit materiel" includes all materiel "whose identity or characteristics have been deliberately misrepresented, falsified, or altered without legal right to do so."[252]

Today, DoD Instruction 4140.01 establishes a DoD policy to apply life-cycle management controls to guard against counterfeit materiel in the DoD supply chain,[253] and it distributes responsibilities across the department heads. The Assistant Secretary of Defense for Sustainment (ASD(S)) acts as "the principal point of contact for all matters relating to the prevention, detection, reporting, and disposition of counterfeit materiel."[254] The Director of Defense Pricing and Contracting (DPC) is responsible for establishing procurement policies and guidance to "prevent the acquisition of counterfeit materiel for secondary items.," as well as reporting requirements to GIDEP and law enforcement agencies.[255] The Under Secretary of Defense for Research and Engineering (USD(R&E)) provides GIDEP training and services, and also provides technical advice and assistance on matters involving the prevention, detection, and reporting of counterfeit materiel.[256] The DoD Component Heads are charged with developing sourcing programs that "promote quality and hardware reliability and assurance and prevent counterfeit materiel or unauthorized product substitution or modification[257]; they are also responsible for establishing programs for monitoring and mitigating the risk of counterfeit materiel entering DoD supply chains, as well as other unauthorized supply chain activities such as malicious insertion and intellectual property

[249] U.S. Department of Defense, DoD Instruction 4140.01, *DoD Supply Chain Materiel Management Policy* (December 14, 2011, as amended March 6, 2019) [hereinafter "DoD Instruction 4140.01"]. DoD Instruction 4140.01 was originally issued as DoD Regulation 4140.1-R (May 23, 2003). It was then reissued as DoD Instruction 4140.01 and the accompanying DoD Manual 4140.01 (Vols. 1-12). *See* Defense Logistics Agency, DoD Regulations and Manuals, https://www.dla.mil/HQ/InformationOperations/DLMS/elibrary/manuals/regulations/.
[250] Interview with Anonymous Source from DoD (notes in possession of authors).
[251] DoD Instruction 4140.01 § G.2.
[252] *Id.*
[253] *Id.* at § 1.2(d).
[254] *Id.* at § 2.2.
[255] *Id.* at § 2.3(a), (b).
[256] *Id.* at § 2.5(b), (c).
[257] *Id.* at § 2.7(c).

theft.[258] The Instruction also provides overarching procedural guidance and refers to Volume 3 of DoD Manual 4140.01, which describes detailed procedures relating to materiel sourcing throughout the DoD supply chain.[259]

b. The Kendall Memo

Shortly after the FY 2012 NDAA was signed into law, Acting Under Secretary of Defense Frank Kendall issued a memorandum to the Secretaries of the Military Departments and Directors of the Defense Agencies, providing overarching DoD counterfeit prevention guidance.[260] The so-called "Kendall Memo" recognized that counterfeit items pose a "serious threat to the safety and operational effectiveness" of DoD systems.[261] The memo announced that in response to that threat, DoD was developing policies and strategies designed to detect and prevent the introduction of counterfeit items, with particular emphasis on mission critical components, critical safety items, electronic parts, and load-bearing mechanical parts.[262] DoD Components were instructed to take immediate action to decrease the probability of counterfeit items, including ensuring program managers were notified when critical items (particularly electronic parts) were not obtained from an OCM or authorized distributor; participate in a review to identify appropriate industry anti-counterfeiting standards; establish testing and verification requirements for items not received from an OCM or authorized distributor; ensure suspect and confirmed counterfeit items were reported to GIDEP; and report confirmed incidents of counterfeits to the appropriate criminal authorities.[263]

c. DoD Instruction 4140.67

The DoD Counterfeit Prevention Policy, DoD Instruction No. 4140.67, subsequently issued on April 26, 2013, and cancelled the Kendall Memo.[264] The purpose of DoD Instruction 4140.67 was to establish policy, provide direction, and assign responsibilities for prevention, detection, and remediation

---

[258] *Id.* at § 2.7(f).
[259] *Id.* at § 3.3.
[260] Acting Under Secretary of Defense Frank Kendall, Memorandum for Secretaries of the Military Departments and Directors of the Defense Agencies ("Overarching DoD Counterfeit Prevention Guidance") (March 16, 2012) [hereinafter "the Kendall Memo"].
[261]Kendall Memo, at 1. The Kendall Memo defined "counterfeit materiel" 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." Used items represented as new items were included as "counterfeit materiel." *Id.*, at 1.
[262] *Id.* at 1.
[263] *Id.* at 1-2.
[264] Department of Defense Instruction 4140.67, *DoD Counterfeit Prevention Policy*, § 1(d), at 1 (April 26, 2013) [hereinafter "DoD Instruction 4140.67"].

of counterfeit materiel in the DoD supply chain.[265] It sets out 10 separate DoD policies, including, *inter alia*, employing a risk-based approach to reduce the frequency and impact of counterfeit materiel; documenting all occurrences of counterfeit materiel in GIDEP; investigating all cases of suspected counterfeit materiel and notifying investigative organizations and others; seeking restitution and remediation when counterfeit materiel is obtained; and providing DoD workforce with appropriate education and training.[266]

Like the Kendall Memo, DoD Instruction 4140.67 allocates responsibility for counterfeit prevention and mitigation across the DoD.[267] The Under Secretary of Defense for Acquisition and Sustainment is responsible for establishing integrated DoD policy and implementing guidance on all anti-counterfeiting matters, and for developing acquisition and procurement policies, procedures and regulations. The USD(A&S) is also charged with ensuring collaboration with other federal agencies and international partners, as well as coordinating with DoD Components to establish a risk-based approach to anti-counterfeiting that is not unique to the DoD.[268] Specific responsibilities are further allocated to the Assistant Secretary of Defense for Sustainment and the Assistant Secretary of Defense for Acquisition.[269] The DoD Component Heads[270] share responsibility for implementing DoD anti-counterfeiting policies, procedures, and contract requirements, including procuring critical materiel from suppliers that meet appropriate counterfeit avoidance criteria, detecting counterfeit materiel using sampling and testing techniques, investigating occurrences of suspect and confirmed counterfeit materiel, and reporting such occurrences to GIDEP and appropriate authorities.[271]

---

[265] *Id.* at § 1.
[266] *Id.* at § 3.
[267] DoD Instruction 4140.67 adopts the definition of "counterfeit materiel" used in the Kendall Memo ("An item that is an unauthorized copy or substitute that has been identified, marked, 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.") *See* DoD Instruction 4140.67, Glossary, at 12.
[268] *Id.* at 7.
[269] *Id.* at 8.
[270] The DoD Components include the Office of the Secretary of Defense, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD. DoD Instruction 4140.67 § 2(a), at 1.
[271] *Id.* at 9-10.

d. DoD Instruction 5200.44

DoD Instruction 5200.44 is a cybersecurity policy that addresses protection of mission critical functions to achieve trusted systems and networks.[272] The Instruction applies to all DoD information systems and weapons systems that are or include national security systems, systems with a high impact level for any of the three security objectives (i.e., confidentiality, integrity, and availability), and other DoD information systems determined to be critical to direct fulfillment of military or intelligence missions.[273] It also applies to mission critical functions and critical components in applicable systems, including spare and replacement parts, and it contemplates future applicability to non-ICT components.[274]

The purpose of DoD Instruction 5200.44 is to establish policy and assign responsibilities to "minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, . . ., by foreign intelligence, terrorists, or other hostile elements."[275] It implements DoD's Trusted Systems and Networks ("TSN") strategy to manage risks to system integrity and trust by integrating various disciplines, including systems engineering, supply chain risk management (SCRM), security, intelligence and counterintelligence, cybersecurity, hardware and software assurance, and information systems security.[276]

The Instruction is noteworthy because it directly links counterfeiting and cybersecurity concerns. A stated policy of the DoD is to manage risk to the trust in applicable systems throughout the entire system lifecycle, including TSN processes, tools, and techniques to:

> (2) Control the quality, configuration, software patch management, and security of software, firmware, hardware, and systems throughout their lifecycles, including components or subcomponents from secondary sources. Employ protections that manage risk in the supply chain for components or subcomponent products and services (e.g., integrated circuits, field-programmable gate arrays (FPGA), printed circuit boards) when they are identifiable (to the supplier) as having a DoD end-use.

---

[272] Department of Defense Instruction 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)* (Nov. 5, 2012, as amended Oct. 15, 2018) [hereinafter "DoD Instruction 5200.44"].
[273] *Id.* at § 2(c).
[274] *Id.* at § 2(d). The Instruction states that only information and communications technology (ICT) components in applicable systems shall be considered for the processes described in the Instruction, until such a time as the Applicability section is modified. The Responsibilities section instructs the Under Secretary of Defense for Acquisition, Technology, and Logistics in coordination with the DoD Component Heads to evaluate the feasibility and usefulness of applying the processes in Instruction 5200.44 to non-ICT components that are critical to DoD weapons and information systems, and to issue policy as appropriate. *See* DoD Instruction 5200.44, Enclosure 2 § 1(f), at 7.
[275] *Id.* at § 1(a).
[276] *Id.* at § 1(b).

(3) Detect the occurrence of, reduce the likelihood of, and mitigate the consequences of unknowingly using products containing counterfeit components or malicious functions in accordance with DoDI 4140.67. . . .

(6) Implement item unique identification (IUID) for national level traceability of critical components in accordance with DoDI 8320.04.[277]

e. Other DoD Guidance

In 2018, the Department of the Navy issued SECNAV Instruction 4855.20A, its Counterfeit Materiel Prevention policy.[278] Department of Navy Activities were instructed to "[i]mplement a risk-based approach to identify and prevent the introduction of materiel that is at high risk of counterfeiting," and "[e]nsure all instances of counterfeit materiel or suspect counterfeit materiel are reported" to GIDEP and other required authorities.[279] SECNAV Instruction 4855.20A adopted the definition of "counterfeit materiel" used in DoD Instruction 4140.47.[280]

The Army Materiel Command also developed a Counterfeit Parts and Materials Prevention Program Guidebook in 2018.[281] The guidebook provides detailed counterfeit prevention, detection, and mitigation processes. However, because it is a guidebook, it can only provide recommendations and cannot tell Army Materiel Command personnel what they must do. A source from the DoD indicated that there is a forthcoming Army Regulation that will require the Army to follow a counterfeit risk management program (CRM). It is expected that the regulation will issue at the end of 2020 or in early 2021. There will also be an accompanying pamphlet that will contain extensive details on how the regulation should be carried out. Nevertheless, the source noted that there is nothing to ensure that the regulation will be enforced; while an audit could be requested to show that a command is not following a regulation, audits typically occur only after there has a been a serious problem. The source also

---

[277] *Id.* at § 4.
[278] Department of the Navy, SECNAV Instruction 4855.20A, *Counterfeit Materiel Prevention* (hereinafter "SECNAV Instruction 4855.20A") (Nov. 5, 2018). SECNAV Instruction 4855.20A replaced Navy Counterfeit Prevention Policy 4855.20 (adopted April 22, 2015) and canceled NAVSO P-7000 (*Counterfeit Materiel Process Guidebook: Guidelines for Mitigating the Risk of Counterfeit Materiel in the Supply Chain*, adopted June 20, 2017).
[279] SECNAV Instruction 4855.20A § 5.
[280] "Counterfeit Materiel" includes "[i]tems that are unauthorized copies or substitutes that have been identified, marked, or altered by a source other than the items' legally authorized source or have been misrepresented to be authorized items of the legally authorized source." SECNAV Instruction 4855.20A, Enclosure 2 (Definitions), at 1.
[281] Army Materiel Command, Counterfeit Parts and Materials Prevention Program Guidebook (December 2018), available at https://www.dau.edu/cop/dmsms/DAU%20Sponsored%20Documents/AMC%20Counterfeit%20Parts%20and%20Materials%20Guidebook%20V1.0.pdf.

commented that an effective program requires education about what is required, along with someone to champion the program. However, the source feels that counterfeiting is not currently an important issue to the Army and it will likely get little attention unless there is a catastrophic failure or a weapon system gets hacked.[282]

In addition, another source has indicated that Aerocyonics, Inc. has been developing a counterfeit mitigation guidebook for the Air Force in 2020. No further details about that effort were available.

5. Other Federal Laws Relating to Counterfeiting

Several other federal laws also relate to counterfeiting, including the Lanham Act and criminal provisions dealing with trafficking in counterfeit goods, mail fraud, and wire fraud.

a. Lanham Act Civil Causes of Action for Trademark Infringement, Counterfeiting, and False Advertising

The Lanham Act allows for federal registration of trademarks and service marks with the United States Patent and Trademark Office.[283] In addition, it creates civil causes of action for trademark infringement, false advertising, dilution, and other claims.[284]

Section 32 of the Lanham Act provides a remedy for infringement of a registered mark:

> Any person who shall, without the consent of the registrant—
>
> (a) use in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive; or
>
> (b) reproduce, counterfeit, copy or colorably imitate a registered mark, and apply such reproduction, counterfeit, copy or colorable imitation to labels, signs, prints, packages, wrappers, receptacles or advertisements intended to be used in commerce upon or in connection with the sale, offering for sale, distribution, or advertising of goods or services on or in connection with which is likely to cause confusion, or to cause mistake, or to deceive,
>
> shall be liable in a civil action by the registrant for the remedies hereinafter provided.[285]

Note that the remedy is by way of a civil action brought by the owner of the mark; the consumers who are confused, mistaken or deceived by the unauthorized use of the mark have no standing to bring an action

[282] Interview with Anonymous Source (notes in possession of authors).
[283] 15 U.S.C. § 1051.
[284] 15 U.S.C. §§ 1114, 1125.
[285] 15 U.S.C. §§ 1114(1).

for trademark infringement. Use of a counterfeit mark subjects the user of the infringing mark to treble damages,[286] and it also gives the trademark owner the right to elect an award of statutory damages instead of actual damages and profits.[287]

However, under the Lanham Act, not all trademark infringements rise to the level of counterfeiting. The term "counterfeit" is defined as "a spurious mark which is identical with, or substantially indistinguishable from, a registered mark."[288] To be "substantially indistinguishable, two marks must be nearly identical . . . with only minor differences which would not be apparent to an unwary observer."[289] That is, a "counterfeit mark" is a non-genuine mark identical to the registered, genuine mark of another, where the genuine mark was registered for use on the same goods to which the infringer applied the mark.[290] "The essence of counterfeiting under the Lanham Act is that the use of the infringing mark seeks to trick the consumer into believing he or she is getting the genuine article, rather than a colorable imitation."[291]

Several government and industry representatives who were interviewed in connection with this report felt that the Lanham Act does not provide a broad enough range of relief for brand owners, because they believed that it does not address situations where products bear a genuine trademark but other markings on the product have been changed in order to deceive purchasers. However, several civil cases have addressed these types of facts and have found potential liability.

For example, in *Intel Corp. v. Terabyte International, Inc.*,[292] the Ninth Circuit Court of Appeals held that a broker was liable for trademark infringement for distributing Intel math coprocessors which

---

[286] 15 U.S.C. § 1117(b).

[287] 15 U.S.C. § 1117(c). The Anticounterfeiting Consumer Protection Act of 1996 first introduced statutory damages as an alternative to actual damages and profits. In 2008, the PRO-IP Act ("Prioritizing Resources and Organization for Intellectual Property Act") substantially increased the statutory damages available to trademark owners. Today, Section 1117(c) provides that in a case involving the use of a counterfeit mark, the plaintiff may elect to recover:

> (1) not less than $1,000 or more than $200,000 per counterfeit mark per type of goods or services sold, offered for sale, or distributed, as the court considers just, or
>
> (2) if the court finds that the use of the counterfeit mark was willful, not more than $2,000,000 per counterfeit mark per type of goods or services sold, offered for sale, or distributed, as the court considers just.

[288] 15 U.S.C. §§ 1127; Tiffany and Co. v. Costco Wholesale Corp., 971 F.3d 74, 95 (2d Cir. 2020).

[289] Louis Vuitton Malletier, S.A. v. Sunny Merch. Corp., 97 F. Supp. 3d 485, 499 (S.D.N.Y. 2015).

[290] Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., 658 F.3d 936, 946 (9th Cir. 2011).

[291] Coty, Inc. v. Excell Brands, LLC, 277 F. Supp. 3d 425, 468 (S.D.N.Y. 2017).

[292] Intel Corp. v. Terabyte Int'l, Inc., 6 F.3d 614 (9th Cir. 1993).

had been relabeled from slower chips to faster and more expensive math coprocessors.[293] The court noted that "[o]ne of the most valuable and important protections afforded by the Lanham Act is the right to control the quality of the goods manufactured and sold under the holder's trademark."[294] Terabyte argued that its actions did not constitute trademark infringement because it was selling real Intel math coprocessors and only the model designations had been changed. Terabyte contended that there was no confusion as to the *source* of the product (i.e., Intel) and that any confusion about the capability of the products was irrelevant to liability for trademark infringement, but the court disagreed.

The court observed that Terabyte's interpretation of the Lanham Act improperly ignored the good will, reputation, and consumer protection functions associated with a particular trademark.[295] Instead, the court said that the public relies upon the trademark so that "it will get the product which it asks for and wants to get."[296] It further stressed that full disclosure about the condition of a product is required in order to avoid liability for trademark infringement.[297] The court stated:

> Intel's math coprocessors were modified, i.e., relabeled, to deceive the public. Intel did not perform or authorize the chip modifications, and only the most formalistic of approaches could lead to a conclusion that Intel was the "source" of those chips once they were relabeled. The relabeling was so basic that "it would be a misnomer to call the article by its original name." . . . The modified math coprocessors exhibited a significantly higher failure rate compared to genuine Intel math coprocessors of the same model. In essence, the modified math coprocessors were counterfeit copies of the faster and more expensive models. By distributing those products as particular genuine Intel math coprocessors, Terabyte threatened Intel's reputation and good will and deceived its customers who believed they were purchasing those particular models of math coprocessors.[298]

The court concluded that Intel marked the chips with its name only in connection with the slower processing speed, and the chips became counterfeits when they were remarked with a speed designation that Intel would not have given them. As a result, Terabyte's conduct was prohibited by the Lanham Act.[299]

---

[293] *Id.* The court explained that Intel labeled its math coprocessors by laser etching the model number on the chip itself. On the infringing chips, those markings were either physically removed or covered and replaced with different markings, including the Intel logo. *See id.* at 616, n. 1.
[294] *Id.* at 618, *citing* El Greco Leather Prod. Co., Inc. v. Shoe World, Inc., 806 F.2d 392, 395 (2d Cir. 1986), *cert. denied,* 484 U.S. 817 (1987).
[295] *Id.* at 619, *citing* Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763, 774 (1992) (trademarks foster competition and the maintenance of quality by securing to the producer the benefits of good reputation).
[296] *Id*.
[297] *Id.*, *citing* Champion Spark Plug Co. v. Sanders, 331 U.S. 125 (1947).
[298] *Id. at* 619-20 (citations omitted).
[299] *Id.* at 620.

Other courts have reached similar conclusions. See, e.g., *Beltronics USA, Inc. v. Midwest Inventory Distribution LLC*,[300] holding that the unauthorized resale of a materially different trademarked product can constitute trademark infringement. The district court determined that Beltronics demonstrated a substantial likelihood of success on the merits and was entitled to a preliminary injunction, and the appellate court affirmed; that is, Beltronics had a substantial likelihood of showing that the removal or alteration of serial number labels on Beltronics radar detectors being sold by the defendants caused a likelihood of confusion concerning the source of the Beltronics products and eroded consumer goodwill toward the Beltronics mark.[301] Echoing *Intel,* the court indicated that removing labels raised an issue about quality control, one of the most important protections afforded by the Lanham Act.[302]

As a result, it appears the problem isn't that the Lanham Act doesn't provide a cause of action for trademark infringement and counterfeiting that would apply where a broker sells parts bearing the trademark of the actual manufacturer but where the model numbers, date codes, serial numbers or other markings have been changed. Instead, it seems more likely the real problem is that trademark owners are either unwilling or unable to bring civil actions against counterfeiters. There are several reasons why they might be reluctant to do so. First, the amount of money at stake may be relatively insignificant in the eyes of the trademark owner, particularly in a case involving a few parts destined for a DoD contract.

In addition, trademark actions can be expensive to maintain, and legal fees and other costs in the hundreds of thousands of dollars would not be unusual.[303] The Lanham Act does authorize a court to enter an award of attorney fees to a prevailing party in an exceptional case.[304] An exceptional case is one in which the infringing party acts in a malicious, fraudulent, deliberate, or willful manner,[305] such as willful infringement or vexatious litigation tactics. However, the amount of the award is discretionary, and no award of attorney fees or costs would be made until the case was successfully concluded in favor

---

[300] 562 F.3d 1067, 1072 (10th Cir. 2009). The Tenth Circuit cited a long line of opinions from other circuits reaching similar conclusions.
[301] Beltronics USA, Inc. v. Midwest Inventory Distribution, LLC, 522 F. Supp. 2d 1318, 1327 (D. Kan. 2007), *aff'd,* 562 F.3d 1067.
[302] *Id.,* 522 F. Supp. 2d at 1328. *But see,* Analog Devices, Inc. v. West Pacific Industries, 152 F.3d 923 (9th Cir. 1998) (unpublished disposition), finding that plaintiff was not entitled to a preliminary injunction where a reseller of computer chips bearing Analog's mark, which were supposed to be destroyed, resold the chips "as is."
[303] In the *Intel* case, the district court entered an order in 1992 directing Terabyte to pay Intel's attorney fees in the amount of $206,410. However, on appeal, that order was set aside and returned to the district court for further consideration. *See* Intel Corp. v. Terabyte Int'l, Inc., 6 F.3d at 621-23.
[304] 15 U.S.C. § 1117(a).
[305] Securacomm Consulting, Inc. v. Securacom Inc., 224 F.3d 273, 281 (3d Cir. 2000); Burger King Corp. v. Pilgrim's Pride Corp., 15 F.3d 166, 168 (11th Cir. 1994).

of the trademark owner. Trademark owners may also be concerned that even if they are able to secure a judgment against a counterfeiter (including compensatory damages, attorney fees, and costs), the defendant may be judgment proof (i.e., lacking the economic means to satisfy any judgment). Further, if the counterfeiter is located in another country, U.S. courts may be unable to exercise jurisdiction over them in the first place.[306]

It may also be the case that brand owners seldom find it necessary to file a civil action against an alleged infringer. Andrew Olney, the General Manager of Technology Development at Analog Devices, Inc., indicated that if Analog sees a broker using the Analog logo, it will send a cease and desist letter to that broker. He noted that, upon receipt of a cease and desist letter, the vast majority of brokers in the U.S. will stop displaying the Analog logo.[307] Others have also suggested that targeted use of demand letters to the registrants and Internet service providers for infringing websites is "a more cost-effective means of deterring low-priority counterfeit behavior."[308] Finally, some of the allegedly infringing brokers could also be the trademark owner's customers, and suing one's customers is almost never a sound business strategy.[309] Many authorized distributors also sell unauthorized product, and distributors will sometimes seek out parts for a particular customer, essentially acting as a broker in those transactions. Alternatively, perhaps trademark owners feel that counterfeiting activity is better left to the criminal system.

---

[306] *See* Christopher S. Finnerty and Morgan T. Nickerson, *Business As Usual: Think of the battle against counterfeiting simply as a normal expense*, CORPORATE COUNSEL (May 2011) ("The foreign or judgment-proof defendant has long been the bane of counterfeit litigation. Companies have exhausted entire legal budgets chasing defendants in mainland China with little or no chance of recovery. While foreign strategies are not without merit, they are expensive and transform the enforcement/legal department into an expensive cost center within a company."

[307] Andrew Olney Interview Summary (Appendix 19), at 2. However, Mr. Olney acknowledged that it is more difficult stopping trademark infringement in other countries, especially China. Even in the U.S., a few brokers may simply set up another company with a new name and then continue using the Analog logo and trademarks.

[308] Christopher S. Finnerty and Morgan T. Nickerson, *Business As Usual: Think of the battle against counterfeiting simply as a normal expense*, CORPORATE COUNSEL (May 2011). The authors recognize that while this does not stop the manufacturer of the counterfeits, it forces sellers to rehost their website and to face the threat of having it constantly removed by the ISP.

[309] Even in the *Beltronics* case, Beltronics' authorized distributors were not named as defendants, despite the fact that they were selling Beltronics products to defendant Midwest Inventory Distribution outside of the geographic area in which they were supposed to be selling Beltronics merchandise to dealers. The serial number labels on the Beltronics radar detectors were either removed or replaced with fake labels, allegedly in an attempt to prevent Beltronics from detecting the unauthorized distribution. It is unclear from the opinion which party was responsible for removing or replacing the labels. *See* Beltronics USA v. Midwest Inventory Distrib., LLC, 522 F. Supp. 2d at 1325.

Lack of standing may present another impediment. Lanham Act Section 43(a) provides multiple causes of action to the owners of both registered and unregistered marks:[310]

> Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which—
>
> (A) is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, service, or commercial activities by another person, or
>
> (B) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities,
>
> shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act. [311]

Section 43(a) thus creates two distinct causes of action: false association and false advertising.[312]

It could be argued that some acts of counterfeiting, including selling used parts as new, could constitute either false association or false advertising. However, although Section 43(a) suggests that a civil action may be brought by "*any person* who believes that he or she is or is likely to be damaged," the courts have clearly held that consumers and purchasers do not have standing to sue. Only the owner of a registered or unregistered trademark can bring an action for false association. Likewise, a false advertising claim can only be brought by a plaintiff who alleges an injury to a commercial interest in reputation or sales.[313] Again, this means that DoD, contractors, and subcontractors have no standing to bring a trademark-based action against a lower tier subcontractor or a supplier who provides them with counterfeit electronic parts. Their remedy is for breach of contract and/or debarment of the supplier.

b. Criminal Penalties for Trafficking in Counterfeit Military Goods and Services

The Trademark Counterfeiting Act of 1984 also created a federal statute that criminalized trafficking in counterfeit goods or services. The statute provided criminal penalties for anyone who intentionally traffics in goods or services and knowingly uses a counterfeit mark on or in connection with

---

[310] Note that only Section 43(a) creates a cause of action for unregistered marks. Lanham Act Section 32 and the criminal provisions in 18 U.S.C. § 2320 apply only to registered marks.
[311] 15 U.S.C. §1125(a) (referred to as "Lanham Act § 43(a)").
[312] *See* Lexmark Intern., Inc. v. Static Control Components, Inc., 572 U.S. 118, 122 (2014).
[313] *Id.,* 572 U.S. at 131-132. The court explained that a consumer who is hoodwinked into purchasing a disappointing product or a business that is misled by a supplier into purchasing an inferior product is not under the aegis of the Lanham Act.

such goods.[314] The Stop Counterfeiting in Manufactured Goods Act of 2006 expanded liability and made it a crime to traffic labels, hangtags, and other types of packaging, thereby targeting counterfeiters who imported blank fake products and applied counterfeit labels and packaging after the items were in the U.S.[315] Section 818 of the FY 2012 NDAA subsequently made it a crime, with enhanced penalties, to traffic in counterfeit military goods and services.[316]

Today, 18 U.S.C. § 2320 provides as follows:

> (a) Offenses.—Whoever intentionally –
>
> (1) traffics in goods or services and knowingly uses a counterfeit mark on or in connection with such goods or services,
>
> (2) traffics in labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging of any type or nature, knowing that a counterfeit mark has been applied thereto, the use of which is likely to cause confusion, to cause mistake, or to deceive,
>
> (3) traffics in goods or services knowing that such good or service is *a counterfeit military good or service* the use, malfunction, or failure of which is likely to cause serious bodily injury or death, the disclosure of classified information, impairment of combat operations, or other significant harm to a combat operation, a member of the Armed Forces, or to national security, or
>
> (4) traffics in a counterfeit drug,
>
> or attempts or conspires to violate any of paragraphs (1) through (4) shall be punished as provided in subsection (b).[317]

The term "counterfeit military good or service" is defined as a good or service that uses a counterfeit mark on or in connection with such good or service and that is either (a) falsely identified or labeled as meeting military specifications, or (b) is intended for use in a military or national security application.[318]

For purposes of the criminal provisions relating to trafficking in counterfeit goods or services, the term "counterfeit" carries a different meaning than under the Lanham Act or the relevant provisions of the DFARS. Under 18 U.S.C. § 2320, the term "counterfeit mark" means:

> (A) a spurious mark –
>
> (i) that is used in connection with trafficking in any goods, services, labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging of any type or nature;

[314] 18 U.S.C. § 2320(a)(1).
[315] Stop Counterfeiting in Manufactured Goods Act, H.R. 32, 109th Cong. (2006).
[316] FY 2012 NDAA § 818(h).
[317] 18 U.S.C. § 2320(a) (emphasis added).
[318] 18 U.S.C. § 2320(f)(4). The term "counterfeit mark" is defined in 18 U.S.C. § 2320(f)(1).

(ii) that is identical with, or substantially indistinguishable from, a mark registered on the principal register in the United States Patent and Trademark Office and in use, whether or not the defendant knew such mark was so registered;

(iii) that is applied to or used in connection with the goods or services for which the mark is registered with the United States Patent and Trademark Office, or is applied to or consists of a label, patch, sticker, wrapper, badge, emblem, medallion, charm, box, container, can, case, hangtag, documentation, or packaging of any type or nature that is designed, marketed, or otherwise intended to be used on or in connection with the goods or services for which the mark is registered in the United States Patent and Trademark Office; and

(iv) the use of which is likely to cause confusion, to cause mistake, or to deceive; or

(B) a spurious designation that is identical with, or substantially indistinguishable from, a designation as to which the remedies of the Lanham Act are made available by reason of section 220506 of title 36.[319]

Thus, a counterfeit mark is an imitation or "knock-off" of a registered mark, used in connection with the same type of goods or services with which the mark is registered, which is likely to cause confusion or mistake or to deceive. However, a "counterfeit mark" does not include any mark or designation where, at the time of manufacture or production, the manufacturer or producer was authorized by the owner of the mark or designation to use it for the type of goods or services manufactured or produced.[320]

Under the 1984 version of the Act, an individual could be fined up to $250,000 and imprisoned for up to five years. Those penalties have steadily increased, and today Section 2320 provides that whoever commits an offense under subsection (a) will be subject to the following penalties:

(A) if an individual, shall be fined not more than $2,000,000 or imprisoned not more than 10 years, or both, and if a person other than an individual, shall be fined not more than $5,000,000; and

(B) for a second or subsequent offense under subsection (a), if an individual, shall be fined not more than $5,000,000 or imprisoned not more than 20 years, or both, and if other than an individual, shall be fined not more than $15,000,000.[321]

Incidents involving serious bodily injury or death carry even heavier penalties.[322]

[319] 18 U.S.C. § 2320(f)(1).
[320] *Id.*
[321] 18 U.S.C. § 2320(b)(1).
[322] 18 U.S.C. § 2320(b)(2).

The FY 2012 NDAA created similar enhanced penalties for trafficking in counterfeit military goods or services. Section 2320(b)(3) provides:

> Whoever commits an offense under subsection (a) involving a counterfeit military good or service or counterfeit drug—
>
> (A) if an individual, shall be fined not more than $5,000,000, imprisoned not more than 20 years, or both, and if other than an individual, shall be fined not more than $15,000,000; and
>
> (B) for a second or subsequent offense, if an individual, shall be fined not more than $15,000,000, imprisoned not more than 30 years, or both, and if other than an individual, shall be fined not more than $30,000,000.

Forfeiture and destruction of the infringing goods, and an order requiring the defendant to pay restitution to the victim of the offense, are also available as remedies.[323]

c. Other Criminal Provisions

Other sections of the criminal code are also frequently invoked in actions involving allegations of counterfeiting. Mail fraud and wire fraud are two of the most common.

Mail fraud is addressed by 18 U.S.C. § 1341, which states:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, or to sell, dispose of, loan, exchange, alter, give away, distribute, supply, or furnish or procure for unlawful use any counterfeit or spurious coin, obligation, security, or other article, or anything represented to be or intimated or held out to be such counterfeit or spurious article, for the purpose of executing such scheme or artifice or attempting so to do, places in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service, or deposits or causes to be deposited any matter or thing whatever to be sent or delivered by any private or commercial interstate carrier, or takes or receives therefrom, any such matter or thing, or knowingly causes to be delivered by mail or such carrier according to the direction thereon, or at the place at which it is directed to be delivered by the person to whom it is addressed, any such matter or thing, shall be fined under this title or imprisoned not more than 20 years, or both.[324]

The Supreme Court has said that there are two elements in mail fraud: (1) having devised or intending to devise a scheme to defraud (or to perform specified fraudulent acts), and (2) use of the mail for the

[323] 18 U.S.C. §§ 2320(c), 2323.
[324] 18 U.S.C. § 1341 (as amended, Jan. 7, 2008).

purpose of executing, or attempting to execute, the scheme (or specified fraudulent acts).[325] However, to be part of the execution of the fraud, the use of the mails need not be an essential element of the scheme.[326] Instead, it is sufficient for the mailing to be "incident to an essential part of the scheme,"[327] or "a step in [the] plot."[328]

> Wire fraud is addressed by 18 U.S.C. §1343, which states in part:
>
> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.[329]

There are three elements of wire fraud: (1) a scheme to defraud, (2) use of the wires in furtherance of the scheme, and (3) a specific intent to deceive or defraud.[330] Use of emails is a type of communication that may give rise to wire fraud.[331] Similarly, use of cellular telephones may constitute wire fraud.[332]

Trafficking in counterfeit goods or services, mail fraud, and wire fraud all constitute racketeering activity under 18 U.S.C. § 1961.[333] It is unlawful for a person to do any of the following: (1) to use or invest any income derived, directly or indirectly, from a pattern of racketeering activity to acquire an interest in or establish the operations of any enterprise engaged in interstate or foreign commerce; (2) to acquire or maintain any interest in or control of such an enterprise through a pattern of racketeering activity; (3) for an employee of such an enterprise, to engage in the conduct of such enterprise's activities through a pattern of racketeering activity; or (4) to conspire to do any of the foregoing.[334] A pattern of racketeering activity requires at least two acts of racketeering activity.[335] A violation of the act can result

---

[325] Schmuck v. U.S., 489 U.S. 705, 721 (1989) (mailing of innocent title applications to state department of transportation satisfied the mailing element, where used car distributor purchased used cars, rolled back their odometers, and resold them to retail dealers at inflated prices).
[326] *Id.* at 710, *citing* Pereira v. U.S., 347 U.S. 1, 8 (1954).
[327] *Id.* at 710-11, *citing* Pereira v. U.S., 347 U.S. at 8.
[328] *Id*. at 711, *citing* Badders v. U.S., 240 U.S. 391, 394 (1916).
[329] 18 U.S.C. §1343(as amended Jan. 7, 2008).
[330] U.S. v. Hussain, 972 F.3d 1138, 1143 (9th Cir. 2020), *citing* Pasquantino v. U.S., 544 U.S. 349, 358 (2005) ("the wire fraud statute punishes fraudulent use of domestic wires").
[331] *See, e.g.,* U.S. v. Hussain, 972 F.3d 1138 (9th Cir. 2020).
[332] U.S. v. Nunez, 78 Fed. Appx. 989 (5th Cir. 2003).
[333] 18 U.S.C. § 1961(1).
[334] 18 U.S.C. § 1962.
[335] 18 U.S.C. § 1961(5).

in fines, imprisonment, and forfeiture of the proceeds of the racketeering activity and associated enterprise.[336] Civil remedies are also available[337]; however, it appears they are seldom successful.[338]

d. Criminal Indictments and Prosecutions for Counterfeiting

Several of the government and industry representatives who were interviewed in connection with this report felt that the Department of Justice fails to bring a sufficient number of criminal actions for trafficking in counterfeit goods. Often they attribute this to a disconnect between the definition of "counterfeit" under 18 U.S.C. § 2320 (which is viewed as focusing too much on registered trademarks) and the broader definition of "counterfeit electronic part" in the DFARS (which arguably focuses more on the characteristics of the part itself). Nevertheless, there have been a number of successful criminal cases involving allegations of counterfeiting, as well as related claims for mail fraud and wire fraud, that have received significant press. They include:

- Shannon Wren and Stephanie McCloskey were indicted on charges including conspiracy, trafficking in counterfeit goods, and mail fraud, following a grand jury proceeding on September 8, 2010.[339] The indictment alleged that Wren and McCloskey, through a company known as VisionTech Components, imported and resold integrated circuits bearing counterfeit marks, some of which were falsely represented as military grade. The sales generated gross profits in excess of $15,800,000, and a number of the ICs were resold for use in military applications. McCloskey was sentenced to 38 months in prison after entering a guilty plea and agreeing to cooperate with authorities. Wren died from an accidental drug overdose while the case was pending.[340]

- Hao Yang was indicted under charges of trafficking in counterfeit goods, trafficking in counterfeit military goods (i.e., integrated circuits), and conspiracy to traffic in counterfeit goods and counterfeit military goods on June 12, 2013.[341] Yang agreed to plead guilty to conspiring to traffic in counterfeit goods and counterfeit military goods, and on April 17, 2014, he was

[336] *See* 18 U.S.C. § 1863.
[337] 18 U.S.C. § 1864.
[338] *See, e.g.,* Gucci America, Inc. v. Alibaba Group Holding Ltd., 2016 WL 6110565 (S.D.N.Y. 2016) (dismissing civil RICO allegations based on counterfeiting, where plaintiffs failed to allege the existence of an "enterprise").
[339] U.S. v. Shannon L. Wren and Stephanie A. McCloskey, Case No. CR-10-245, Indictment (D.D.C. Sept. 8, 2010). Note that the case against Wren and McCloskey was filed before the amendments that criminalized trafficking in counterfeit military goods and services.
[340] U.S. Customs and Immigration Enforcement, News Release: *VisionTech Administrator Sentenced to Prison for Role in Sales of Counterfeit Circuits Destined to U.S. Military* (October 25, 2011), available at https://www.ice.gov/news/releases/visiontech-administrator-sentenced-prison-role-sales-counterfeit-circuits-destined-us.
[341] U.S. v. Hao Yang, Case 1:13-cr-00305-JFM, Indictment (D. Maryland June 12, 2013).

sentenced to 21 months in prison.[342] He was also required to forfeit five bank accounts worth over $59,000, a 2010 Acura purchased with proceeds of his illegal activities, and various other items valued at over $280,000.[343]

- Virgie Dillard, Roland Evans, and Mark Morgan each agreed to plead guilty to conspiracy to commit wire fraud, in connection with their roles in a scheme to sell counterfeit and modified computer equipment to the U.S. Army.[344] The DOJ's press release indicated that Dillard's company, Missouri Office Systems and Supplies, Inc., supplied over $1 million worth of counterfeit Cisco products (including network hardware such as transceivers and switches) to Army Recreation Machine Program locations in the U.S. and abroad. Dillard received five years of probation, while Evans and Morgan were sentenced to 37 and 30 months in federal prison, respectively. The court also ordered them to pay $1,073,022 in restitution to the U.S. Army.[345]
- Peter Picone was indicted on charges of conspiracy to traffic in counterfeit goods and counterfeit military goods, two counts of trafficking in counterfeit goods (integrated circuits bearing counterfeit marks of Xilinx, Inc. and National Semiconductor), wire fraud, conspiracy to commit wire fraud, and conspiracy to commit money laundering on June 25, 2013.[346] After entering a guilty plea, Picone was sentenced to 37 months in prison, ordered to pay restitution in the amount of $352,076 to 31 companies whose goods he counterfeited, and required to forfeit $70,050 and 35,870 counterfeit integrated circuits.[347] The press release announcing his sentence indicated that some of the counterfeit integrated circuits imported by Picone were resold to contractors that intended to supply them to the U.S. Navy for use in nuclear submarines.[348]

---

[342] Department of Justice, U.S. Attorney's Office, District of Maryland, Press Release: *Pennsylvania Man Who Sold Counterfeit Military Goods Sentenced To 21 Months In Prison* (April 17, 2014), available at https://www.justice.gov/usao-md/pr/pennsylvania-man-who-sold-counterfeit-military-goods-sentenced-21-months-prison.
[343] *Id.*
[344] Department of Justice, U.S. Attorney's Office, Western District of Missouri, Press Release: *KC Business Owner Among Three Sentenced for $1 Million Scheme to Defraud the Army* (October 31, 2014), available at https://www.justice.gov/usao-wdmo/pr/kc-business-owner-among-three-sentenced-1-million-scheme-defraud-army.
[345] *Id.*
[346] U.S. v. Peter Picone, Case No. 3:13-CR-128 AWT, Indictment (D. Conn. June 25, 2013).
[347] Department of Justice, Office of Public Affairs, Press Release: *Massachusetts Man Sentenced To 37 Months In Prison For Trafficking Counterfeit Military Goods* (Oct. 6, 2015), available at https://www.justice.gov/opa/pr/massachusetts-man-sentenced-37-months-prison-trafficking-counterfeit-military-goods-0.
[348] *Id.*

- Jeffrey Krantz was fined $100,000 and sentenced to three years of probation in December 2015 for supplying customers with falsely remarked microprocessor chips, many of which were used in U.S. military and commercial helicopters. Krantz sold over a thousand chips to his co-conspirator, Jeffrey Warga (see below), who then resold them to a Connecticut company that wanted new and original chips. Over 300 chips were rejected by the Connecticut company because they contained the wrong die inside; over 900 others had altered date codes. Krantz and Warga knew the chips were from a supplier in China and that there was a high probability that they were remarked and were not authentic product.[349]

- In 2016, Jeffrey Warga was fined $10,000 and sentenced to three years of probation for his role in conspiring with Jeffrey Krantz to supply customers with falsely remarked microprocessor chips, many of which were used in U.S. military and commercial helicopters.[350]

- Rogelio Vasquez, the owner of PRB Logics Corporation (a California seller of electronic components) was arrested in May 2018 for selling counterfeit integrated circuits, some of which could have been used in military applications. A 30-count indictment alleged that Vasquez "acquired old, used and/or discarded integrated circuits from Chinese suppliers that had been repainted and remarked with counterfeit logos. The devices were further remarked with altered date codes, lot codes or countries of origin to deceive customers and end users into thinking the integrated circuits were new, according to the indictment. Vasquez then sold the counterfeit electronics as new parts made by manufacturers such as Xilinx, Analog Devices and Intel."[351] Vasquez was charged with wire fraud, 20 counts of trafficking in counterfeit goods, and one count of trafficking in counterfeit military goods.[352] He was sentenced to 46 months in prison and ordered to pay $144,000 in restitution. The press release announcing his sentencing further

[349] Department of Justice, U.S. Attorney's Office, District of Connecticut, Press Release: *New York Man Who Supplied Falsely Remarked Computer Chips Used in U.S. Military Helicopters is Sentenced* (Dec. 10, 2015), available at https://www.justice.gov/usao-ct/pr/new-york-man-who-supplied-falsely-remarked-computer-chips-used-us-military-helicopters.
[350] Department of Justice, U.S. Attorney's Office, District of Connecticut, Press Release: *Owner of Rhode Island Electronics Parts Company that Defrauded Customers is Sentenced* (January 21, 2016), available at https://www.justice.gov/usao-ct/pr/owner-rhode-island-electronics-parts-company-defrauded-customers-sentenced.
[351] Department of Justice, U.S. Attorney's Office, Central District of California, Press Release: *Orange County Electronics Distributor Charged with Selling Counterfeit Integrated Circuits with Military and Commercial Uses* (May 1, 2018), available at https://www.justice.gov/usao-cdca/pr/orange-county-electronics-distributor-charged-selling-counterfeit-integrated-circuits.
[352] *Id.*

disclosed that some of the counterfeit parts sold by Vasquez ultimately ended up in a classified weapon system used by the U.S. Air Force.[353]

6. Industry Standards

A number of industry standards have been created to address various aspects of counterfeit mitigation and prevention, including both business practices and testing of parts. Henry Livingston of BAE Systems maintains a matrix of the many standards relating to counterfeiting, including scope, dates of release and revision, adoption by DoD, appropriate users, and subject matter.[354] A few of the standards relevant to counterfeit avoidance and prevention are discussed below.

a. IDEA

The Independent Distributors of Electronics Association ("IDEA") is an association of independent distributors that promotes quality initiatives in the supply chain.[355] It focuses on disseminating information to its members and other independent distributors with the goal of "stamping out counterfeit components."[356] IDEA provides Responsible Procurement Solutions™, a process for procurement of electronic components, inspection, and disposition of suspect counterfeits.[357] Faiza Khan, the Executive Director of IDEA, stated that IDEA's mission "is to ensure that what goes in an independent distributor's door and then goes out to a purchaser should never be substandard."[358]

IDEA created a set of standards for purchasing and handling of electronic components, which were intended to let the industry know that IDEA's member companies do not wish to be associated with unethical businesses which had given independent distributors an extremely poor reputation in the supply chain.[359] IDEA currently has two standards by which its members must abide: IDEA-STD-1010 (Acceptability of Electronic Components Distributed in the Open Market) and IDEA-QMS-9090 (Quality

---

[353] Department of Justice, U.S. Attorney's Office, Central District of California, Press Release: *O.C. Businessman Sentenced to 46 Months in Prison for Selling Counterfeit Integrated Circuits with Military and Commercial Uses* (May 30, 2019), available at https://www.justice.gov/usao-cdca/pr/oc-businessman-sentenced-46-months-prison-selling-counterfeit-integrated-circuits.
[354] Henry Livingston, *Counterfeit Avoidance and Detection Standards for Hardware Products,* (last updated June 2020), available at https://counterfeitparts.files.wordpress.com/2020/06/standards_analysis_20200610.pdf.
[355] Faiza Khan Interview Summary (Appendix 19), at 1.
[356] *Id.* at 1.
[357] *See* https://www.idofea.org/about.html.
[358] Faiza Khan Interview Summary, at 1.
[359] *Id.* at 1.

Management System Standard for Independent Distributors of Electronics Association Members).[360] A new purchasing standard directed to buyers is also under development.[361]

The original IDEA-STD-1010 was released in October 2006, and the current version, IDEA-STD-1010-B was released in April 2011.[362] Ms. Khan indicated that the next revision, IDEA-STD-1010-C, is currently under development and should be available near the end of 2021.[363] IDEA-STD-1010-B relates to visual inspection and distinguishes between counterfeit and substandard parts.[364] It defines a "counterfeit product" as "[a]ny part, documentation, packaging, labeling, or identifying information that has been modified so as to fraudulently misrepresent authenticity."[365] "Substandard," on the other hand, means a "device that does not meet the manufacturer's stated specifications for form, fit, or function."[366]

The standard includes requirements for product handling, packaging, and storage, and addresses issues such as electrostatic discharge, moisture sensitivity, floor life and shelf life, and oxidation risk.[367] Testing facilities must be qualified, including ISO Certification at a minimum and consideration of issues such as available equipment, business practices, and personnel.[368] Extensive testing and inspection requirements and guidelines are provided, including step-by-step instructions for evaluating packing materials and detailed physical examination of parts (including visual inspection, solvent tests, and mechanical inspection).[369] Advanced inspection techniques which may be useful in detecting further indicators of counterfeit products are also described, including solderability testing, fluorescent dye penetrant, x-ray fluorescence ("XFR") analysis, x-ray examination, acoustic microscopy ("AM") testing, and decapsulation.[370] Numerous photographs, drawings, and graphs are provided to illustrate every step in the testing and inspection process. Section 12 contains 181 photographs comparing acceptable and

[360] *Id.* at 1; *see also* https://www.idofea.org/idea-products/quality-standards.html.
[361] Faiza Khan Interview Summary, at 1.
[362] Independent Distributors of Electronics Association, IDEA-STD-1010-B: *Acceptability of Electronic Components Distributed in the Open Market* (hereinafter IDEA-STD-1010-B) (2011).
[363] Faiza Khan Interview Summary, at 1.
[364] *Id.* at 2.
[365] IDEA-STD-1010-B § 5.9. Ms. Khan observed that while some people also include refurbished parts as counterfeits, IDEA classifies refurbished parts as "substandard." She indicated that IDEA does not want to use the "counterfeit" label too loosely. *See* Faiza Khan Interview Summary, at 2.
[366] IDEA-STD-1010-B § 5.9.
[367] *Id.* at § 6.
[368] *Id.* at § 8.
[369] *Id.* at § 10.
[370] *Id.* at § 11.

nonconforming product conditions.[371] Finally, the standard provides detailed inspection checklists and a lengthy list of other relevant standard generating bodies and associations.[372]

IDEA-QMS-9090, the Quality Management Standard, is intended for use by IDEA members, although other independent distributors may also use it as guidance.[373] This standard addresses issues relating to storage and shipment of parts, such as moisture sensitivity, storage conditions, limiting access to warehouses, escrow payments, and use of drop shipments. Organizations are required to have a Control of Nonconforming Material process in place that includes "instructions to segregate counterfeit product in a controlled area and disposition counterfeit product to prevent it from re-entering the supply chain."[374] In addition, the organization must report the counterfeit product to IDEA, ERAI, GIDEP, and/or appropriate government agencies within 60 days after confirming that it is counterfeit.[375]

b. SAE International

SAE International describes itself as "a global association of more than 128,000 engineers and related technical experts in the aerospace, automotive and commercial vehicle industries."[376] One of SAE's core competencies is voluntary consensus standards development.[377] SAE's Aerospace Council contains multiple technical committees charged with creating standards relating to counterfeit prevention and mitigation. The G-19 Counterfeit Electronic Components Committee was created in November 2007 to address aspects of preventing, detecting, responding to, and counteracting the threat of counterfeit electronic components.[378] The G-21 Counterfeit Materiel Committee was organized in October 2010 to address aspects of preventing, detecting, responding, and counteracting the threat of counterfeit materiel.[379]

i) SAE AS5553

SAE AS5553, entitled "Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition," was issued in April 2009 for use by organizations

---

[371] *Id.* at § 12.
[372] *Id.* at §§ 14, 16.
[373] *See* Faiza Khan Interview Summary, at 2.
[374] Independent Distributors of Electronics Association, IDEA-STD-9090: *Quality Management System Standard for Independent Distributors of Electronics Association Members* § 10.1 (2018).
[375] *Id.* at § 10.2.
[376] SAE International, *About Us*, available at https://www.sae.org/about.
[377] *Id.*
[378] SAE Aerospace, Committee Charter, SAE G-19 Counterfeit Electronic Components Committee (Nov. 2007), available at https://www.sae.org/servlets/works/committeeHome.do?comtID=TEAG19.
[379] SAE Aerospace, Committee Charter, SAE G-21 Counterfeit Materiel Committee (October 2010), available at https://www.sae.org/servlets/works/committeeHome.do?comtID=TEAG21.

that procure, integrate, or repair EEE parts or assemblies.[380] The standard has been updated three times since then, with the current version, AS5553C, issuing in March 2019. The standard states that it was created "in response to continually evolving, significant, and increasing risk of counterfeit electrical, electronic, and electromechanical (EEE) parts entering the aerospace supply chain, posing significant performance, reliability, and safety risks."[381]

SAE AS5553C defines a "counterfeit EEE part" as either an "unauthorized (a) copy, (b) imitation, (c) substitute, or (d) modified EEE part, which is knowingly, recklessly, or negligently misrepresented as a specified genuine item from an original component manufacturer or authorized aftermarket manufacturer;" or a "previously used EEE part which has been modified and is knowingly, recklessly, or negligently misrepresented as new without disclosure to the customer that it has been previously used."[382] The standard notes that its definition may differ from civil or criminal laws relating to counterfeiting, and it suggests that used parts sold as new may not be viewed as counterfeit under some civil and criminal statutes.[383]

SAE AS5553C requires organizations to develop and implement "a risk-based counterfeit EEE parts control plan" that documents the processes used for "risk identification, mitigation, detection, avoidance, disposition, and reporting of suspect counterfeit or counterfeit parts and/or assemblies containing such EEE parts."[384] These processes include training of personnel and purchasing parts from authorized sources whenever possible.[385] The standard further provides for use of a documented risk assessment and risk mitigation process, including testing and inspection, when parts are not available from the authorized sources.[386] Flow downs, traceability, and reporting are also required.[387] AS5553 was adopted by the DoD on August 31, 2009.

ii) SAE AS6171

SAE AS6171 ("Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, Electromechanical Parts") was issued in October 2016, and the current revision, SAE

[380] SAE International, AS5553C: *Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition* (hereinafter "SAE AS5553C"), at 3 (2019).
[381] *Id.* at 1.
[382] *Id.* at § 2.2.2.
[383] *Id.*
[384] *Id.* at § 3.1.
[385] *Id.* at §§ 3.1.1, 3.1.3. The standard also adopts the language from DFARS Contract Clause 7008, which authorizes procurement of parts from suppliers who obtain electronic parts exclusively from authorized sources, when those parts are still in production or available in stock. *Id.* at 7.
[386] *Id.* at § 3.1.3.
[387] *Id.* at §§ 3.1.4, 3.1.7, 3.1.8.

AS6171A, was released in April 2018.[388] The standard was adopted by the DoD on March 28, 2017. SAE AS6171A states that it "provides uniform general requirements, practices, and methods for testing Electrical, Electronic, and Electromechanical (EEE) parts to mitigate the risks of receiving or using Suspect/Counterfeit (SC) EEE parts."[389] It is intended to be used in conjunction with individual AS6171 "slash sheets" that provide "detailed requirements for testing as well as methods of calculation of counterfeit defect and counterfeit type coverages by a sequence of tests."[390]

SAE AS6171A uses a definition of "counterfeit part" which is similar but not identical to that used in SAE AS5553. SAE AS6171A defines a "counterfeit part" as "[a]n unauthorized (a) copy, (b) imitation, (c) substitute, or (d) modified part, which is knowingly, recklessly, or negligently misrepresented as a specified genuine part of an authorized manufacturer;" or a "previously used electronic part which has been modified and is knowingly, recklessly, or negligently misrepresented as new without disclosure to the customer that it has been previously used."[391] It then lists and describes seven counterfeit part types: recycled parts, remarked parts, overproduced parts, out-of-specification/defective parts, cloned parts, forged documentation/part substitution, and tampered parts.[392] A "suspect counterfeit part" is a part "for which there is objective, credible evidence indicating that the part is likely a Counterfeit Part."[393]

The AS6171A standard is applicable where parts have an unknown chain of custody, have been acquired from a broker or independent distributor, or when other risk elements have raised concerns that parts may be counterfeit.[394] A risk assessment model is used to quantify the level of risk associated with the use of a part obtained from an unauthorized supplier, and testing sequences are then recommended based on a resulting risk score.[395] AS6171A requires testing laboratories to work closely with the party requesting testing in determining the legitimacy of the parts to be inspected. The test laboratory is also encouraged to work with the authorized manufacturer of the parts in determining the risk that the parts are counterfeit.[396]

---

[388] SAE International, AS6171: *Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts*, Rev. A, at 1 (2018) [hereinafter "SAE AS6171A"].
[389] *Id.* at 1.
[390] *Id.* at 1. The standard lists 11 slash sheets addressing different techniques for detection of suspect/counterfeit EEE parts. *See id.* at § 2.1.1.
[391] *Id.* at § 2.2.4.
[392] *Id.* at § 2.2.4.
[393] *Id.* at § 2.2.1.
[394] *Id.* at § 1.1.
[395] *Id.* at § 3.1.
[396] *Id.* at § 3.

AS6171A sets out numerous part detection testing methods which are described in detail in the following AS6171 Slash Sheets:

- AS6171/1: Suspect/Counterfeit Test Evaluation Method

- AS6171/2: Techniques for Suspect/Counterfeit EEE Parts Detection by External Visual Inspection, Remarking and Resurfacing, and Surface Texture Analysis Test Methods. External visual inspection methods are designed to identify a high percentage of recycled and remarked counterfeit parts. The parts are inspected for alterations of markings and accompanying paperwork, and optical inspection at a suitable magnification is used to ensure that date and lot codes fall within the expected range. Further testing can include subjecting a small number of parts to destructive Remarking and Resurfacing tests.[397]

- AS6171/3: Techniques for Suspect/Counterfeit EEE Parts Detection by X-ray Fluorescence Test Methods. XFR spectroscopy is a non-destructive test used for material composition detection and to determine layer thicknesses in multilayer structures.[398]

- AS6171/4: Techniques for Suspect/Counterfeit EEE Parts Detection by Delid/Decapsualtion Physical Analysis Test Methods. Used to inspect the die and internal construction of an electronic part. Whenever possible, it is preferable to compare the part under inspection with an authentic part from the authorized manufacturer.[399]

- AS6171/5: Techniques for Suspect/Counterfeit EEE Parts Detection by Radiological Test Methods. Internal and external inspection intended to detect deliberate misrepresentation or damage.[400]

- AS6171/6: Techniques for Suspect/Counterfeit EEE Parts Detection by Acoustic Microscopy (AM) Test Methods. Ultra-high frequency ultrasound used to identify and characterize latent defects such as cracks, voids, delaminations, and sub-surface flaws.[401]

- AS6171/7: Techniques for Suspect/Counterfeit EEE Parts Detection by Electrical Test Methods. Intended to determine whether the part operates in accordance with part specifications.[402]

- AS6171/8: Techniques for Suspect/Counterfeit EEE Parts Detection by Raman Spectroscopy Test Methods. Used for identification of materials.[403]

- AS6171/9: Techniques for Suspect/Counterfeit EEE Parts Detection by Fourier Transform Infrared Spectroscopy (FTIR) Test Methods. Another test used for identification of materials.[404]

---

[397] *Id.* at § 4.
[398] *Id.*
[399] *Id.*
[400] *Id.*
[401] *Id.*
[402] *Id.*
[403] *Id.*
[404] *Id.*

- AS6171/10: Techniques for Suspect/Counterfeit EEE Parts Detection by Thermogravimetric Analysis (TGA) Test Methods. By exposing a sample to a precisely controlled temperature and monitoring weight change, a compositional analysis can be obtained and then compared to an authentic part or a specification.[405]

- AS6171/11: Techniques for Suspect/Counterfeit EEE Parts Detection by Design Recovery Test Methods. A reverse engineering method used to recover design information, which could then be compared to an authentic part or a documented original design.[406]

The AS6171/2 Slash Sheet is arguably the most relevant to the second part of this report, which relates to machine vision technologies.

iii) SAE AS6081

SAE AS6081 ("Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors") was issued in November 2012,[407] and it was adopted by the DoD on June 10, 2013. The standard states that it was created in response to "a significant and increasing volume of fraudulent/counterfeit electronic parts entering the aerospace supply chain, posing significant performance, reliability, and safety risks," and it attributes many of these parts to purchases from sources other than OCMs or their authorized agents.[408] To mitigate the risk of buying, receiving, and selling fraudulent or counterfeit parts, AS6081 standardizes practices for distributors of EEE parts purchased and sold from the Open Market,[409] including practices relating to supplier management, procurement, inspection, testing, and evaluation.[410]

The standard utilizes definitions of "counterfeit part," "fraudulent part," and "suspect part" which once again differ from the definitions in SAE AS5553 and AS6171A. For purposes of AS6081, a "counterfeit part" is 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."[411] A "fraudulent part" is "[a]ny suspect part misrepresented to the

[405] *Id.*
[406] *Id.*
[407] SAE International, AS6081, *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors* (Nov. 2012) [hereinafter "SAE AS6081"].
[408] *Id.* at 1.
[409] The "Open Market" is defined as the "trading market that supplies parts that are not exclusively from or directly traceable to the OCM or authorized (franchised) distributors." It includes the purchase and sale of parts where full supply chain traceability is unknown, such as parts salvaged from electronic waste. *Id.* at § 3.4.20.
[410] *Id.* at 1, 3.
[411] *Id.* at § 3.3.

Customer as meeting the Customer's requirements."[412] A "suspect part" is 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 in the standard.[413]

AS6081 requires covered distributors[414] to develop and implement a fraudulent/counterfeit electronic parts control plan that documents the distributor's processes used for risk mitigation, disposition, and reporting of fraudulent and counterfeit parts.[415] Those processes include an assessment of potential suppliers to determine the risk of receiving fraudulent or counterfeit parts and creation of a list of approved suppliers.[416] The distributor's plan must preclude purchasing parts from suppliers that have repeatedly failed to detect and avoid fraudulent or counterfeit parts. Instead, the distributor must only purchase new and authentic parts from OCMs or their authorized distributors, or from suppliers who obtain such parts exclusively from the OCM or authorized distributors, when parts are available from such sources and can meet the customer's delivery requirements.[417] The distributor must retain records documenting supply chain traceability wherever possible.[418]

If parts are procured from a source other than an OCM or an authorized distributor, or if there is some reason to doubt a part's authenticity, then the distributor must perform tests and inspections intended to detect fraudulent and counterfeit parts.[419] The standard provides a minimum testing plan that includes inspection of documentation and packaging, external visual inspection, inspection for remarking and resurfacing, X-ray inspection, lead finish evaluation, and internal analysis of a representative sample by delidding or decapsulation followed by optical examination under magnification.[420] However, SAE AS6081 does not address the need for risk-based testing. When parts are identified as suspect, fraudulent or counterfeit, they must be physically identified (e.g., labeling, marking); physically segregated from acceptable, non-suspect parts and placed in quarantine; and the supplier must be notified and provided

[412] *Id.* at § 3.2.
[413] *Id.* at § 3.1.
[414] The standard uses the term "organization," which refers to distributors that supply electronic parts from any source other than an OCM or an authorized distributor. It includes independent distributors and brokers, as well as authorized distributors which are sourcing parts from outside the OCM's authorized supply chain. *See id.* at § 3.4.21.
[415] *Id.* at § 4.2. Requirements must also be flowed down to the distributor's suppliers, contractors, and subcontractors.
[416] *Id.* at § 4.2.2.
[417] *Id.*
[418] *Id.* at § 4.2.4.
[419] *Id.* at § 4.2.6.4.
[420] *Id.*

with the opportunity to verify the findings.[421] Suspect or confirmed fraudulent/counterfeit parts must be controlled to prevent their use or reentry into the supply chain, and within 60 days must be reported to customers, Government authorities and GIDEP, industry reporting programs such as ERAI, and appropriate law enforcement authorities.[422]

iv) SAE AS6496

SAE AS6496 was issued in August 2014 to enhance the effectiveness of existing practices within the authorized distribution channel for mitigating the risk that fraudulent and/or counterfeit parts will enter the supply chain.[423] It is recommended for use by authorized distributors that are purchasing and selling electronic components, supplies, and equipment which were acquired directly from the manufacturer or another authorized distributor,[424] and it focuses on commercial practices rather than inspection and testing. AS6496 adopts definitions of "counterfeit part" and "fraudulent part" that are identical to the definitions contained in AS6081.[425] However, AS6496 defines a "suspect part" as a part "which may indicate by visual inspection, testing, or other information that it may be counterfeit and/or fraudulent."[426]

SAE AS6496 requires the authorized distributor to develop and implement a plan that documents its processes used for risk mitigation, disposition, and reporting of suspect and confirmed counterfeit parts.[427] At a minimum, it must have a distribution agreement in place with any manufacturer it represents as an authorized distributor, and it must provide the full manufacturer's warranty to the customer.[428] When acting as an authorized distributor, the organization must purchase parts for resale only from the manufacturer (or from another authorized distributor of the same manufacturer); however, purchasing directly from the manufacturer is preferred.[429] Emphasis is placed on traceability back to the

---

[421] *Id.* at § 4.2.6.6. If parts are not found to be suspect, fraudulent, or counterfeit following inspection and testing, a report of the inspection and test results must be provided to the customer either in advance of shipment or with the shipment of the parts. *See id.* at § 4.2.6.8.
[422] *Id.* at § 4.2.9. Appendix D to AS6081 contains an extensive list of reporting contacts, including customs agencies for European countries, United Kingdom legal authorities and anti-counterfeiting organizations, and U.S. government agencies and industry reporting programs such as IDEA and ERAI. *See* SAE AS6081, Appendix D, at 38-44.
[423] SAE International, AS6496, *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Authorized/Franchised Distribution* (August 2014) [hereinafter "SAE AS6496]. SAE AS6496 was adopted by DLA in March 2017.
[424] SAE AS6496 at § 1.2.
[425] *Id.* at § 2.3.
[426] *Id.* at § 2.3 (emphasis in original).
[427] *Id.* at § 3.2.
[428] *Id.*
[429] *Id.* at § 3.4.2.

manufacturer or another authorized distributor. Records documenting such traceability must be retained (including the certificate of conformance, if provided), and military parts delivered by the distributor must be accompanied by certificates from both the manufacturer and the distributor.[430] If the organization provides a quote for an item for which it is not authorized, it must disclose that to the customer at the time of quotation; in those instances, the distributor is acting as an independent distributor.[431]

The distributor is also required to have a process to evaluate and minimize the risk associated with potential counterfeit product entering into its own inventory, particularly from customer returns.[432] Returns are not disallowed, but if the distributor accepts a return, it must have a process to verify that the returned parts were purchased from that distributor and not from another source.[433] If traceability cannot be verified, or if there is any evidence of alteration, mishandling, or repackaging, the distributor should consider whether the parts are suspect.[434] Suspect, fraudulent, and counterfeit parts must be quarantined and cannot be reintroduced to the supply chain.[435] Counterfeit parts must be reported to appropriate organizations, including customers, GIDEP, and law enforcement authorities.[436]

c. CCAP-101

The Components Technology Institute, an engineering services company located in Huntsville, Alabama, issued the latest version of its CCAP-101 standard in July 2013.[437] CCAP-101 is a certification program for the detection and avoidance of counterfeit electronic components supplied by independent distributors.[438] CCAP-101 apparently offers two alternative definitions of "counterfeit component." In the section entitled "Scope," the standard states that "Counterfeit Electronic Component," as used in this document, "refers to any component which violates any intellectual property rights, trademark or logo, is not new or is not authentic to the requirements of the manufacturer part number ordered by the Customer." [439] In the Definitions section, CCAP-101 defines a "counterfeit component" as "[a] component that has been confirmed to be a copy, imitation, fake, is represented as new and unused or

[430] *Id.* at §§ 3.5, 3.5.1. The term "military parts" is not defined by the standard.
[431] *Id.* at § 3.3.1. If the distributor has unauthorized parts in inventory, they must be segregated from authorized parts. *See id.* at § 3.9.1.
[432] *Id.* at § 3.6.1.
[433] *Id*.
[434] *Id.*
[435] *Id.*
[436] *Id.* at § 3.10.
[437] Components Technology Institute, Inc., CCAP-101, *Counterfeit Parts Avoidance Program, Certification For* (Rev. E-1, July 11, 2013).
[438] *Id.* at 1.
[439] *Id.* Note the definition is so broad that it even encompasses components that infringe upon the patent rights of another.

markings have been altered. All components that cannot be authenticated through test & inspection shall be treated as counterfeit."[440]

The CCAP-101 Counterfeit Components Avoidance Program is "designed to meet the objectives of AS5553 to detect and avoid counterfeit electronic component [sic] purchased from [Independent Distributors]."[441] Nevertheless, CCAP-101 does not address the need for risk-based testing as required by AS5553. Independent distributors must agree that all components certified and delivered under the program have been subjected to the requirements stated in CCAP-101 and that they have performed the due diligence required to avoid delivery of counterfeits.[442] That includes establishing and maintaining a documented quality system that conforms to ISO 9001, as well as the additional requirements set out in the CCAP standard such as inspection, testing, and traceability.[443] Required testing includes microscopic inspection and visual inspection, as well as additional specified tests for particular types of components.[444] The independent distributor is also required to have a formal procedure for selecting, approving, and monitoring its suppliers.[445]

d. Other Standards

The JEDEC Solid State Technology Association, an international standards body, published its JESD243 standard, entitled "Counterfeit Electronic Parts: Non-Proliferation for Manufacturers" in March 2016.[446] JESD243 identifies "the best commercial practices for mitigating and/or avoiding counterfeit products by all manufacturers of electronic parts, including . . . *original component manufacturers* (OCMs), *authorized aftermarket manufacturers*, and other companies that manufacture electronic parts under their own logo, name, or trademark."[447] The standard requires a manufacturing organization's management to define and document its policy for preventing counterfeit electronic parts from entering the supply chain, along with its policy for disposition and reporting of counterfeit and suspect counterfeit parts.[448] In addition, manufacturers are required to develop and implement a counterfeit parts control

[440] *Id.* at 3.
[441] *Id.* at 4.
[442] *Id.*
[443] *Id.* at 5-6. ISO 9001 is an international quality management standard. *See* https://www.iso.org/standard/62085.html.
[444] *Id.* at 7-19.
[445] *Id.* at 7.
[446] JEDEC Solid State Technology Association, JESD243, *Counterfeit Electronic Parts: Non-Proliferation for Manufacturers* (March 2016) [hereinafter "JESD243"].
[447] JESD243, at 1.
[448] *Id.* at § 4.1.

plan, including a list of authorized distributors and a list of approved suppliers.[449] The standard also addresses returns and restocking items into inventory.[450]

The International Electrotechnical Commission prepared a pair of standards on avoiding use of counterfeit electronic parts in avionics. The first standard, IEC 62688-1, addresses avoiding use of counterfeit, fraudulent, and recycled electronic components in avionics.[451] It defines a "counterfeited component" as "material good imitating or copying an authentic material good which may be covered by the protection of one or more registered or confidential intellectual property rights."[452] The companion standard covers management of electronic components from non-franchised sources.[453]

7. Recommendations and Conclusions

Based on the foregoing review and analysis, several recommendations can be made.

a. An Agreed-Upon Definition of "Counterfeit" is Needed

In FY 2012 NDAA Section 818, Congress instructed the Secretary of Defense to establish Department-wide definitions of the terms "counterfeit electronic part" and "suspect counterfeit electronic part" within 180 days after enactment of the Act.[454] Congress specifically indicated that those definitions "shall include previously used parts represented as new."[455] Nevertheless, as the previous discussion has revealed, there is no DoD-wide definition of "counterfeit" or "counterfeit electronic part"; instead, different agencies use slightly different definitions of those terms. Further, standard setting organizations, industry associations, and other federal laws and regulations use widely varying definitions of the term "counterfeit" and related terms.

Some of the current definitions include the following:

---

[449] *Id.* at § 4.2.
[450] *Id.* at § 4.3. In November 2016, JEDEC published a revised version of JESD31, *General Requirements for Authorized Distributors of Commercial and Military Semiconductor Devices*. JESD31 identifies general requirements for authorized distributors that supply commercial and military products, including semiconductors, integrated circuits, and hybrids. *See* JEDEC Solid State Technology Association, JESD31E, *General Requirements for Authorized Distributors of Commercial and Military Semiconductor Devices* (Nov. 2016).
[451] International Electrotechnical Commission, IEC 62668-1:2019, *Process management for avionics – Counterfeit prevention – Part 1: Avoiding the use of counterfeit, fraudulent and recycled electronic components* (2019-09).
[452] *Id.* at § 3.1.5.
[453] International Electrotechnical Commission, IEC 62688-2:2019, *Process management for avionics – Counterfeit prevention – Part 2: Managing electronic components from non-franchised sources* (2019-09).
[454] FY 2012 NDAA § 818(b)(1).
[455] *Id.*

- DFARS § 202.101: *Counterfeit electronic part* means an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.[456]

- DoD Instruction 4140.01: "Counterfeit materiel" is "[m]ateriel whose identity or characteristics have been deliberately misrepresented, falsified, or altered without legal right to do so."[457]

- DoD Instruction 4140.67: "Counterfeit materiel" is "[a]n item that is an unauthorized copy or substitute that has been identified, marked, 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."[458]

- SECNAV Instruction 4855.20A: "Counterfeit materiel" includes "[i]tems that are unauthorized copies or substitutes that have been identified, marked, or altered by a source other than the items' legally authorized source or have been misrepresented to be authorized items of the legally authorized source."[459]

- IDEA-STD-1010-B: A "counterfeit product" is "[a]ny part, documentation, packaging, labeling, or identifying information that has been modified so as to fraudulently misrepresent authenticity."[460]

- SAE AS5553C: A "counterfeit EEE part" is:
  1. An unauthorized (a) copy, (b) imitation, (c) substitute, or (d) modified EEE part, which is knowingly, recklessly, or negligently misrepresented as a specified genuine item from an original component manufacturer or authorized manufacturer; or
  2. A previously used EEE part which has been modified and is knowingly, recklessly, or negligently misrepresented as new without disclosure to the customer that it has been previously used.[461]

- SAE AS6171A: A "counterfeit part" is:
  1. An unauthorized (a) copy, (b) imitation, (c) substitute, or (d) modified part, which is knowingly, recklessly, or negligently misrepresented as a specified genuine part of an authorized manufacturer; or

---

[456] 48 C.F.R. § 202.101.
[457] DoD Instruction 4140.01 § G.2, at 19.
[458] DoD Instruction 4140.67, Glossary, at 12.
[459] SECNAV Instruction 4855.20A, Enclosure 2 (Definitions) (2018).
[460] IDEA-STD-1010-B § 5.9.
[461] SAE AS5553C § 2.2.2 (March 2019). This differs substantially from the definition used in SAE AS5553A, which defined a counterfeit as "[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." *See* SAE AS5553A, *as cited by* 79 Fed. Reg. 26092, 26093 (May 6, 2014).

2. A previously used electronic part which has been modified and is knowingly, recklessly, or negligently misrepresented as new without disclosure to the customer that it has been previously used.[462]

- SAE AS6174A: "Counterfeit materiel" is "[f]raudulent materiel 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."[463]

- SAE AS6496 and AS6081: A "counterfeit part" is "[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."[464]

- CCAP-101: A "counterfeit component" is "[a] component that has been confirmed to be a copy, imitation, fake, is represented as new and unused or markings have been altered. All components that cannot be authenticated through test & inspection shall be treated as counterfeit."[465]

- JEDEC Standard JESD243: "Counterfeit part" means "[a]n unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer."[466]

- IEC 62688-1: A "counterfeited component" is "material good imitating or copying an authentic material good which may be covered by the protection of one or more registered or confidential intellectual property rights."[467]

- Lanham Act: A "counterfeit" is a "spurious mark which is identical with, or substantially indistinguishable from, a registered mark."[468]

- 18 U.S.C. § 2320: For purposes of criminal liability, the term "counterfeit mark" means:
  (A) a spurious mark –
  (i) that is used in connection with trafficking in any goods, services, labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging of any type or nature;

[462] SAE AS6171A § 2.2.4.
[463] SAE AS6174A § 2.3.5.
[464] SAE AS6496 § 2.3; SAE AS6081 § 3.3.
[465] Components Technology Institute, Inc., CCAP-101, *Counterfeit Components Avoidance Program, Certification For* (Rev. E-1, 2013), at 3.
[466] JEDEC Solid State Technology Association, JESD243, Counterfeit Electronic Parts: Non-Proliferation for Manufacturers § 3 (2016).
[467] International Electrotechnical Commission, IEC 62668-1:2019, *Process management for avionics – Counterfeit prevention – Part 1: Avoiding the use of counterfeit, fraudulent and recycled electronic components* (2019-09), at § 3.1.5.
[468] 15 U.S.C. § 1127.

(ii) that is identical with, or substantially indistinguishable from, a mark registered on the principal register in the United States Patent and Trademark Office and in use, whether or not the defendant knew such mark was so registered;

(iii) that is applied to or used in connection with the goods or services for which the mark is registered with the United States Patent and Trademark Office, or is applied to or consists of a label, patch, sticker, wrapper, badge, emblem, medallion, charm, box, container, can, case, hangtag, documentation, or packaging of any type or nature that is designed, marketed, or otherwise intended to be used on or in connection with the goods or services for which the mark is registered in the United States Patent and Trademark Office; and

(iv) the use of which is likely to cause confusion, to cause mistake, or to deceive; or

(B) a spurious designation that is identical with, or substantially indistinguishable from, a designation as to which the remedies of the Lanham Act are made available by reason of section 220506 of title 36.[469]

The definitions disagree on several important points. First, the Lanham Act and the criminal statute (18 U.S.C. § 2320) focus on registered trademarks, while the DFARS definition, DoD Instructions, and industry standards focus on various other attributes of the parts themselves. The DFARS definition of "counterfeit electronic part" includes used electronic parts represented as new, as well as the false identification of grade, serial number, lot number, date code, or performance characteristics.

Next, the level of intent that is required differs greatly. DFARS § 202.101 and JEDEC JESD243 both require that a part be "*knowingly* mismarked, misidentified, or otherwise misrepresented." DoD Instruction 4140.01 requires that materiel be "*deliberately* misrepresented, falsified, or altered," while DoD Instruction 4140.67 and SECNAV Instruction 4855.20A only require that material be "misrepresented," without explicitly requiring that the misrepresentation be intentional, knowing or deliberate. SAE AS5553C and AS6171A both include parts that have been "*knowingly, recklessly, or negligently* misrepresented." Meanwhile, SAE AS6174A, AS6496, and AS6081 apply to "*fraudulent*" parts where there has been an "intent to mislead, deceive, or defraud." IDEA-STD-1010-B also requires a fraudulent misrepresentation of authenticity.

Further, use of the term "fraudulent" is problematic. SAE AS6496 and AS6081 both define a "fraudulent part" as "[a]ny Suspect Part misrepresented to the Customer as meeting the Customer's requirements,"[470] and SAE AS6174A includes a similar definition of "fraudulent materiel."[471] Again, there is no requirement that the misrepresentation be knowing or deliberate. Fraud has been defined as "a

[469] 18 U.S.C. § 2320(f)(1).
[470] SAE AS6496 § 2.3; SAE AS6081 § 3.2.
[471] SAE AS6174A § 2.3.4. SAE AS6174A, AS6496, and AS6081 all include a Venn diagram showing that counterfeit parts or materiel are a subset of fraudulent parts or materiel.

knowing misrepresentation or knowing concealment of a material fact made to induce another to act to his or her detriment."[472] Numerous variations on that definition exist, but all share the common themes of a concealment or a false representation that injures another who relies on it.[473] Often, courts will require that the reliance by the second person be reasonable. Use of the term "fraudulent" in SAE AS6174A, AS6496, and AS6081 does not seem to contemplate any of these elements. The definition of "fraudulent part" in SAE AS6171A, on the other hand, does incorporate those elements: "Any part intentionally misrepresented to the Customer with the intent to deceive, causing the Customer to justifiably rely upon the misrepresented facts, as a result of which the Customer could incur damages."[474] The problem with the inclusion of the word "fraud" as part of the definition of "counterfeit" part or materiel is that it raises the spectre of legal fraud, likely making purchasers and contractors less likely to report instances of counterfeit parts for fear of potential liability for defamation, and it sets a high bar for identifying a part as "counterfeit."

A better approach may be for the DFARS and standards definitions to leave out any reference to intent and focus solely on the fact that the parts have been misrepresented. DoD is concerned with impact on weapons systems, not intent; for DoD, counterfeiting is a contractual issue. Intent and fraud become relevant only in more extreme cases, where a supplier is actively engaged in remarking or tampering with parts. Then, DoD may refer the matter to the appropriate law enforcement officials for investigation and possible prosecution. However, in the garden variety case, where a supplier unknowingly passes a counterfeit part to the next level in the supply chain, it appears that DoD is less concerned with the supplier's intent. Instead, DoD wants to know whether the parts are authentic and reliable. The civil and criminal statutes, on the other hand, are focused on protecting the owners of registered trademarks and ensuring consistent quality of their goods, as well as preventing consumers from being confused about the source of goods. In a trademark infringement case, it is not necessary that the defendant acted intentionally, although intentional conduct may be required for a finding of willfulness and enhanced damages. In a criminal case for trafficking in counterfeit goods, intentional conduct is required.

As a result, more thought needs to be given to the definition of "counterfeit" used by the different organizations and agencies. Adoption of a uniform definition of "counterfeit" across DoD for purposes of counterfeit prevention and avoidance is needed, which includes conventional counterfeits, clones, and tampered parts. The standards setting organizations should also reach agreement on the definition of a

[472] Bryan A. Garner, ed., BLACK'S LAW DICTIONARY (11th ed. 2019).
[473] *Id.*
[474] SAE AS6171A § 2.2.2.

counterfeit part; certainly, within an organization, there should not be more than one definition in use.[475] However, DoD and the standards organizations should guard against borrowing elements from the civil and criminal statutes, such as intent, which may not be necessary for DoD acquisitions or risk-based approaches to counterfeit detection and mitigation.

b. A Uniform, DoD-Wide Set of Policies and Procedures to Address Prevention, Detection, and Avoidance of Counterfeiting is Needed

In addition to a uniform definition of "counterfeit," DoD should adopt a uniform set of policies and procedures to address prevention, detection, and avoidance of counterfeiting. DoD's acquisition regulations are contained in the DFARS, but DoD also has a complex set of issuances, agency regulations, guidebooks, and other documents that apply only to particular services, departments, or components. For example, the Department of the Navy issued SECNAV Instruction 4855.20A, its Counterfeit Materiel Prevention policy, in 2018.[476] The Army Materiel Command developed a Counterfeit Parts and Materials Prevention Program Guidebook in 2018,[477] although it only provides recommendations and is not binding on Army Materiel Command personnel. Meanwhile, the Army is working on its own counterfeiting regulation and pamphlet, which are expected to issue in late 2020 or early 2021. A source has also indicated that a consulting firm has been developing a counterfeit mitigation guidebook for the Air Force.

While the efforts of these individual groups are clearly worthy of praise, they likely result in redundancies and the potential for inconsistent approaches. Further, it is often not clear whether the policies are mandatory or merely aspirational, and the scope of their reach may be limited. Instead, the DoD should draw on the efforts of these various groups and adopt one uniform, detailed set of policies and procedures to address counterfeit prevention, detection, and avoidance (beyond the general policies set forth in DoD Instruction 4140.67), which could then be adjusted in minor ways as needed by individual agencies and services. These policies and procedures should be more than just suggestions or

[475] One person who was interviewed in connection with this report suggested that the inconsistent definitions in the SAE standards are a reflection of the evolution in thinking about the definition of a "counterfeit." He expects that as the standards are revised, the definitions will be brought into line with one another. *See* Kevin Sink Interview Summary (Appendix 19), at 4.

[476] Department of the Navy, SECNAV Instruction 4855.20A, *Counterfeit Materiel Prevention* (Nov. 5, 2018) [hereinafter "SECNAV Instruction 4855.20A"]. SECNAV Instruction 4855.20A replaced Navy Counterfeit Prevention Policy 4855.20 (adopted April 22, 2015) and canceled NAVSO P-7000 (*Counterfeit Materiel Process Guidebook: Guidelines for Mitigating the Risk of Counterfeit Materiel in the Supply Chain*, adopted June 20, 2017).

[477] Army Materiel Command, Counterfeit Parts and Materials Prevention Program Guidebook (December 2018), available at https://www.dau.edu/cop/dmsms/DAU%20Sponsored%20Documents/AMC%20Counterfeit%20Parts%20and%20Materials%20Guidebook%20V1.0.pdf.

recommendations; they should be requirements that are enforceable across the DoD. They should relate to reporting obligations as well as procurement. After these policies are developed and disseminated, DoD should then dedicate resources to education of program managers, technical personnel, contract officers, logistical and maintenance personnel relating to counterfeit part threats and DoD anti-counterfeit policies and regulations. More effective use of counterfeit subject matter experts from industry, academia, and government should also be supported.

c. Electronic Parts Should Only Be Sourced from OCMs and Authorized Distributors

For many years, industry members and government experts have been advising DoD that its contractors and subcontractors should only buy parts from the authorized supply chain, unless there is simply no other choice. However, Tier One of the DFARS policy section on sources of electronic parts, as well as the corresponding contract clause, provides that for parts that are in production or currently available in stock, the contractor shall obtain such parts from the original manufacturer of the parts, their authorized suppliers, or *suppliers that obtain such parts exclusively from the original manufacturers of the parts or their authorized suppliers*.[478] The last clause in that section ("suppliers that obtain such parts exclusively from the original manufacturers of the parts or their authorized suppliers") should be removed from Tier One, so that contractors and subcontractors are required to obtain parts only from the original manufacturer of the parts or their authorized suppliers.

During interviews conducted in 2020, several subject matter experts clearly argued that contractors should only obtain parts from original manufacturers and their authorized distributors. Robin Gray, the Chief Operating Officer and General Counsel of the Electronic Components Industry Association ("ECIA") expressed concern that Tier One of Contract Clause 7008 creates a huge loophole and raises a number of questions.[479] He asked:

> How can a contractor know that a supplier is really buying exclusively from OCMs and authorized distributors, and not from other sources? Does the manufacturer's warranty flow through? Have the parts been handled properly? Even if the parts are tested and appear to be authentic, are they reliable?[480]

Mr. Gray said this provision relating to suppliers that obtain parts exclusively from OCMs and authorized distributors was intended as a set-aside for small businesses, but he believes it is highly problematic. He recommended that the provision should either be eliminated or, at the very least, it should be moved to Tier Two and should only be an option when parts are no longer in production and are not available from

[478] 48 C.F.R. § 246.870-2(a)(1)(i); 48 C.F.R. § 252.246-7008(b)(1) (emphasis added).
[479] Robin Gray Interview Summary (Appendix 19), at 3.
[480] *Id.* at 3.

the OCM or an authorized distributor. Mr. Gray also pointed out that many authorized distributors are, in fact, small businesses.[481]

Andrew Olney, the General Manager of Technology Development at Analog Devices, Inc., repeatedly stated that purchasing from authorized distribution channels is the only solution to the counterfeiting problem.[482] Mr. Olney indicated he does not believe that obsolescence provides an excuse for purchasing from unauthorized sources. He stated that Analog very rarely obsoletes parts that go into government systems; the company has parts dating back to the 1970s, and it continues to manufacture parts specifically so that the government will not have to purchase from unauthorized sources.[483] Even in those instances when a part does go out of production, Mr. Olney observed that the government can still purchase parts from a company such as Rochester Electronics (an authorized distributor and licensed manufacturer) and authorized resellers that distribute legacy products.[484]

Dr. Brian Cohen, retired from the Institute for Defense Analyses, also suggested that "the most compelling business case is to only buy parts from an OCM or an authorized distributor."[485] Dr. Cohen said that people tend to ignore this solution, even though it presents a very low risk of counterfeits. He suggested that if parts cannot be obtained through the authorized distribution chain, then boards should probably be redesigned in order to manage risk rather than going to the grey market.[486]

Indeed, in the FY 2017 NDAA, Congress has already instructed the Secretary of Defense to revise the DFARS to require contractors at all tiers to:

> 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 suppliers that meet anticounterfeiting requirements in accordance with regulations issued pursuant to subparagraph (C) or (D) [relating to suppliers identified by DoD or by contractors or subcontractors].[487]

This provision apparently imposes a higher standard: rather than purchasing from suppliers who obtain parts exclusively from the original manufacturers or authorized distributors, suppliers must meet "anticounterfeiting requirements."

---

[481] *Id.* at 3.
[482] Andrew Olney Interview Summary (Appendix 19), at 2.
[483] *Id.* at 3.
[484] *Id.* at 3. *See also* Dan Deisz Interview Summary (Appendix 19), re Rochester Electronics' role in the supply chain.
[485] Dr. Brian Cohen Interview Summary (Appendix 19), at 4.
[486] *Id.* at 4.
[487] FY 2012 NDAA § 818(c)(3)(A)(i), as amended by FY 2017 NDAA § 815 (eff. Dec. 23, 2016).

At the very least, the DFARS should be amended to incorporate this change, as instructed by Congress. Alternatively, Congress should amend Section 818(c) again to require contractors and subcontractors to obtain electronic parts that are in production or currently available in stock only from the original manufacturers of the parts or their authorized dealers or authorized remanufacturers, and not from any other source.

d. Implementation of Section 818 and Subsequent Amendments Should Be Completed

In addition to revising the Tier One provisions regarding sourcing of electronic parts, the remainder of Section 818(c) should finally be implemented. Specifically, Congress instructed the Secretary of Defense to establish qualification requirements pursuant to which the DoD may identify suppliers that have appropriate policies and procedures in place to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts.[488] This provision has yet to be implemented.

Instead, DFARS § 246.870-2 states that when parts are not in production by the original manufacturer or an authorized aftermarket manufacturer, and are not currently available in stock from a Tier One supplier, contractors and subcontractors are required to obtain electronic parts from suppliers identified by the Contractor as contractor-approved suppliers, provided that—

> (A) For identifying and approving such contractor-approved suppliers, the contractor uses established counterfeit prevention industry standards and processes (including inspection, testing, and authentication), such as the DoD-adopted standards at https://assist.dla.mil;
>
> (B) The contractor assumes responsibility for the authenticity of parts provided by such contractor-approved suppliers (see 231.205-71); and
>
> (C) The selection of such contractor-approved suppliers is subject to review, audit, and approval by the Government, generally in conjunction with a contractor purchasing administration office, or if the Government obtains credible evidence that a contractor-approved supplier has provided counterfeit parts. The contractor may proceed with the acquisition of electronic parts from a contractor-approved supplier unless otherwise notified by DoD.[489]

While Section 818(c)(3)(D) does instruct the DoD to issue regulations that authorize contractors and subcontractors to identify and use additional suppliers that meet anti-counterfeiting requirements, Congress did not envision that contractor-approved suppliers would be the only source of electronic parts in Tier Two. Congress specifically instructed the DoD to establish qualification requirements pursuant to which it would identify suppliers that meet anti-counterfeiting requirements, who have in place appropriate policies and procedures to detect and avoid counterfeit electronic parts. That is, DoD would

[488] FY 2012 NDAA § 818(c)(3)(C), as amended by FY 2017 NDAA § 815 (eff. Dec. 23, 2016).
[489] 48 C.F.R. § 246.870-2(a)(ii).

be responsible for establishing qualification requirements for suppliers, and those requirements could then serve as a model for contractors and subcontractors who wanted or needed to identify and use additional suppliers that meet anti-counterfeiting requirements. Instead, all of the burden has been placed on contractors and subcontractors, who must then assume responsibility for the authenticity of parts provided by those suppliers. That appears to be inconsistent with the mandate in Section 818(c), as amended, and may result in a less demanding qualification process.

e. Flow Downs Should Be Imposed at All Levels, Along with Auditing of Contractors with Respect to Flow Down Requirements

It is critical that flow downs be imposed at the level where discrete components are being purchased by subcontractors. If flow downs are only imposed at a higher level, where systems are being supplied to a prime contractor or first level subcontractor, the flow downs are ineffective at preventing counterfeit parts from being integrated into the system. At that point, counterfeit parts may already be present in a system, and testing may be less effective at detecting their presence.

Contractors who are subject to Cost Accounting Standards are required to establish and maintain an acceptable counterfeit electronic part detection and avoidance system.[490] That requirement includes flow down of counterfeit detection and avoidance requirements, including applicable system criteria, to *subcontractors at all levels* in the supply chain that are responsible for buying or selling electronic parts or assemblies containing electronic parts, or for performing authentication testing.[491] The regulations further provide that the contractor must include the substance of Contract Clause 7007 in subcontracts, including subcontracts for commercial items, for electronic parts or assemblies containing electronic parts.[492]

For contracts that are not subject to Cost Accounting Standards, if the contractor obtains an electronic part from a subcontractor that refuses to accept flow down of Contract Clause 7008, the contractor must do the following:

> (A) Promptly notify the Contracting Office in writing. . . .
>
> (B) Be responsible for inspection, testing, and authentication, in accordance with existing industry standards; and

[490] 48 C.F.R. § 252.246-7007(b).
[491] 48 C.F.R. § 252.246-7007(c)(9).
[492] 48 C.F.R. § 252.246-7007(e). Contract Clause 7008, which applies to all contracts (i.e., not only CAS covered contracts) similarly provides that the contractor shall include the substance of Contract Clause 7008 in subcontracts, including subcontracts for commercial items, that are for electronic parts or assemblies containing electronic parts, unless the subcontractor is the original manufacturer.

> (C) Make documentation of inspection, testing, and authentication of such electronic parts available to the Government upon request.[493]

That is, the contractor remains responsible for a subcontractor that refuses to accept flow down.

Nevertheless, individuals who were interviewed in connection with this report indicated that contractors often do not understand that they are responsible for their subcontractors and do not appreciate that they must flow down counterfeit detection and avoidance requirements to subcontractors, while others stated that subcontractors may push back against flow downs. One source indicated that when subcontractors resist and attempt to negotiate flow downs, it often indicates they are not familiar with government contracting.[494]

Conversely, Robert Bodemuller, a Supply Chain Quality Principle Engineer in the Missiles and Fire Control division at Lockheed Martin, stated that he is responsible for inclusion of counterfeit prevention language in the corporate acquisition contracts that his division uses with its subcontractors. Lockheed's CorpDoc3 (one of Lockheed's standard corporate documents used by Missiles and Fire Control) requires sellers to flow down counterfeit prevention language in lower tier subcontracts for the delivery of items that will be included in or furnished as "Work" to Lockheed.[495] Mr. Bodemuller also discussed Lockheed's audits of its suppliers. Several types of audits are routinely conducted, including AS9100 and counterfeit prevention surveys. If nonconformances are identified during the audit, corrective actions could be developed, including education and implementation of new processes. According to Mr. Bodemuller, the most common nonconformance Lockheed finds is that suppliers may not know when to use authorized distribution and may not understand when a particular distributor is authorized.[496]

Contractors and subcontractors must be educated to understand the requirements of the DFARS and, particularly, the requirement that counterfeit detection and avoidance requirements must be flowed down to subcontractors at all levels. Further, more thorough auditing of contractors and subcontractors should be considered with respect to flow down of requirements through multiple tiers of the supply chain down to the part procurement level.

---

[493] 48 C.F.R. § 252.246-7008(b)(3)(i).
[494] Interview with Anonymous Source (notes in possession of authors).
[495] Robert Bodemuller Interview Summary (Appendix 19), at 3.
[496] *Id.* However, Mr. Bodemuller noted that Lockheed does not believe it has an obligation to audit at the lower tiers of the supply chain.

f. DoD Should Require Compliance with the SAE AS6171 Standards for Risk-Based Testing to Determine Authenticity and Reliability of Electronic Parts

DFARS Section 246.870-2 and Contract Clause 7007 require contractors to establish and maintain a counterfeit part detection and avoidance system, which must include risk-based policies and procedures that address a minimum of 12 issues.[497] However, aside from providing a list of minimum considerations, the regulations do not define a "risk-based system" of counterfeit part detection and prevention, and contractors are not provided with any guidance about how to balance the relevant risks against the time and costs involved in testing.

The SAE AS6171 family of standards adopted a risk-based methodology to determine the level of testing that should be utilized to manage the risk associated with use of an electronic part. The set of standards fills the need created by the regulations by providing contractors with instruction on how to develop a test plan for a particular application and part by assigning a risk level to the part and then prescribing a sequence of tests intended to mitigate the assigned risk. The DFARS requires risk-based testing and other measures as well but is ambiguous about what that means and how to go about assigning risk. DoD Instruction 4140.67 provides some additional clarification by saying risk must be balanced against cost and impact of readiness, but it still provides no guidance on how risk should be assessed or the appropriate level of testing commensurate with any assigned level of risk. As a result, contractors are given too much discretion about how to assign risk and how to select an appropriate level of testing in response. This creates a lack of consistency in the level of confidence that the DoD can apply to the anti-counterfeiting measures taken by its contractors. The adoption of industry standards for assigning risk and determining the appropriate level of testing would provide greater clarity and consistency.

DLA Land and Maritime has already adopted the SAE AS6171 set of standards for use by the DoD, but it is still being called out only infrequently in DoD contracts. In fact, DLA itself has not yet incorporated AS6171 into its Qualified Testing Suppliers List ("QTSL"), but this is a logical step that would ensure the Government's internal supplier of electronic parts is using best practices to secure its inventory. DoD should be more consistent in its requirement of SAE AS6171 for risk-based testing to determine the authenticity of parts acquired in the open market, when parts are not available from the OCM or an authorized distributor.

g. GIDEP Reporting Requirements Should Be Revisited and Clarified

New GIDEP reporting requirements took effect on December 23, 2019, applicable to acquisitions by any federal agency of items subject to higher-level quality standards and items that the contracting

[497] 48 C.F.R. § 246.870-2(b); 48 C.F.R. § 252.246-7007(b), (c).

officer determines to be critical items.[498] The requirements also apply to acquisitions of electronic parts or end items, components, parts, or materials containing electronic parts that are by or for the DoD and that exceed the simplified acquisition threshold.[499] However, the reporting requirements do not apply to acquisitions of commercial items, including commercially available off-the-shelf ("COTS") items.[500]

The new regulations fall short of the reporting requirement called for by Section 818(c)(4) of the FY 2012 NDAA. Section 818(c)(4) required reporting by *any* DoD 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 DoD, or purchased by a contractor or subcontractor for delivery to, or on behalf of, the DoD, contains counterfeit electronic parts or suspect counterfeit electronic parts.[501] By limiting the requirement to acquisitions that exceed the SAT (currently $250,000), the new reporting regulations exclude many acquisitions, and therefore many contractors and subcontractors, from the requirement to report counterfeit and suspect counterfeit electronic parts to GIDEP and other authorities. Many acquisitions of electronic parts, and particularly replacement parts, fall well below the SAT and therefore do not give rise to a reporting obligation under FAR Section 46.317. However, replacement parts are a frequent source of infiltration of counterfeit parts into the DoD supply chain. The regulations should be revised to expand the reporting requirement to include all DoD contracts and contractors, as originally envisioned by Section 818.

As prescribed by Section 818(c)(4), FAR Section 52.246-26 requires contractors to submit a report to GIDEP within 60 days of becoming aware that an item purchased by the contractor for delivery to or for the Government is either a counterfeit or suspect counterfeit item, or a common item that has a major or critical nonconformance.[502] The 60-day time period does not result in prompt reporting, and even after the initial notice is filed, GIDEP may take additional time before it issues a suspect counterfeit alert.[503] This leaves open a large window where other organizations do not know that parts have been identified as suspect counterfeits, and they may potentially be using or supplying the same parts to others. In addition, Section 818 instructed that the regulations were to require reporting to appropriate Government authorities as well, but the newly enacted regulations do not require reporting to any entity other than GIDEP. The regulations should be revised to require reporting to "appropriate Government

[498] 48 C.F.R. § 46.317(a).
[499] *Id.*
[500] 48 C.F.R. § 46.317(b).
[501] FY 2012 NDAA § 818(c)(4).
[502] 48 C.F.R. § 52.246-26.
[503] *See* Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Defense Science Board, *Task Force on Cyber Supply Chain* (2017), at 19.

authorities," and contractors should be provided with guidance about the identity of those authorities and how they can be contacted.

Current business practices surrounding the reporting requirements should also be examined to determine whether they have created a loophole that allows contractors to avoid GIDEP reporting. Richard Smith, the Vice President of Business Development at ERAI, Inc., suggested that when GIDEP reporting became mandated, purchasing agents altered their contractual arrangements to purchases contingent on a non-counterfeit finding, meaning that they would never take possession of suspect counterfeit parts and were thereby alleviated of the requirement to report to GIDEP.[504] Another source confirmed that testing labs which conduct inspections before acceptance often have contractual arrangements with the company that hires them, where the lab agrees that it will not disclose the name of the supplier of suspect counterfeit parts. The testing labs believe they have no obligation to report their results to GIDEP because they are not purchasing the parts, and the contractor feels that it is not required to report because it does not accept the parts.[505] It is unclear what subsequently happens to parts that have been identified as suspect counterfeits which are then not accepted by the contractor.

The regulations create a safe harbor for DoD contractors who submit reports in good faith. The rule provides:

> [t]he Contractor or subcontractor that provides a written report or notification under this clause that the end item, component, part, or material contained electronic parts (i.e., an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly) that are counterfeit electronic parts or suspect counterfeit electronic parts shall not be subject to civil liability on the basis of such reporting, provided that the Contractor or any subcontractor made a reasonable effort to determine that the report was factual.[506]

Potential liability for statements made in GIDEP reports has long been a concern of contractors and subcontractors, who are often reluctant or unwilling to identify suppliers or to submit reports at all. However, contractors and subcontractors contend that they need further clarification of what constitutes a "reasonable effort to determine that the report was factual." Guidance regarding the level of investigation required, including inspection and testing, would likely encourage increased reporting by contractors.

Another issue relates to the manner in which reports are submitted to GIDEP. Many entities who file reports designate the problematic part as "nonconforming" rather than "suspect counterfeit." Designating suspect counterfeit parts as "nonconforming" makes it impossible for others to search the

---

[504] Richard Smith Interview Summary (Appendix 19), at 2.
[505] Interview with Anonymous Source (notes in possession of authors). The source further indicated that contractors do not use labs that follow SAE AS6171 test plans.
[506] 48 C.F.R. § 52.246-26(f).

GIDEP database for relevant reports of counterfeit parts. A source indicated that it would be necessary to go through all reports in the Failure Experience category one-by-one in order to identify relevant reports.[507] This is a problem that may actually be exacerbated by the new reporting requirements, since they require reporting of major and critical nonconformances as well as counterfeit and suspect counterfeit items. A 2016 report from the Government Accountability Office found that defense agencies were underreporting suspect counterfeit parts to GIDEP, and it also determined that some agencies were applying a far more stringent standard for establishing how much evidence is needed before reporting a part as a suspect counterfeit.[508]

h. Integration of Counterfeit Microelectronic Part Prevention and Avoidance Strategies into a Broader Hardware Assurance Framework that Addresses Cyber Physical System Security is Needed

There is an increasing awareness that counterfeit parts are no longer restricted to used parts sold as new or remarked parts, but may also include tampered parts and clones. In this context, malware and firmware relates to the electronic parts themselves, not to software on a computer system – it is an issue of cyber physical security, not cybersecurity. SAE's G-32 committee on cyber physical system security is currently in the process of developing a standard to address firmware and software embedded into physical systems. However, subject matter experts interviewed for this report indicate that DoD still approaches counterfeit electronics and cyber physical security as two separate supply chain risks and has isolated cyber physical security from more traditional counterfeiting methodologies.

SAE's AS6171 committee is developing standards to address hardware security issues where a die may have malicious circuitry (i.e., tampered devices with Trojans or backdoors) embedded in it to compromise functionality or confidentiality. AS6171 considers these devices to be counterfeit parts, and test methods in the AS6171 family of standards already address tampered devices to some extent. For example, design recovery (reverse engineering) is detailed in the AS6171/11 standard and is applicable to detection of tampered devices. The G-19A committee is actively working to develop additional standards to detect tampered devices, including a standard on netlist assurance.

Treating tampered devices as counterfeits is the correct approach. Like other kinds of counterfeits, tampered devices are not what they purport to be, and they are the outcome of a supply chain that is not sufficiently controlled. Further, some methods that are presently useful for detecting

---

[507] Interview with Anonymous Source (notes in possession of authors).
[508] U.S. Government Accountability Office, *Counterfeit Parts: DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk* (2016), available at https://www.gao.gov/assets/680/675227.pdf. The report also noted that access to many GIDEP reports is limited to government agencies, which means that contractors are often not aware that reports have been filed about certain parts.

conventional counterfeit parts can provide indications that a part has been tampered with. If parts are already being subjected to other testing to detect evidence of counterfeiting and the level of risk warrants such testing, the tampering analysis should be conducted at the same time. In addition, supply chain measures like tracking and tracing can be helpful. When dealing with a device such as a field programmable gate array (FPGA) that can be modified externally by installing functionality on it, it is obviously desirable to maintain a chain of custody so that a malicious actor does not gain access to and modify the device.

Isolating cyber physical security from traditional counterfeiting results in reduced efficiency in other ways as well. Subject matter experts on one problem will not be consulted on the other problem, when better use of resources could be made by looking at the issues more comprehensively. A coordinated approach to supply chain management will therefore result in a more effective identification of concerning devices than a disjointed one. The Joint Federated Assurance Center ("JFAC") has already integrated counterfeit detection, anti-tamper, functional analysis, firmware security analysis, and other issues within its Hardware Assurance ("HwA") center,[509] and the approach should be applied more broadly across the DoD. Counterfeiting is an ever-moving target. If cyber physical security is viewed as a different problem and separated from counterfeiting, DoD will not have all of the resources that are needed to deal with the latest and most sophisticated counterfeits.

Clones present a special case that falls somewhere between traditional counterfeits and tampered devices. Clones are counterfeit parts in that they are made from the ground up to look like something they are not. However, if they are produced by a nation state for malicious security purposes, they could be very sophisticated and hard to detect, in which case some of the anti-tamper tools may be needed to detect those types of clones and prevent their use in DoD systems. Therefore, DoD must adopt a more holistic approach that recognizes that these are no longer discrete issues but have become intricately intertwined.

i. Conduct a Further Evaluation of the Civil and Criminal Trademark Laws to Consider Whether Further Remedies and/or Enhanced Enforcement are Needed

A number of the persons who were interviewed in connection with this report expressed dissatisfaction with the Lanham Act, as well as with the criminal statutes relating to trafficking in counterfeit goods and services. An anonymous source argued that the criminal statutes should include a

[509] *See* Institute for Defense Analyses, *Hardware Assurance (HwA) Support for Supply Chain Risk Management (SCRM),* Defense Standardization Program Workshop (July 10, 2018), at 5, available at https://www.dsp.dla.mil/Portals/26/Documents/Publications/Conferences/2018/DSP%20Workshop%20July2018/DSPWorkshop-Day2-180710/DSPWorkshop-9Cohen-180710.pdf?ver=2018-08-01-150531-257.

broader definition of "counterfeit" that is based on what is happening in the real world of parts and materiel counterfeiting. The source observed that under the DoD definitions, used parts that are sold as new are considered to be counterfeits. The Department of Justice, on the other hand, uses a definition of "counterfeit" that does not include "used sold as new," but instead focuses solely on use of another party's trademarks and logos, excluding other counterfeiting mechanisms. As a result, the source believes that it is very difficult for DoD to get criminal convictions of contractors (who sell used items as new) for counterfeiting, because the DOJ only considers that activity to be fraud, not counterfeiting. The source also believes that for this same reason, some DoD components rarely seek a counterfeiting conviction and are reluctant to report items as suspect counterfeits.[510]

Other government sources made similar arguments about the need for a more expansive definition of "counterfeiting" in the criminal statutes, in order to encompass counterfeiters who misrepresent characteristics or qualities of electronic parts other than registered trademarks. It is beyond the scope of this report to make specific recommendations in this regard. However, a more detailed study of the criminal counterfeiting statute, as well as the cases brought under that statute, should be conducted to determine whether revisions to the laws are needed. Further analysis of the challenges of enforcing civil and criminal statutes against counterfeiters should also be undertaken, with greater participation of the Department of Justice, Department of Homeland Security, Department of Energy, and DoD representatives, investigators and prosecutors, in order to identify required resources and strategies for more effective enforcement.

B. ADOPTION OF MACHINE VISION TECHNOLOGIES TO EVALUATE THE AUTHENTICITY AND SECURITY OF MICROELECTRONIC PARTS

For purposes of this section of the report, the term "machine vision" refers to methods for automated image acquisition and/or processing using computer algorithms. Machine vision can include the use of software and hardware-based automation for:

- Positioning an object within the field of view of an image sensor, which can be accomplished through hardware (i.e., robotics), software (i.e., image manipulation), or a combination thereof;
- Adjusting the illumination conditions to obtain consistency in the appearance of the object;
- Determining the image acquisition conditions (for such parameters as exposure time, sensitivity, filtering, resolution, etc.);
- Capturing and storing an image;
- Processing the image (i.e., performing a set of transformations to the image or associated data to optimize its suitability for the intended analysis);

[510] Interview with Anonymous Source (notes in possession of authors).

- Identifying relevant features of the image (which could be as simple as geometric shapes or as complex as abstract patterns or spatial wavelengths of color or contrast using machine learning and artificial intelligence tools); and
- Extracting information by analyzing the features (e.g., performing quantitative measurements such as size or shape, comparing to reference data or criteria of acceptability, documenting defects, etc.).

Machine vision systems offer the possibility of improved speed, accuracy, and repeatability over manual image acquisition and processing systems, and the ability to apply complex algorithms to the analysis of images.[511] The automation of the imaging process also hinders the application of subject matter expertise, subjective evaluation, and consideration of other factors that were not explicitly addressed in the development of the software that are introduced by human involvement.

Machine vision for the purpose of counterfeit part detection generally involves the use of automated image acquisition and analysis of electronic parts for detection of defects or comparison to reference images or a database of features that allow classification of the part as authentic or suspect counterfeit.

1. Regulations and Standards as Potential Obstacles to Adoption of Machine Vision Technologies

Section 843 of the FY 2019 NDAA required an evaluation of the rules, regulations, and processes that may hinder the development and incorporation of machine vision technologies to determine the authenticity and security of microelectronic parts in weapon systems.

a. Regulations

On their face, the FAR and DFARS do not exclude the possible use of machine vision technologies to screen for counterfeit electronic parts. DFARS § 252.870-2 requires CAS-covered contractors to establish and maintain an acceptable counterfeit electronic part detection and avoidance system.[512] The system must include risk-based policies and procedures that address a minimum of 12 factors, including training of personnel, inspection and testing of electronic parts (including criteria for acceptance and rejection), and methodologies to identify suspect counterfeit electronic parts and to rapidly determine if a suspect counterfeit electronic part is, in fact, counterfeit.[513]

[511] The Automated Imaging Association (AIA) is an industry association dedicated to advancing the use and understanding of machine vision technology. It maintains a list of machine-vision related standards and an archive of webinars. *See* https://www.visiononline.org/vision-standards-details.cfm?type=7.
[512] 48 C.F.R. § 246.870-2(b)(1).
[513] 48 C.F.R. § 246.870-2(b)(2).

Contract Clause 7007 further explains some of these requirements. With respect to inspection and testing of electronic parts, it states:

> Tests and inspections shall be performed in accordance with accepted Government- and industry-recognized techniques. Selection of tests and inspections shall be based on minimizing risk to the Government. Determination of risk shall be based on the assessed probability of receiving a counterfeit electronic part; the probability that the inspection or test selected will detect a counterfeit electronic part; and the potential negative consequences of a counterfeit electronic part being installed (e.g., human safety, mission success) where such consequences are made known to the Contractor.[514]

Contract Clause 7008 requires inspection, testing, and authentication of electronic parts "in accordance with existing applicable industry standards," in Tier Three or when the contractor cannot establish traceability from the original manufacturer.[515]

As a result, one potential obstacle to adoption of machine vision technologies is failure to comply with accepted Government- and industry-recognized techniques and existing industry standards. Another potential obstacle is the proven reliability (or lack thereof) of machine vision systems in detecting counterfeit electronic parts.

b. Compliance with Industry Standards

There are two principal questions that must be considered in determining whether machine vision technologies comply with current industry standards or whether those standards present an obstacle to adoption of machine vision:

> *1. Can machine vision satisfy the narrow requirement of visual inspection in current industry standards?*
>
> *2. Can machine vision replace the testing called out in the standards and satisfy the DFARS's requirement for risk-based testing?*

As described in detail below, it appears that the answer to both questions is "No." If it is determined that machine vision is an accurate method for determining the authenticity of electronic components, at most it could supplement, but not replace, the testing methodologies set out in industry standards. Its best use may be in track and trace systems.

i) Can Machine Vision Satisfy the Requirements for Visual Inspection?

It is readily apparent that machine vision can never satisfy the requirements for certain individual types of testing indicated by the relevant standards, such as solvent testing, X-ray fluorescence, acoustic

[514] 48 C.F.R. § 252.246-7007(b)(2).
[515] 48 C.F.R. §§ 252.246-7008(b)(3)(i), (c)(2).

microscopy, and Raman spectroscopy. However, a more detailed analysis is required to determine whether machine vision can satisfy the narrow requirement for external visual inspection imposed by the anti-counterfeiting standards.

SAE's AS6171/2A provides guidance and requirements on visual and SEM inspection of EEE parts for counterfeit part detection.[516] A trained inspector is required to conduct a physical examination of the devices.[517] Visual inspection consists of two separate steps, general external visual inspection ("EVI") and detailed EVI. First, 100 percent of parts in the lot are subjected to a general EVI to determine whether there are any gross visual anomalies.[518] This is intended to be a cursory inspection of the visible sides containing the part marking, and no specific magnification is required. As long as parts are visible through the packaging (i.e., trays, tubes, or tape), they do not need to be removed. The external shipping package and traceability documentation must also be inspected and imaged.[519]

Next, sample components are subjected to a detailed EVI at 10X to 40X magnification, including number of leads per part, package type, pin 1 placement, and correct part number. Leads are inspected for a number of conditions, such as nonuniform color, exposed base material, repaired or bent leads, missing leads, and corrosion.[520] The package body must also be inspected for variances in marking styles and country of origin, visible remarkings, and logo variations, and the external package must be inspected for suspect indicators such as scratch marks, blacktopping, solder residue, adhesives, uneven thickness, and texture discrepancies.[521] Differences in the corner radius, color discrepancies, and texture discrepancies between the top, bottom and sides of the part must be documented.[522] The report must include images of the top and bottom of the part, close-up images of the leads from the side and end perspective, at least one corner, and any anomalies found.[523] The standard notes that visual inspection "may require positioning components at multiple angles to highlight potential conditions, e.g., beyond the standard top, bottom, side, corner, and 45° angled views to obtain images highlighting the suspect condition."[524]

---

[516] SAE International, AS6171/2A, *Techniques for Suspect/Counterfeit EEE Parts Detection by External Visual Inspection, Remarking and Resurfacing, and Surface Texture Analysis Using SEM Test Methods* 1 (2017).
[517] *Id.* at § 3.1.
[518] *Id.* at § 5.3.1. The standard indicates that IDEA standard IDEA-1010-B can be used as a reference document, since it contains numerous examples of potential anomalies.
[519] *Id.*
[520] *Id.* at 7.
[521] *Id.* at 12, 17.
[522] *Id.* at 17.
[523] *Id.* at 30.
[524] *Id.* at 7.

AS6081 also requires an external visual inspection that ensures all parts in the lot meet certain general criteria and "appear in good condition to the *unaided eye.*"[525] Samples then undergo detailed optical examination at magnification and lighting sufficient to detect particular features, such as package type, part dimensions, pin 1 placement, and lead condition.[526]

Similarly, IDEA-STD-1010-B requires a trained inspector to perform a visual inspection of packaging materials, followed by the tray, reel, or tubes containing the electronic components.[527] A detailed visual inspection of discrete components is then conducted under magnification. The inspector must examine the surface of the parts, including the logo and markings, inconsistencies in package size, burn holes and blister marks, colored dots or ink marks that might represent evidence of previous testing, and evidence of sanding, etching, or blacktopping. The leads must be examined for evidence of damage, oxidation, scratches, gloss, color, and texture.[528] CCAP-101 also requires a detailed visual inspection of the package, component markings, and lead condition.[529]

Machine vision systems such as those evaluated in this report (i.e., Alitheon, Covisus, and Creative Electron) are not set up to identify the defects for which the standards require detection during detailed EVI.[530] They are also not designed to manipulate the part in order to allow images from all the perspectives required by the standards. Theoretically, they could be designed to do so, but that is a very different objective than the one for which those systems have been developed in their current form. Automated inspection and imaging of microelectronic parts for compliance with the standards would require extensive programming and training of machine vision algorithms and redesign of part handling mechanical systems.

In principle, machine vision could be used to satisfy the requirements for general EVI by providing a cursory inspection of all components in the lot to determine if there are any gross anomalies. Machine vision would not satisfy the documentation review portion of general EVI, and in order for machine vision to replace manual inspection, the AS6171 standard would need to be revised to allow for automated inspection and anomaly detection. Similarly, the AS6081 standard would have to be revised to allow automated, machine vision-based inspection in place of inspection by the unaided eye.

---

[525] SAE AS6081 at 19 (emphasis added).
[526] *Id.* at 20.
[527] IDEA-STD-1010-B at 32-37.
[528] *Id.* at 45-50.
[529] CCAP-101 at 11-12.
[530] *See* Section V(A) (Evaluation of Existing Machine Vision and AI Technologies), *supra*, for a description of the functionality of these systems.

Furthermore, if parts were to be inspected while still in their packaging, the machine vision technology would have to be capable of imaging the parts through the packaging while still maintaining accuracy.

ii) Can Machine Vision Replace Standard Techniques and Qualify as Risk-Based Testing?

As discussed in Sections A(2)(b) and A(3) above, the DFARS requires contractors to utilize risk-based processes for inspection, testing, and tracking of electronic parts. Contract Clause 7007 requires CAS-covered contractors to establish and maintain a counterfeit part detection and avoidance system which includes risk-based policies and procedures that address inspection and testing of parts.[531] Tests and inspections are to be performed in accordance with "*accepted Government- and industry-recognized techniques*."[532] The counterfeit part detection and avoidance system must also include risk-based processes that enable tracking of electronic parts from the original manufacturer to acceptance by the DoD, regardless of whether the parts are supplied as discrete electronic parts or are contained within larger assemblies.[533]

Contract Clause 7008, which applies to all contracts, requires traceability. If the contractor is not the OCM or an authorized distributor, the contractor must:

> (1) Have risk-based processes (taking into consideration the consequences of failure of an electronic part) that enable tracking of electronic parts from the original manufacturer to product acceptance by the Government, whether the electronic part is supplied as a discrete electronic part or is contained in an assembly;
>
> (2) If the Contractor cannot establish this traceability from the original manufacturer for a specific electronic part, be responsible for inspection, testing, and authentication, in accordance with *existing applicable industry standards.*[534]

SAE AS5553 similarly requires covered organizations to "develop and implement a risk-based counterfeit EEE parts control plan that documents its processes used for risk identification, mitigation, detection, avoidance, disposition, and reporting of suspect counterfeit or counterfeit EEE parts and/or assemblies containing such EEE parts."[535] Suppliers must have a "documented risk assessment and risk mitigation process, by the organization with technical responsibility, for procurements from other than: (1) authorized sources, or (2) sources who provide EEE parts obtained exclusively from authorized

[531] 48 C.F.R. § 252.246-7007(c)(2).
[532] *Id.* (emphasis added).
[533] *Id.* at § 252.246-7007(c)(4).
[534] 48 C.F.R. § 252.246-7008(c)(1), (2) (emphasis added).
[535] SAE AS5553 at 6.

sources."[536] The risk mitigation process must address two issues: the likelihood of receiving a suspect counterfeit or counterfeit EEE part from the source, and the consequences of a suspect or counterfeit EEE part being installed.[537] Note that AS5553 does not include the likelihood that a counterfeit part would be detected among the criteria for assessing risk, as do the DFARS and AS6171. AS5553C notes that testing and inspections should be performed in accordance with industry standards such as AS6171, AS6081, CCAP-101, and IDEA-STD-1010.

At best, if proven to be accurate, machine vision systems may be able to assist with the traceability requirements of Contract Clauses 7007 and 7008. Machine vision systems may be able to compare a subject part to a database of known, registered parts and to make a determination about whether the subject part is a match to a particular part in the database. That determination could potentially enable traceability back to the original manufacturer and assist with concluding that the part is authentic.

However, even if machine vision can determine that a part is authentic, it cannot provide critical information about the reliability of the part, the risk that it will fail, and the potential negative consequences if that part is installed in a DoD system. Standards-based testing collects numerous pieces of information that may indicate whether a part has been mishandled or mistreated, used, contaminated, or altered in some way. SAE AS6171A and its associated slash sheets require that parts be subjected to an array of tests based on an assessed level of risk.[538] In addition to external visual inspections, those tests may include X-ray fluorescence spectroscopy to detect material composition of a part and layer thicknesses, including a lead finish examination; delid/decapsulation to verify that die attributes are consistent with expectations; X-ray inspection to detect deliberate misrepresentation or damage to the part; acoustic microscopy to identify latent physical defects such as cracks, voids, and delaminations; electrical testing to determine whether the part operates in accordance with specifications; Raman and FTIR spectroscopy to identify chemical or material modifications in the part; thermogravimetric analysis; and design recovery (reverse engineering). Machine vision technologies cannot provide these key indicators about the reliability of a part or the likelihood that a part has been tampered with or altered in some way.

Multiple subject matter experts confirmed that machine vision is not capable of providing information necessary for a risk-based decision about whether to supply, accept, or use electronic parts.

---

[536] *Id.* at 7. Note that AS5553C contains the same weakness as the DFARS – it does not require testing when parts are purchased from a supplier that obtains such parts exclusively from the original manufacturers or their authorized suppliers. *See* 48 C.F.R. § 246.870-2(a)(1).
[537] *Id.*
[538] SAE AS6171C at 29.

Dan Deisz, the Director of Design Technology at Rochester Electronics, instructed that while machine vision systems may be able to determine that a part is authentic, authenticity is not equivalent to reliability. Mr. Deisz observed that an authenticity determination provides no information about how the part has been stored, including environmental problems such as moisture absorption and temperature change, and how it has affected internal structures of the part such as the die attach.[539] Robin Gray, the Chief Operating Officer and General Counsel of the Electronic Components Industry Association, also pointed out that even if machine vision technologies can prove that a part is genuine, they cannot show how it was stored and handled or whether it has been tampered with or tainted with malware.[540] Robert Bodemuller, a Supply Chain Quality Principle Engineer in the Missiles and Fire Control division at Lockheed Martin, echoed these sentiments. Mr. Bodemuller commented, "if a part was marked years ago, testing cannot tell you where that part has been since it was marked or how it was handled during that time; testing only confirms that he part was marked at some time in the past."[541]

That is, machine vision cannot replace risk-based testing and does not provide any information about reliability of a part and its potential for failure. At most, use of machine vision systems would be an addition to current testing regimens that could assist with traceability, but it cannot provide a substitute for the testing required by current industry standards.

2. Business Obstacles to Adoption of Machine Vision Technologies

Potential business obstacles to adoption of machine vision technologies relate to a lack of clarity as to which level of the supply chain these technologies would be implemented and the lack of a strong business case for adoption of machine vision by suppliers and contractors.

a. At What Level of the Supply Chain Would These Technologies Be Implemented?

Although there have been preliminary discussions about use of machine vision technologies to screen for counterfeit electronic parts, there does not appear to be any level of clarity or agreement about the level of the supply chain where these technologies would be implemented. It is unclear whether DoD would use machine vision to screen finished systems and replacement parts that it obtains from its contractors and suppliers, or whether contractors and subcontractors would be responsible for using

[539] Dan Deisz Interview Summary (Appendix 19), at 4. Mr. Deisz also indicated that it is not possible to have a perfect library of known good parts against which to compare a device under test. That is, it may not be possible to account for all good versions of a product, since some parts were fabricated in multiple locations

[540] Robin Gray Interview Summary (Appendix 19), at 4.

[541] Robert Bodemuller Interview Summary (Appendix 19), at 5.

machine vision to test electronic parts before incorporating them into systems and/or providing them to DoD.

Existing regulations strongly suggest that contractors and subcontractors would bear responsibility for implementing machine vision technologies. Contract Clauses 7007 and 7008 both place responsibility for inspection and testing on the contractor and its subcontractors.[542] Contract Clause 7007 requires contractors to establish and maintain an acceptable counterfeit electronic part detection and avoidance system, which includes inspection and testing of electronic parts. Contract Clause 7008 specifies that for purchases from Tier Two, a contractor must use a contractor-approved supplier that uses established counterfeit prevention industry standards and processes (including inspection, testing, and authentication). For purchases from Tier Three, the contractor is responsible for inspection, testing, and authentication.

Further, in the Final Rule for DFARS Case 2014-D005, it was suggested that DoD should use its testing resources to assist small firms in validating the authenticity of electronic parts or provide through the Mentor-Protégé program a structure that would validate and test electronic parts for small subcontractors. DoD responded that it did not have sufficient resources to take on the responsibility for validating the authenticity of electronic parts for small businesses. It noted this would shift responsibility for compliance away from the prime contractor.[543] As a result, it appears that DoD would likely be reluctant to shoulder this additional burden, and contractors and subcontractors would be tasked with responsibility for implementing machine vision technologies.

b. Is There A Good Business Case for Adoption of Machine Vision Technologies by Contractors and Suppliers?

Many of the subject matter experts who were interviewed in connection with this report expressed serious doubts about whether the defense industry would be receptive to adopting machine vision technologies. Robin Gray, the Chief Operating Officer and General Counsel of the Electronic Components Industry Association, indicated that industry does not believe it is necessary to incur the cost of machine vision testing when buying from an OCM or an authorized distributor. Further, because he believes that machine vision technologies cannot show how a part was stored and handled or whether it has been tampered with or tainted with malware, Mr. Gray felt that machine vision technologies would only benefit the grey market, not OCMs. To the contrary, he feels machine vision could actually encourage purchases from unauthorized sources.[544]

[542] 48 C.F.R. §§ 252.246-7007, 252.246-7008.
[543] *See* 81 Fed. Reg. at 50646.
[544] Robin Gray Interview Summary (Appendix 19), at 4.

Andrew Olney, the General Manager of Technology Development at Analog Devices, Inc., affirmatively stated that Analog sees absolutely no value in machine vision technologies for authentication. He believes operators do not have the expertise to make accurate authentication determinations and are wrong approximately 50 percent of the time. Mr. Olney also sees no value in a database of registered parts. He indicated that in order for a system to make accurate authentication determinations, proprietary information from OCMs will be required, and he does not believe manufacturers will agree to supply that information.[545]

Brian Cohen, formerly of the Institute for Defense Analyses, was also quite skeptical about use of machine vision to screen for counterfeit parts. While he feels that machine learning and deep learning could potentially be used to identify parts that do not match a known authentic part, he believes that machine vision alone is too narrow. Further, Dr. Cohen stressed that DoD should not be in the business of screening for counterfeit parts and should not be expected to screen entire systems supplied to it by its prime contractors. Instead, Dr. Cohen believes the primes should have responsibility for screening. He suggested that DoD needs to make a business case for the use of machine vision technologies by its suppliers, not by DoD itself. However, he cautioned that in order to be compelling, the cost of screening and testing in general should not exceed the cost of the product itself.[546]

Kevin Sink, Vice President of Total Quality at TTI, Inc., stated that machine vision has promise if only a camera and a database are required. That is, "[i]n order to be attractive, these technologies must be low cost and cannot require that anything extra be added to the part."[547] Mr. Sink does feel that machine vision could potentially be better than added DNA or other taggants which require additive production steps and specialized readers. However, he stressed that companies do not want to spend money for add-ons.[548]

An anonymous source from industry also suggested that if machine vision is expensive to implement and requires significant administrative overhead, companies will likely push back against its use. The types of expenses to be considered include not only initial capital investment, but also space considerations, hiring and training of personnel, and impact on throughput. The source indicated that the size of the company would be an important factor in determining the types of costs it could absorb. If machine vision was inexpensive to acquire and relatively easy to use, then perhaps companies might be

[545] Andrew Olney Interview Summary (Appendix 19), at 3.
[546] Dr. Brian Cohen Interview Summary (Appendix 19), at 4.
[547] Kevin Sink Interview Summary (Appendix 19), at 5.
[548] *Id.*

more receptive. However, the source also questioned the accuracy of machine vision: if it was inexpensive and simple to use but not accurate, that would not argue in favor of its adoption.[549]

Robert Bodemuller, a Supply Chain Quality Principle Engineer at Lockheed Martin, expressed similar concerns about other tracking technologies, such as applied DNA and diamond dust. Mr. Bodemuller believes that "the concept of operations ("conops") for these technologies needs to be better defined, including added costs, how they will be used, and what additional benefit they will provide." Specifically, Mr. Bodemuller feels that "the associated testing takes too long (as much as 6 to 8 weeks) and is too expensive."[550] The same types of questions might be raised about machine vision as well.

In addition, the fact that machine vision systems might be able to determine that a part is authentic but provide no information about its potential reliability could create another business obstacle to adoption. OEMs may oppose use of a system that connects them with faulty and unreliable parts. If a part is identified as authentic but then fails prematurely and negatively affects missions or weapons systems or the safety of the warfighter, it could also seriously harm the reputation and good will of the manufacturer. Manufacturers may oppose implementation of a system that places them at such a risk.

3. Patenting Issues

A search of issued patents and pending patent applications can provide useful information about a technology. It can identify companies that are working in a particular area and, specifically, where they are investing their efforts. A search can show when innovations began to appear and how well developed or undeveloped a field may be. A patent search can also reveal whether the Government has rights in existing patents. Perhaps most importantly, a search can signal how to avoid infringing on the rights of others.

A U.S. utility patent gives its owner the right to prevent others from making, using, offering for sale, or selling the patented invention in the United States, or importing the patented invention into the United States, during the term of the patent.[551] 35 U.S.C. § 271(a). In order to receive patent protection, an invention must be novel, useful, and nonobvious, and it must constitute patent-eligible subject matter.[552] The patent application must also satisfy certain disclosure requirements known as enablement, written description, and claim definiteness in order for a patent to issue.[553] Today, U.S. patents are

[549] Interview with Anonymous Source (notes in possession of authors).
[550] Robert Bodemuller Interview Summary (Appendix 19), at 4-5.
[551] 35 U.S.C. § 271(a).
[552] 35 U.S.C. §§ 101, 103.
[553] 35 U.S.C. 112(a), (b).

enforceable for 20 years from the date the patent application was filed;[554] previously, utility patents were valid and enforceable for 17 years from the date the patent issued.

Patents are freely transferable, and a patent can be sold or assigned to another owner. In addition, third parties can receive a license to practice some or all of the inventions claimed in a patent, subject to certain terms and conditions. Typically, when the federal government funds the research that gives rise to a patentable invention, the contractor may elect to retain title to the invention, and the government receives a nonexclusive, nontransferable, irrevocable, paid-up license to practice the subject invention throughout the world.[555] Patent owners may also be required to give licenses based on their participation in standards setting organizations. Since a standard, by definition, eliminates alternative technologies, incorporation of a patented technology into a standard eliminates alternatives to that patented technology.[556] As a result, most standards organizations require participating firms that supply essential technologies for inclusion in a standard to commit to licensing their technologies on fair, reasonable, and nondiscriminatory terms ("FRAND terms").[557]

Patents are organized into specific technology groupings based on common subject matter. When a patent application is filed with the United States Patent and Trademark Office ("USPTO"), it is assigned to at least one class and subclass, based on the invention disclosed. As of January 1, 2013, the USPTO adopted the Cooperative Classification System,[558] a system developed in cooperation with the European Patent Office. The Cooperative Classification System ("CPC") divides all inventions into nine main categories such as "chemistry; metallurgy," "physics," or "electricity." Each category is divided into multiple classes and sub-classes. For instance, "physics" divides into 15 subclasses, such as "optics," "computing; calculating; counting," and "displaying; advertising; signs; labels or name-plates; seals." These subclasses continue to further divide into extremely narrow fields. Each patent application can be assigned multiple CPC classifications. A patent searcher can then use the CPC to search for relevant patents and published applications by identifying appropriate classes and subclasses, thereby allowing the searcher to conduct targeted searches in very specific groups of inventions.

---

[554] 35 U.S.C. § 154(a)(2).
[555] 35 U.S.C. § 202(c)(4).
[556] Broadcom Corp. v. Qualcomm Inc., 501 F.3d 297, 314 (3d Cir. 2007).
[557] *See* discussion *id., citing* Daniel G. Swanson & William J. Baumol, *Reasonable and Nondiscriminatory (RAND) Royalties, Standards Selection, and Control of Market Power,* 73 Antitrust L.J. 1, 5, 10–11 (2005). The FRAND commitment thus becomes a "key indicator of the cost of implementing a potential technology." *Id., citing* In the Matter of Rambus, Inc., No. 9302, at 4, 2006 WL 2330117 (F.T.C. Aug. 2, 2006).
[558] Previously, the USPTO used the United States Patent Classification System.

The field of machine vision is not a new field; some of the patents in the following results are many years old. The earliest patent identified in this search expired in 1997. Machine vision has its roots in systems designed to monitor quality of production in manufacturing facilities. The field has apparently evolved rapidly over the last twenty years, as companies not only began investing further into quality control at manufacturing plants, but also expanded use of machine vision to technologies such as video games and self-driving vehicles.

The following patent landscape search is a high-level, preliminary search of issued U.S. patents and patent applications. Patents and applications were reviewed based on the broad technology or method disclosed. This should not be viewed as a comprehensive list of all patents related to counterfeit detection through machine vision, but rather an indication of the types of technologies and methods utilized in this field. It should also be understood that in most cases, the USPTO publishes applications 18 months after filing, which means that there are likely more recently filed relevant applications which have not yet been published. A more detailed review of all patents and patent applications in a narrower field with an emphasis on the claim language could be completed if a preferred counterfeit detection method is identified.

a. Search Methodology

The patent search process utilized the patent classification system previously described. A standard keyword search could potentially return thousands or even tens of thousands of irrelevant search results. However, keywords can be combined with a classification system search to return fewer, more targeted results. The search described herein was conducted using keywords that were selected based on the definition of "machine vision" set forth above, as well as feedback from the CALCE engineering team during the search process.

First, a broad keyword-based search was conducted using the search term "counterfeit." This search yielded 59,915 issued patents and published patent applications. The search was then narrowed by adding the keywords "machine vision," which reduced the number of search results to 716. The vast majority of these results related to detection of counterfeit currency. All non-currency related results were then reviewed for applicability to this project. That review involved first reading the abstract, then examining the claims at a high level. If it appeared that the abstract and claims related to the present project, the patent specification was then reviewed. Only one representative patent was included if it was part of a family of related patents.

The classifications that were noted include:

G06K9/00577	Recognising objects characterised by unique random properties, i.e. objects having a physically unclonable function [PUF], e.g. authenticating objects based on their unclonable texture markers for authenticating, copy prevention
G06Q30/0185	Product, service or business identity fraud
G06F21/30	Authentication, i.e. establishing the identity or authorization of security principals
G06T7/001	Industrial image inspection using an image reference approach
G06K9/036	Evaluation of quality of acquired pattern
G01R31/2813	Checking the presence, location, orientation or value, e.g. resistance, of components or conductors
G06N20/00	Machine learning
G06K9/78	Combination of image acquisition and recognition functions
G06Q30/018	Business or product certification or verification
G06T7/001	Industrial image inspection using an image reference approach
G01R31/2801	Testing of printed circuits, backplanes, motherboards, hybrid circuits or carriers for multichip packages [MCP]
G07D7/2033	Matching unique patterns, i.e. patterns that are unique to each individual paper
G06K7/10	Methods or arrangements for sensing record carriers, e.g. for reading patterns by electromagnetic radiation, e.g. optical sensing; by corpuscular radiation

A second search was started using the classifications referenced above. Each classification was searched individually. If the results were greater than 100, that search was further narrowed by using the key words “counterfeit,” “machine vision,” or both as appropriate. Each patent was reviewed as described above, and relevant results were recorded on the attached spreadsheet.

A third search started with the search term “machine vision” and was then narrowed by adding the search term “counterfeit.” Surprisingly, this disclosed several relevant patents that were not identified in the first two searches. Other search terms used include “image analysis.”

A final search used the list of companies included in the MASER project. Patents and applications owned by most of those companies were already identified in the previous searches, but a few additional patents were located that appeared to be relevant to this search.

b. The Patent Landscape

The current patent landscape for counterfeit detection by machine-vision has been divided into three main categories: identification of relevant features, image processing, and analyzing relevant features within an image.[559] These categories are further divided into how the invention performs counterfeit detection. Several inventions are captured in multiple categories. Information relating to each patent or publication is organized in the following way:

Patent or App. No. *Title of Patent or Application*
Owner Name Status
Brief description of the invention disclosed.

The following notations are used in the descriptions of patents and applications provided below:

> * Indicates patents with government funding -- The government may have a limited license to practice the invention, based on providing funding for the development of the invention.
>
> ^ Indicates expired patents -- Expired patents are no longer enforceable, and the claimed inventions have gone into the public domain. Some patents may have expired due to non-payment of fees and could be reinstated when the outstanding fees are paid.
>
> # Indicates abandoned applications -- Abandoned applications have no patent protection. These can serve as prior art when applying for a patent.

i) Identification of Relevant Features

This category of inventions identifies a feature of the object such as a surface or internal feature. The largest group of inventions creates a signature from features of the object. The other groups identify a specific surface texture, anomalies, or defects.

(a) "Fingerprint" or "Pattern" Features

The following inventions identify unique patterns on each class of object. These unique features can originate during the manufacturing process, either intentionally or unintentionally. This is further divided into the type of fingerprint: structural features on the surface of the object, signals given off the object, and measuring aspects of the object.

(1) Structural Features

This sub-group identifies pre-determined physical features of an object.

[559] Appendix 20 contains a Patent Landscape Table of Search Results on Machine Vision Technologies for Counterfeit Electronic Part Detection.

US4218674^ *Method and a system for verifying authenticity safe against forgery*
Dasy Inter SA Expired: 8/19/1997
A system that uses random magnetic fibers in a document as an identifier. Document is pulsed (scanned) and the system reads a binary code returned.

US7576842^ *Random-type identifying material, 3-D identifying system and method using the same*
Kwang-Don Park Expired – fee related
Method of identifying an object by scanning and identifying random particles within a 3D object and saving to a database. A later scan identifies the same particles and compares to the database to determine authenticity of the object.

US8908920 *Systems and methods for tracking and authenticating goods*
Covectra Expiration:6/21/2032
A device that creates a label on an object with embedded random "flecks" as a unique signature for a class of goods.

US8989500 *Method for Extracting Random Signatures from a Material Element and Method For Generating a Decomposition Base to Implement the Extraction Method*
Signoptic Technologies Expiration: 8/11/2027
Identifies non-moving elements within part of an object, generates a signature based on the vector of those random elements.

US9443298 *Digital fingerprinting object authentication and anti-counterfeiting system*
Alitheon (filed by AuthenTec Inc.) Expiration: 4/4/2032
A method of imaging an object, identifying authentication regions based on the class of good, identifying at least one feature within each region, and creating and storing a fingerprint based on the identified features.

US9582714 *Digital fingerprinting track and trace system*
Alitheon Expiration: 3/2/2032
A method of scanning an object and identifying features on the object. One method of verifying the authenticity of items includes searching the features for known indica of counterfeit goods.

US9646206 *Object identification and inventory management*
Alitheon Expiration: 11/28/2032
A method of scanning each object and defining a unique signature based on features within a selected region of interest. When the object is later scanned the system compares the signature to a database of previously scanned images and determines if the signatures match based upon a pre-determined difference threshold.

US9672678 *Method and system of using image capturing device for counterfeit article detection*
Datalogic USA Expiration: 8/6/2035
An image capturing system and method utilizing a camera system that can emit multiple wavelengths of light (such as infrared, red, or ultraviolet) to illuminate hidden security features on an imaged object.

US9972224 *Fibers with multicomponent fibers used for coding*
Eastman Chemical Co Expiration: 3/24/2036
Manufacturing method wherein the system embeds specific shapes into fibers. Authenticity can later be determined by using imaging to detect the embedded shapes.

US10055670 *Image recognition device, image sensor, and image recognition method using feature*
Omron Corp Expiration: 5/31/2034
System for identifying features on a model and saving an image. Then comparing subsequent images and weighing the similarity of the identified features to determine authenticity.

US10614302 *Controlled authentication of physical objects*
Alitheon Expiration: 11/7/2037
A method of scanning an item to create an image and identifying one or more authentication regions within the image. A fingerprint can be identified based on features within the authentication region. To authenticate the item, the fingerprint can then be compared against a database.

US10621594 *Multi-level authentication*
Alitheon Expiration: 11/7/2037
A method of scanning an item to create an image and identifying one or more authentication regions within the image. A fingerprint can be identified based on features within the authentication region. To authenticate the item, the fingerprint can then be compared against a database.

US20180053312 *Authentication-based tracking*
Alitheon Application Date: 8/19/2016
A method of first authenticating an object based on authentication regions on the object which are used to create digital fingerprints. This also proposes a method of tracking the object over time by comparing the fingerprint to images taken of the object. This can be used to detect counterfeits by monitoring wear and tear on the object.

US20200065577 *System and method for detecting the authenticity of products*
Guy Le Henaff Application date: 11/5/2019
The system directs a user to take picture of a specific "region of interest," and searches for a predetermined random signature in the region of interest.

WO2020028288 *Systems and methods to prevent counterfeiting*
Avery Dennison Corporation Application Date: 7/30/2019
A method of identifying an object by intentional random microscopic features at a predetermined location on the object.

(2) Signal

This sub-group identifies different unique signatures given off of an object. Usually the invention generates this signature by bombarding the object with some form of energy, such as with x-ray radiation.

US7256398 *Security markers for determining composition of a medium*
NCR Corp (filed by Prime Technology LLC) Expiration: 6/10/2024
A method of authentication by manufacturing glass with security markers. The markers are illuminated with one or more wavelengths of light and the photoluminescence of the emitted light is measured.

US7420474* *Idiosyncratic emissions fingerprinting method for identifying electronic devices*
* U.S. Air Force Research Laboratory, AFRL/SNT
Barron Associates Expiration: 11/23/2025
A method of generating a digital fingerprint for an electronic device based on the emissions (EM, RF, audio, and/or vibrational) from the device.

US8341759 *Detecting counterfeit electronic components using EMI telemetric fingerprints*
Oracle America Expiration: 10/16/2027
A method of generating a digital footprint for a computer based on electromagnetic interference signals and determining authenticity by comparing the signature to a reference signature.

US9959430* *Counterfeit microelectronics detection based on capacitive and inductive signatures*
*U.S. Secretary of Navy
U.S. Secretary of Navy Expiration: 6/20/2036
A method of creating a fingerprint by applying low-level alternating current across the power pin of an integrated circuit. Authenticity can be verified by comparing the fingerprint against the fingerprint of a representative device.

US10027697* *Detection of counterfeit and compromised devices using system and function call tracing techniques*
*U.S. Department of Energy
U.S. Dept. of Energy (Filed by Florida International University) Expiration: 4/28/2037
Detecting counterfeit or defective products on the energy grid by call tracing (e.g., system calls raised during a time interval are traced and compiled, assembled, or listed) and developing call lists of genuine devices.

US10054624 *Electronic component classification*
Battelle Memorial Institute Expiration: 12/12/2034
A method of attaching an integrated circuit to a testing device that measures the noise off of the circuit. The noise can be separated into segments and read as a fingerprint/key. That fingerprint can be compared to a known device to verify authenticity.

US10149169 *Non-contact electromagnetic illuminated detection of part anomalies for cyber physical security*
Nokomis Inc. Expiration: 4/23/2035
A device for detecting counterfeit electronic devices by illuminating the device with RF energy and measuring the emitted electromagnetic energy. This can indicate detailed configuration, quality, authenticity, status and state of electrical devices.

US10235523 *Avionics protection apparatus and method*
Nokomis Inc. Expiration: 8/31/2036
A system for detecting compromised electronic devices by detecting unintended emitted electronic energy and/or unintended conducted energy from Avionic Line Replacement Units.

US10475754 *System and method for physically detecting counterfeit electronics*
Nokomis Inc. Expiration: 12/10/2035
A system of inspecting semiconductors or integrated circuits by pulsing with a high precision oscillator signature and reading an RF signature.

US10571505* *Method and apparatus for detection and identification of counterfeit and substandard electronics*
*U.S. Navy
Nokomis Expiration: 3/6/2034
A system with a hollow enclosure with a RF antenna for detecting electromagnetic emissions (signal) from electronic devices placed within the enclosure. The system processes the signal to determine if the signature is from an authentic device.

US20170160320 *Methods and apparatuses for identifying anomaly within sealed packages using power signature analysis counterfeits*
Power Fingerprinting Inc. Application Date: 12/2/2016
A system and method for detecting counterfeit electronic devices by exciting the part with RF and/or EM emissions and receiving a resultant power signature signal. The signature can be compared to the signal from a reference device.

(3) Measurement

This sub-group creates a unique signature for an object by measuring features of the object.

US10298236 *On-chip aging sensor and counterfeit integrated circuit detection method*
University of California Expiration 11/2/2036
An on-chip aging sensor which indicates the chip usage time based on induced electromigration. Incorrect aging can indicate a recycled chip. The unique signature of the aging chip can also be used to detect counterfeit electronics.

US10460326 *Counterfeit integrated circuit detection by comparing integrated circuit signature to reference signature*
Global Circuit Innovations Inc. Expiration: 2/23/2038
A method of detecting counterfeit integrated circuits by connecting a curve tracer to a circuit's power and ground connections to generate a curve on the curve tracer's screen. The curve serves as a signature and can be compared to the signature from a reference integrated circuit.

(b) Object Texture

The following inventions review the surface texture of an object to determine the authenticity of the object.

US8325987 *Amorphous alloy member and its application for authenticity determining device and method, and process for manufacturing amorphous alloy member*

Fuji Xerox Co. Expiration: 2/11/2031

Determining the surface roughness of an irregular region of a series of alloy members manufactured from the same mold. Later determine authenticity of an alloy member by comparing the surface roughness in the irregular region.

US10341555* *Characterization of a physical item*

* U.S. Army Research Office

Chromologic Expiration: 12/29/2035

A method and device wherein the device rakes two lights across an object and a camera captures microscope details of surface of the object. Those details are translated to signature for the class of object and saved to a database. A scan of a new object can reference the signature to determine if it is from the same class of object by how closely the two signatures match.

US20180268214 *Method and Apparatus for Authentication of a 3D Structure*

Alpvision Application Date: 5/21/2018

A method of capturing an image of an object, automatically comparing to a reference, and instructing the user a second angle to take another image of the object. The two images are used to create a 3D structure that are compared to the reference image.

US20190286102 *System and method to protect items associated with additive manufacturing*

General Electric Co. Application Date: 3/16/2018

A method of encoding a unique signature into parts manufactured by 3D printing (additive manufacturing).

(c) Defect Detection

The following patents identify anomalies or defects on or within the object. These defects are usually known from the manufacturing method.

US8472677 *Method and device for identifying a printing plate for a document*

Advanced Track and Trace Expiration: 12/6/2029

A method whereby a tester prints a reference document using a printing plate then compares the reference document to a test object to determine if both were printed from the same plate based on identified defects.

US9059189 *Integrated circuit with electromagnetic energy anomaly detection and processing*

Nokomis Expiration: 11/4/2032

A method of collecting radiofrequency energy from an integrated circuit to detect waveform defects/variances which can indicate inauthentic circuits. Some of these methods can be used in conjunction with a device to detect changes over time that could indicate software/hardware changes or tampering.

US9721337 *Detecting defects on a wafer using defect-specific information*

KLA Corp. 10/15/2032

A method of detecting defects by targeting a specific pattern on a wafer and scanning for known defects.

US10145894 *Defect screening method for electronic circuits and circuit components using power spectrum analysis*

NTES of Sandia Expiration: 11/24/2032

A method of applying electrical current to a circuit and measuring the power spectrum. This method detects defects by comparing the power spectrum analysis with reference data.

ii) Image Processing Technologies

This category of inventions differs from the other two categories because it either trains a machine learning system or makes a change, either in the image or in how the image is taken.

(a) Process by Training A Machine Learning System

This group of inventions scans multiples of the same object or class of objects to train a neural network. These inventions can be used over time to teach a machine vision system to recognize authentic versus counterfeit objects.

US9885745* *Apparatus and method for integrated circuit forensics*

US Secretary of Navy Expiration: 9/25/2034

A system that uses integrated circuits of known provenance to train a "decision engine" by scanning with various sensors. Unknown integrated circuits can then be tested and the system generates a probability score that the tested device is authentic.

US10586318 *Automated model-based inspection system for screening electronic components*

Raytheon Co. Expiration: 4/24/2037

A method of training an automated system to detect part identifiers and/or defects, primarily through visual inspection and image analysis. The analysis can provide feedback to the imaging system to adjust the camera's focal point on the part.

US20170032285 *Authenticating physical objects using machine learning from microscopic variations*

Entrupy Inc. Application Date: 4/9/2015

A method of authentication using machine learning by training a system with a data set to recognize microscopic variations to identify a class of objects.

US20190189236 *Artificial intelligence based monitoring of solid state drives and dual in-line memory modules*

Intel Corp. Application Date: 2/21/2019

A method of detecting counterfeit SSDs and DIMMs by training an automated neural network with initial probe tests of non-volatile memories dies. The memory controller performs field tests at startup using the trained ANN to detect memory health but can also be used to verify authenticity.

US20190219525 *Method and System to Automatically Inspect Parts Using X-Rays*

Guilherme Cardoso Application Date: 1/16/2019

Utilizing artificial intelligence to determine where on a sample to inspect with x-ray.

US20190279329 *Systems and methods for enhancing machine vision object recognition through accumulated classifications*

Capital One Services LLC Application Date: 5/21/2019

A machine vision system that improves object classification through multiple views of the same object in different settings. Accuracy scores improve through more images of the object in different types of lighting, perspectives, contrast, brightness, and size.

(b) Manipulating a Digital Image

This group of inventions manipulates the image for improved processing. Some inventions resize the object within the image, while others rotate the object.

US8798313 *Counterfeit detection system*

Hewlett Packard Development Co. Expiration: 7/14/2030

A method of counterfeit detection wherein an image is classified then reduced in size using multiple methods to create multiple reduced-size images. An algorithm determines the most accurate reduced-size image which can be transmitted for further analysis.

US10055672 *Methods and systems for low-energy image classification*

Microsoft Technology Licensing LLC. Expiration: 6/21/2035

A device and method of image size reduction wherein the system identifies points of interest in an image, the system uses one or more modules (filter, gradient, pool, and normalizer) to extract features within those points of interest, then transmits those features to an external computer to classify the image based on the features.

US10089478 *Authentication method and system*

CoPilot Ventures Fund III LLC Expires: 9/4/2023

Normalizes observable characteristics corresponding to a unique pattern.

(c) Process by Physical Manipulation

This group of inventions manipulates the object, usually by adjusting the object within the field of the image sensor.

US9796089* *Supervised autonomous robotic system for complex surface inspection and processing*

*U.S. Airforce and U.S. Army

Carnegie Mellon University Expiration: 3/17/2034

A robotic system that moves over the surface of a 3D object that maps the surfaces of the object and creates a digital 3D model of the object.

US9798910 *Mobile hand-held machine vision method and apparatus using data from multiple images to perform processes*

Cognex Corp. Expiration: 8/8/2027

A system and method with a camera connected to a computer wherein the computer provides feedback to the user about how to manipulate the camera to image the surface of a 3D object.

US10593007 *Methods and arrangements for configuring industrial inspection systems*
Digimarc Corp. 6/18/2036
A method of capturing multiple images of an object, interpreting the images, and adjusting the camera settings to best capture hard to capture watermarks on an object.

US20130022167# *High Speed, Non-Destructive, Reel-to-Reel Chip/Device Inspection System and Method Utilizing Low Power X-rays/X-ray Fluorescence*
Creative Electron Inc Abandoned
A system and method of high-speed x-ray inspection of electronic parts by using a conveyor belt to move the parts past an x-ray detector. The system adjusts the conveyor speed for the best possible high-speed inspection of the part.

iii) Analyzing Relevant Features

This category of inventions analyzes an image of the object within software. The inventions can complete this task by comparing the object to a reference object or use quantitative measures of the features. This category is different from identifying features in that these inventions typically compare and use an algorithm that determines the match percentage.

(a) Comparing Features to A Reference

This group of inventions compare the object to a reference. Sometimes the reference object is from the same class of objects from the same manufacturer, and other times by comparing the object to an object of known provenance. Integrated circuit (IC) counterfeit detection usually scans the internal parts of the IC to compare to OEM.

US8472677 *Method and device for identifying a printing plate for a document*
Advanced Track and Trace Expires: 12/6/2029
A method whereby a tester prints a reference document using a printing plate then compares the reference document to a test object to determine if both were printed from the same plate based on identified defects.

US8848905 *Deterrence of device counterfeiting, cloning, and subversion by substitution using hardware fingerprinting*
NTES of Sandia Expiration: 9/14/2032
A method of detecting counterfeit devices by using a Physically Unclonable Function (PUF) circuit which generates a random key value. The PUF is coupled with a key generator. The values can be compared later to verify authenticity.

US9031329 *Photo forensics using image signatures*
Truepic Analyze LLC (filed by Fourandsix Technologies) Expiration: 3/11/2033
Method of analyzing multiple attributes of an image against reference image to determine if there is an imperfect match.

US9053364 *Product, image, or document authentication, verification, and item identification*
Authentiform Expiration: 10/30/2033
A method of comparing an image against a reference image, comparing the difference between predetermined shapes on the same plane, and calculating the difference between the two images to determine authenticity.

US9646373 *System and Method for Counterfeit IC Detection*
IEC Electronics Corp. Expiration: 11/26/2034
A method of counterfeit detection for integrated circuits wherein a system classifies the IC based on an optical image of the package. Then, one or more ICs are x-rayed and the x-ray images are compared to a reference x-ray from the IC class.

US9767459 *Detection of counterfeit electronic items*
Optimal Plus LTD Expiration: 3/14/2036
A method of counterfeit detection wherein test data from an electronic item is compared to the manufacturing test data from a similar cluster of items.

US10127447* *System and method for authentication*
* U.S. Department of Energy
ClearMark Systems Expiration: 3/12/2035
A method of authentication by capturing characteristic data from an item, deriving authentication data from the characteristic data, and comparing the authentication data to a database.

US10460326 *Counterfeit integrated circuit detection by comparing integrated circuit signature to reference signature*
Global Circuit Innovations Inc Expiration: 2/23/2038
A method of detecting counterfeit integrated circuits by connecting a curve tracer to a circuit's power and ground connections to generate a curve on the curve tracer's screen. The curve serves as a signature and can be compared to the signature from a reference integrated circuit.

US10055670 *Image recognition device, image sensor, and image recognition method using feature*
Omron Corp Expires: 5/31/2034
System for identifying features on a model and saving an image. Then comparing subsequent images and weighing the similarity of the identified features to determine authenticity.

US20170160320 *Methods and apparatuses for identifying anomaly within sealed packages using power signature analysis counterfeits*
Power Fingerprinting Inc. Application Date: 12/2/2016
A system and method for detecting counterfeit electronic devices by exciting the part with RF and/or EM emissions and receiving a resultant power signature signal. The signature can be compared to the signal from a reference device.

US20180268214 *Method and Apparatus for Authentication of a 3D Structure*
Alpvision Application Date: 5/21/2018
A method of capturing an image of an object, automatically comparing to a reference, and instructing the user a second angle to take another image of the object. The two images are used to create a 3D structure that are compared to the reference image.

US20190279377 *Determination method, determination system, determination device, and program*
NEC Corp. Application Date: 3/12/2019
A method of comparing the physical features of an item (such as the brand, a logo, a clasp, and/or a decorative part) to a stored image of the item type.

(b) Quantitively Measuring Features

This group of inventions measure the features of an object. Often the inventions compare multiple data points about the object. The invention might measure color, photoluminescence, or size. These measurements are compared to a reference object.

US6944331 *Locating regions in a target image using color matching, luminance pattern matching and hue plane pattern matching*
National Instruments Corp. Expiration: 5/30/2023
A method of region location by comparing the color of random pixels in a refence image to a target image. The system then searches for luminance patterns and uses hue planes or color-based pattern matching to ensure that the correct location was found.

US8712163 *Pill identification and counterfeit detection method*
Eyenode LLC Expiration: 12/14/2032
A method of determining counterfeit pills by comparing an image of a test pill to a saved image. First the image is mapped by comparing contrast shifts, then the method compares color and/or texture, shape, size, indicia, and imprints or markings.

US9384390 *Sensing data from physical objects*
Digimarc Expiration: 1/19/2027
Measuring and storing directional albedo (light reflection) then later re-measuring and comparing against stored data.

US10055672 *Methods and systems for low-energy image classification*
Microsoft Technology Licensing LLC. Expiration: 6/21/2035
A device and method of image size reduction wherein the system identifies points of interest in an image, the system uses one or more modules (filter, gradient, pool, and normalizer) to extract features within those points of interest, then transmits those features to an external computer to classify the image based on the features.

US10094874 *Scanning method for screening of electronic devices*
NTES of Sandia Expiration: 10/18/2032
A method of screening suspect bad/counterfeit devices from functional/authentic devices by performing a power spectrum analysis and comparing the results to a standard.

US10101280* *Device and method for detection of counterfeit pharmaceuticals and/or drug packaging*
* US Department of Health and Human Services Expiration 3/31/2030
US Department of Health and Human Services
A system for detecting counterfeit medication and/or drug packaging by shining multiple lights with different wavelengths onto the medication and measuring the wavelength of the reflected light.

US10585139* *IC device authentication using energy characterization*
* Defense Ordnance Technology Consortium
Science Applications International Corp SAIC Expiration: 2/14/2039
A method of verifying an integrated circuit (IC) by measuring the quiescent current (QC) value while applying multiple voltage steps to the IC. The QC values can be compared to the QC values of an authentic IC to verify the tested IC's authenticity.

iv) Related technologies

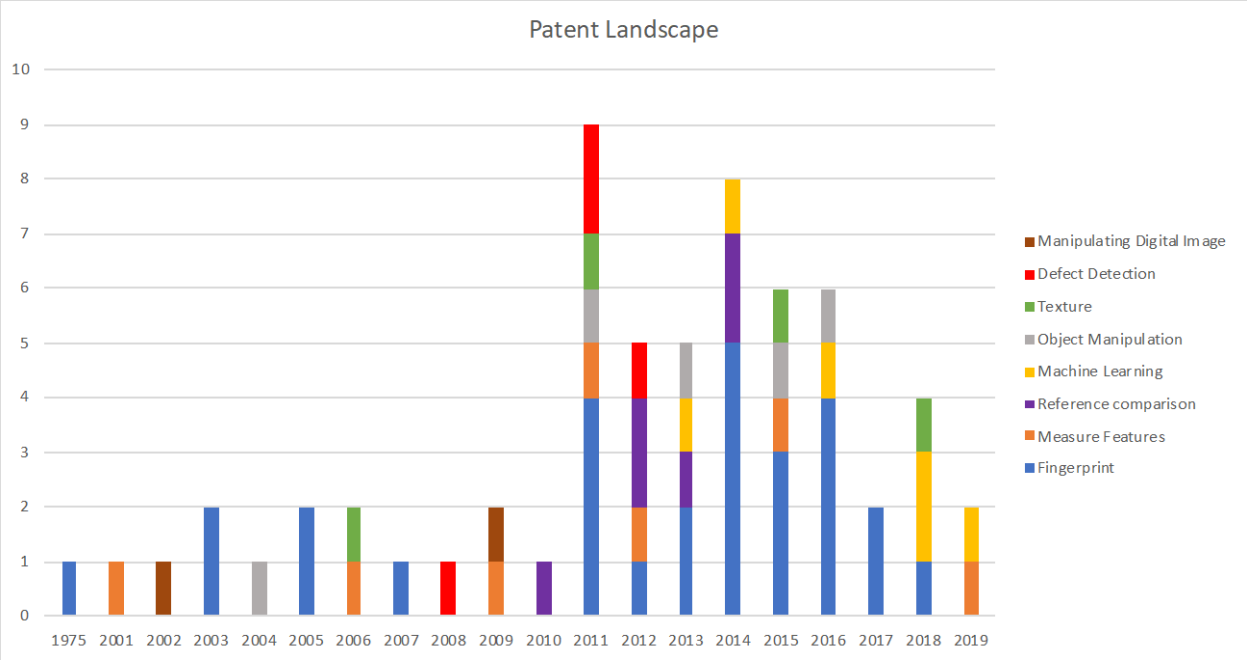
(a) Optical Character Recognition (OCR)

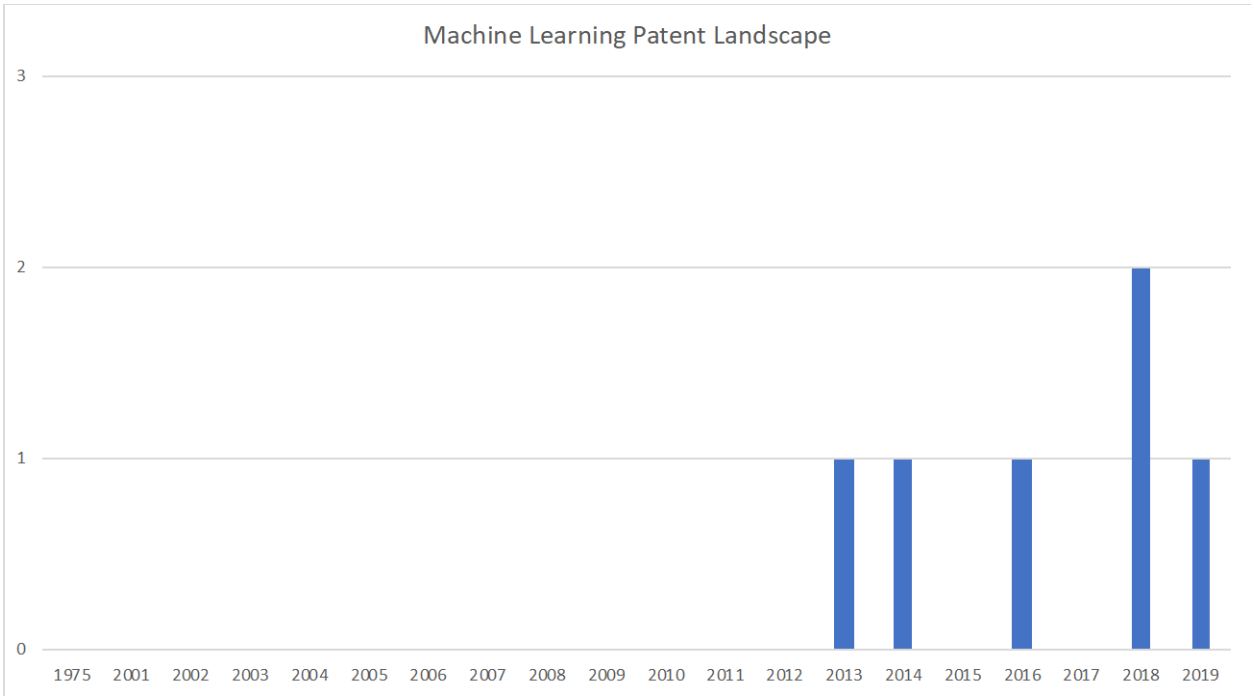
OCR generally works by scanning an image and performing various processes to help identify characters within the scanned image. The process attempts to identify features or patterns of a character and outputs plain text. While OCR is becoming more accurate and works well for recognizing text, the OCR processing method is intended to be inclusive rather than exclusive. It appears that the processing would have to be dramatically altered in order for the technology to be useful for counterfeit detection.

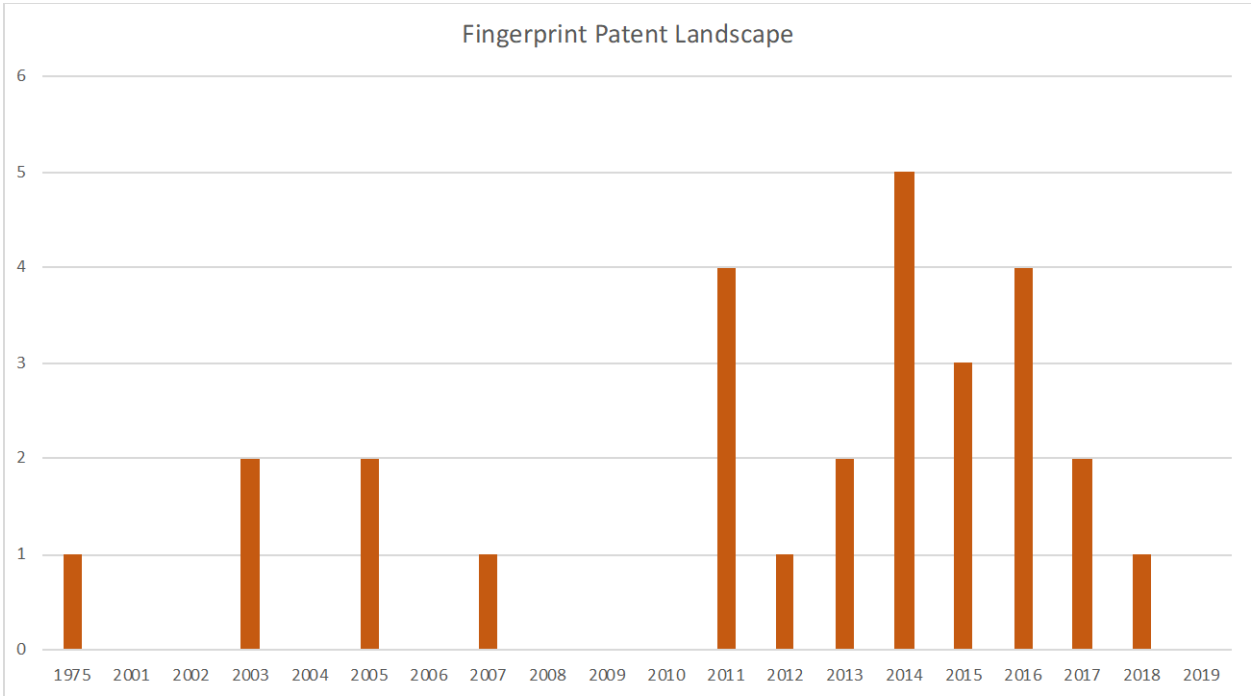
(b) Serialization

Many manufacturers of high-end goods and electronic circuits use a process of adding serial numbers to an article. Sometimes the manufacturer adds the serial number in a difficult to detect manner. This is useful for counterfeit detection if counterfeiters do not find or fake the serial number, but it is not useful without the manufacturer's assistance.

v) Patent Landscape Graphs




Machine Learning Patent Landscape
3
2
1
0
1975
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019


Fingerprint Patent Landscape
6
5
4
3
2
1
0
1975
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019

vi) Patenting Trends

Counterfeiters have become dramatically more sophisticated over the last 20 years. Various reports indicate a general trend of an increasing number of counterfeit integrated circuits detected in the 2000s.[560,561,562] The magnitude of counterfeits varies by report, but the general trend is consistent across reports. After 2011, the reports describe a wide range of experiences in detecting counterfeit integrated circuits, from remaining consistent to decreasing year-over-year.[563,564,565]

This landscape search disclosed a spike of related patent applications in 2011. The spike can possibly be attributed, at least in part, to the release of the Senate Armed Services Committee Report and the associated interest in counterfeit detection and prevention generated by the report.[566] Prior to 2011, few companies filed relevant patent applications. Similarly, the sophistication of the patents also developed over time. The number of "fingerprint" patents increased, and it appears that the sophistication of the fingerprint detection methods also increased.

In addition, researchers began applying other types of technologies to the problem of counterfeit detection. For example, companies have filed an average of one machine learning counterfeit detection patent per year since 2013. These machine learning inventions train a computer model using known provenance objects to automatically detect counterfeit objects.

The search also disclosed that the Government either owns, or has an interest in, many of the patents identified. Ten patents listed above contain a notice indicating that the invention was made with Government support and that the Government has certain rights in the invention. A few others are owned by a Government agency.

---

[560] Ujjwal Gwin, et al., *Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain,* 102 PROCEEDINGS OF THE IEEE 1207 (2014).
[561] Ujjwal Gwin, Daniel DiMase, and Mohammad Tehranipoor, *Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead,* J. ELECTRON TEST (2014), available at http://tehranipoor.ece.ufl.edu/jetta14-2.pdf.
[562] Electronics Takeback Coalition, *Study Shows Growing Counterfeit Electronics Problem Poses National Security Threat,* available at http://www.electronicstakeback.com/wp-content/uploads/Fact_sheet_on_counterfeits.pdf.
[563] U.S. Government Accountability Office, *Counterfeit Parts: DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk* (2016), available at https://www.gao.gov/assets/680/675227.pdf
[564] Damir Akhoundov, *2019 ERAI Reported Parts Statistics,* ERAI Blog, available at https://www.erai.com/erai_blog/3167/2019_erai_reported_parts_statistics.
[565] Semiconductor Industry Association, Submission to Request for Public Comments on Report on the State of Counterfeit and Pirated Goods Trafficking and Recommendations (July 26, 2019), available at https://www.semiconductors.org/wp-content/uploads/2019/07/SIA-Comments-84-FR-32861-Counterfeiting.pdf.
[566] *See* Senate Armed Services Committee Report, published May 21, 2012.

While this preliminary patent search is far from comprehensive, it can nevertheless serve to indicate the types of technologies currently being investigated and developed to detect counterfeit objects, and to identify the companies working in the field. The technology appears to have advanced from basic digital fingerprints and has started to incorporate machine learning into the authentication process. The search identified a small number of companies utilizing machine learning to enhance counterfeit detection. A future targeted U.S. patent search and a literature search within the machine learning field will likely yield more companies in the space and additional technologies under development as the area continues to be explored by researchers. Searches of international patents and patent applications could also be considered.

4. Recommendations and Conclusions

A number of recommendations and conclusions can be reached based on the foregoing discussion.

a. Machine Vision Systems Should Be Developed Further to Comply with Current Industry Standards on General External Visual Inspection

Current machine vision technology cannot replace certain types of testing intended to identify defects during detailed external visual inspection, nor can machine vision, as currently designed, manipulate parts to allow imaging from all the perspectives required by the standards. Theoretically, machine vision might be used to satisfy some of the requirements for general external visual inspection by providing a cursory inspection of all components in a lot to determine if there were any gross anomalies, assuming the machine vision technology was capable of imaging parts in trays, tubes, or tapes while still maintaining accuracy. This would require revision of standards such as AS6171 and AS6081 to allow for automated inspection and anomaly detection. However, machine vision would not satisfy the documentation review portion of general EVI. As a result, machine vision may be able to supplement standard testing techniques, but it cannot replace them. Machine vision should be developed further to comply with current industry standards on general EVI.

b. DoD Needs to Develop a Better Understanding of the Costs and Benefits of Machine Vision and How It Can Best Be Implemented

There does not yet appear to be any level of agreement about the supply chain level or levels at which machine vision technologies would be best implemented, if they were to be adopted for anti-counterfeiting purposes. Does the DoD intend to utilize machine vision systems to screen all incoming parts and assemblies for counterfeit parts, or will contractors and subcontractors be expected to conduct machine vision-based inspection of parts before they are delivered to DoD? Must parts be screened every time they are passed to the next level in the supply chain, or will verification of previous inspection be

accepted? Will OCMs be required to image parts before they leave the manufacturing facility, and will they be required to register those parts in a database for purposes of allowing future authentication determinations to be made by DoD, contractors, or testing labs? If so, how will the integrity of the database be secured? Many issues must be resolved before machine vision technologies can be considered for adoption in anti-counterfeiting applications. DoD needs to develop a better understanding of the costs and benefits of machine vision in order to determine how it can best be implemented.

c. DoD Needs to Develop a Strong Business Case for Adoption of Machine Vision Technologies

It is unclear whether there is a compelling business reason for use of machine vision technologies by the defense industry for authentication purposes. Several of the subject matter experts consulted in connection with this report were either skeptical about or opposed to adoption of machine vision for use in counterfeit prevention. Use of machine vision could potentially lead to increased purchases from the grey market; however, even if parts obtained from unauthorized sources were determined to be authentic, there would still be no guarantee that the part was reliable or, worse yet, that it had not been tampered with or tainted with malware. OCMs will likely oppose use of a technology that has the ability to connect them with faulty and unreliable parts, which could lead to reputational harm and erosion of good will. In addition, it has been suggested that OCMs will not agree to provide proprietary information required to authenticate a part. Adoption of machine vision technologies to satisfy general EVI requirements in standards could present a more attractive business case, including automation of a time-consuming task that is currently performed manually. This could open the door for adoption of machine vision for other purposes.

d. Consideration Must Be Given to the Costs of Adopting Machine Vision Technologies

Companies will need to understand the expenses associated with acquiring, using, and maintaining machine vision systems, including initial capital investment, administrative overhead, database maintenance and security, personnel costs, and impact on throughput. If machine vision technologies are costly to acquire and implement but provide little benefit to the user, companies will likely oppose their adoption. Potential licensing costs must also be investigated, including the risk that users of machine vision techniques might be forced to accept FRAND licenses in order to practice essential technologies included in industry standards. Until the actual costs of machine vision technologies are explored and understood, it is not possible to weigh them against any purported benefits that might be realized from adoption of machine vision. DoD should obtain a complete analysis of financial costs of adopting machine vision technologies in real world application scenarios, including trial implementation in actual operational environments.

Appendix 19.

Interview Summaries for Policy Analysis

Robert Bodemuller Interview Summary

Maryland Carey Law conduced two discussions with Robert Bodemuller. Mr. Eichelman had an initial conversation with Mr. Bodemuller at the DMSMS Symposium in Phoenix, Arizona, in early December 2019. Subsequently, CALCE and Maryland Carey Law held a Skype conference with Mr. Bodemuller on April 14, 2020.

Mr. Bodemuller is a Supply Chain Quality Principle Engineer in the Missiles and Fire Control division at Lockheed Martin, located in Grand Prairie, Texas. He is responsible for the inclusion of counterfeit prevention language into the corporate acquisition contracts that Lockheed Martin Missiles and Fire Control (MFC) uses with its subcontractors. Mr. Bodemuller provided a copy of Lockheed's CorpDoc 3, [1] which contains General Provisions for Subcontracts/Purchase Orders for Non-Commercial Items Under a U.S. Government Prime Contract (All Agencies). CorpDoc 3 contains anticounterfeiting provisions in Section 7 entitled "Counterfeit Work," but it does not include any FAR or DFARS flow down provisions. He noted that Lockheed also uses a CorpDoc 3A (entitled "Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) for Fixed Price Subcontracts/Purchase Orders for Non-Commercial Items Under a United States Department of Defense Prime Contract") to incorporate the mandatory language of the FAR and DFARS (including subsections 7007 and 7008) to Lockheed's subcontractors.

Mr. Bodemuller explained that using standard corporate documents helps to guide the relationships with subcontractors. As a result, one of the CorpDocs is automatically incorporated into all Lockheed defense contracts. Although the different divisions and businesses within Lockheed may use different CorpDocs that are tailored to their needs, Section 7 relating to counterfeiting is identical in all CorpDoc versions. CorpDoc 3 is the standard contract used most frequently by Missiles and Fire Control.

However, Mr. Bodemuller indicated that subcontractors sometimes attempt to negotiate the language in Lockheed's CorpDocs. In his experience, the most common area of negotiation with subcontractors relates to the definition of "Counterfeit Work," which includes electronics

[1] Lockheed's CorpDocs are available at https://www.lockheedmartin.com/en-us/suppliers/business-area-procurement/aeronautics/terms-and-conditions/commercial-terms-and-conditions.html.

and all other parts.[2] "Work" is often a controversial term because it is defined broadly[3] and applies to all parts, as well as labor and services, even though the DFARS anticounterfeiting provisions apply only to electronics. Mr. Bodemuller explained that because Lockheed is aware that DoD is concerned about counterfeiting in all areas, it decided to apply the DFARS requirements to all parts. The term "Counterfeit" is still controversial with some subcontractors also, although Lockheed uses the DFARS definition.

Lockheed's standard contracts also contain a provision stating that the Seller "shall not deliver Counterfeit Work or Suspect Counterfeit Work" to Lockheed Martin. Mr. Bodemuller observed that some sellers want to change that provision to state that the Seller "shall not knowingly deliver Counterfeit Work or Suspect Counterfeit Work," thereby attempting to limit their liability for any counterfeit or suspect counterfeit goods that were delivered without actual or constructive knowledge of the counterfeit nature of those goods.

Another provision that Sellers sometimes question is the requirement in Section 7(c) that products shall be purchased only from the Original Component Manufacturer or Original Equipment Manufacturer, or through an OCM/OEM authorized distributor chain. CorpDoc 3 further states that the Seller may only purchase products from a source other than an OCM, OEM, or authorized distributor if (i) those sources are unavailable, (ii) the Seller's inspection and other counterfeit risk mitigation processes will be employed to ensure the authenticity of the Work, and (iii) the Seller obtains the advance written approval of Lockheed Martin. Mr. Bodemuller stated that for his division at Lockheed, those provisions are non-negotiable. Other Lockheed divisions might only require advance written notice for purchases outside the authorized distribution chain, rather than advance written approval, since some Sellers object that seeking permission in advance takes too much time.

Further, the terms and conditions in Lockheed's standard contracts simply state that the Seller will employ its inspection and counterfeit risk mitigation processes to ensure the authenticity of the work, without providing greater specificity or addressing the 12 criteria set forth in DFARS Section 7007(c). According to Mr. Bodemuller, each Lockheed business area addresses this term differently. In Missiles and Fire Control, each purchase order contains counterfeit prevention text notes. Industry standards such as AS 5553 and 6171 may be used for guidance. For example, AS 6171 is referenced when a Seller must obtain advance written

---

[2] CorpDoc 3 defines "Counterfeit Work" as "Work that is or contains unlawful or unauthorized reproductions, substitutions, or alterations that have been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used Work represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics." CorpDoc 3, Section 7(a).

[3] ""Work" means all required labor, articles, materials, supplies, goods, and services constituting the subject matter of this Contract." CorpDoc 3, Section 8(f).

approval to order an electronic part from the grey market because it is not available from an OEM or authorized distributor. In that instance, Lockheed requires that testing must be performed by an independent test house, not by the independent distributor supplying the parts. Mr. Bodemuller observed that AS 6171 reflects a moderate level of risk. However, he can recall only one occasion in five years when a subcontractor had to obtain parts from the grey market due to scheduling constraints. Instead, DoD did design refreshes in many problems, which minimized obsolescence problems.

Mr. Bodemuller noted that he has been employed at Lockheed for five years and, during that time, he has never been in a situation where a seller has supplied counterfeit parts. He believes that the counterfeit prevention process has matured greatly during the last five to ten years, thereby reducing the incidence of counterfeit parts. In the event of a breach, Mr. Bodemuller said that Lockheed's CorpDocs contain a provision requiring the seller to immediately replace the counterfeit work with genuine work. The seller is also liable for all costs relating to removal and replacement of the counterfeit work, including testing after the counterfeit work has been replaced. However, Mr. Bodemuller acknowledged that in many situations, this requirement could potentially bankrupt a supplier, in which case Lockheed might negotiate a cap on damages.

Mr. Bodemuller next discussed Lockheed's experience with DCMA audits, as well as Lockheed's audits of its own subcontractors. Prime contractors like Lockheed are routinely audited by DCMA once every year. DCMA provides a checklist which addresses each of the criteria in DFARS Sections 7007 and 7008, and Lockheed provides detailed procedures from its Control Plan. A DCMA site representative (usually an expert in the process) then conducts a review. Mr. Bodemuller stressed that the annual DCMA review is not technically an "audit" that results in an approved process that would allow Lockheed to be reimbursed for any counterfeit parts supplied in a DoD contract.

When Lockheed audits its suppliers, the process looks very different. Several different types of audits are routinely conducted, including AS9100 and counterfeit prevention surveillance surveys. Special process are mandatory, but not for counterfeit prevention. Surveillance audits are conducted by field quality engineers. They have a lengthy checklist, but they ask questions selectively for each audit. The information collected then goes into an SMS (Supplier Management System) for suppliers. If nonconformances are identified during the audit, corrective actions could be developed, including education and implementation of new processes. According to Mr. Bodemuller, the most common nonconformance Lockheed finds is that suppliers may not know when to use authorized distribution and may not understand when a particular distributor is authorized.

In Subsection 7(h), Lockheed's CorpDoc3 requires sellers to flow down paragraphs (a) through (h) or equivalent provisions in lower tier subcontracts for the delivery of items that will be included in or furnished as Work to Lockheed. However, Mr. Bodemuller stated that Lockheed does not believe it has an obligation to audit at the lower tiers of the supply chain. The Missile Defense Agency ("MDA") has severe flow downs and requires audits of Lockheed's

subcontractors. MDA requests parts lists (BOMs or bills of materiel) for assemblies provided to Lockheed, but subcontractors are often unwilling to provide those parts lists. Subcontractors such as Honeywell and Raytheon have design authority over their assemblies and, while they meet the required specifications, the companies do not want to disclose the BOMs. Mr. Bodemuller said that MDA is concerned about its inability to obtain parts lists, since it believes that most counterfeit parts enter the supply chain at the third and fourth tiers. Further, it may be difficult for Lockheed to inspect items such as missiles that are already assembled; there are issues about costs, which are typically imposed on the buyer rather than the seller, and the manpower required for these sorts of inspections. Mr. Bodemuller also noted that lower tier suppliers have no idea what kinds of assemblies their parts will ultimately be incorporated into.

Mr. Bodemuller also explained that it is more difficult to include anticounterfeiting language in commercial contracts. Although Lockheed attempts to incorporate the same provisions relating to Counterfeit Work, it has less leverage and commercial suppliers may be unwilling to agree to that language. Although use of COTS products is discouraged in DoD contracts, it is also expected. DFARS Section 7008 provides some relief for prime contractors over the original provisions in Section 7007.

Mr. Bodemuller discussed Lockheed's obligation to report counterfeit parts to GIDEP, and he offered a few suggestions to make GIDEP more useful. First, he believes that there is not enough information available on GIDEP, since few reports are made. Lack of reporting may be attributable to the fact that GIDEP is required to notify the supplier when a report is made, which has led to concerns about potential liability. Also, many of the reports in the GIDEP database are for agency use only due to ITAR concerns. As a result, Mr. Bodemuller told us that he consults ERAI more often than GIDEP because it contains more information.

Mr. Bodemuller ended the discussion by emphasizing that he is more concerned with addressing the needs of the warfighter than focusing on issues such as liability for counterfeit parts. He believes that the counterfeit risk can be significantly reduced by focusing on four factors: sourcing, testing and inspection, training, and traceability. In his experience, reporting suspect counterfeits to GIDEP is not that helpful. Instead, companies should purchase parts only from OEMs, OCMs, and authorized suppliers; if they must go to the grey market, then they should test and inspect.

With respect to traceability, Mr. Bodemuller indicated that certificates of conformance are essentially useless for parts coming from the grey market. He noted that MFC places little value on certificates of conformance. Mr. Bodemuller wants to talk to shippers and receivers and to review purchase orders, in order to confirm an unbroken chain of traceability back to the OCM. He observed that even within the authorized distributor chain required by AS5553, traceability can be difficult because authorized distributors routinely buy and sell parts to one another.

Mr. Bodemuller expressed concerns about newer tracking technologies, such as applied DNA and diamond dust. He believes that the concept of operations ("conops") for these

technologies needs to be better defined, including added costs, how they will be used, and what additional benefit they will provide. Specifically, he feels that the associated testing takes too long (as much as 6 to 8 weeks) and is too expensive. Further, if a part was marked years ago, testing cannot tell you where that part has been since it was marked or how it was handled during that time; testing only confirms that the part was marked at some time in the past. On the other hand, Mr. Bodemuller thinks that Blockchain is more promising, because it has potential dual use for traceability plus procurement. That is, purchase orders and other procurement transactions could be processed through Blockchain, thereby creating a complete contractual record for a part. He believes this could provide attractive efficiencies, and then traceability would be a side benefit.

Dr. Brian Cohen Interview Summary

Maryland Carey Law and CALCE had a conversation with Dr. Brian Cohen on May 27, 2020. Dr. Cohen retired from the Institute for Defense Analyses ("IDA") at the end of 2019, after working there for approximately 35 years.[1] In that capacity, he advised the Department of Defense and the Office of the Secretary on supply chain issues, including counterfeiting, beginning in approximately 2005. Following his retirement, Dr. Cohen created CyberTech Solutions, LLC, a consulting firm with clients in both government and industry.

Our discussion began with an overview of Dr. Cohen's work with IDA. IDA is a federally funded research organization that works with the Office of the Secretary of Defense (OSD) and Joint Agencies. In the early 2000s, IDA became involved with efforts to understand tampering and malicious insertion and other adversarial actions affecting the supply chain, as well as with helping DoD adapt to the changing threat space. This effort resulted in DoD Instruction 5200.44 (Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, issued in 2012) and DoD Instruction 4140.67 (DoD Counterfeit Prevention Policy, issued in 2013).

In 2003, Dr. Cohen became involved with the Trusted Foundry Program (now a part of DMEA). The original pillars of the Trusted Foundry Program were custom designed parts, state of the art fab technology, and security. Starting in 2005 at the urging of senior leadership at OSD, the Trusted Foundry Program started an accreditation program aimed at expanding the "Trusted Suppliers" who could meet he security needs of DoD. That program, although primarily focused on less than state of the art, has expanded to more than 70 suppliers. The program is still active today and continues to be funded by the government. However, approximately three to five years ago, people started looking for other solutions because the provider (formerly IBM, now Global Foundries) could no longer provide state of the art solutions that met the security requirements of the "Trusted Supplier" program for the government's relatively small demand. Dr. Cohen explained that state of the art manufacturing is extremely expensive if you only need a small number of chips (e.g., 1000). In addition, the chips themselves are hugely complex and involve significant design costs, even if existing IP is being utilized. He estimated that it could cost approximately $250 million to design a custom chip, before manufacturing costs are added, and a 5 nm or 7 nm fab is not sufficient.[2]

In addition, Dr. Cohen has been involved with advising the Office of the Secretary of Defense on hardware assurance issues. He helped organize and hold a series of 10 workshops on trusted microelectronics that were co-hosted with the National Defense Industrial Association ("NDIA"). Dr. Cohen stated that he must also give credit to Ms. Catherine Ortiz of Defined

[1] Dr. Cohen emphasized that the thoughts he shared with us were his own personal observations, not the views of IDA.

[2] For further detail, see Institute for Defense Analyses, Semiconductor Industrial Base Focus Study – Final Report (December 2016), available at https://www.ida.org/-/media/feature/publications/s/se/semiconductor-industrial-base-focus-study--final-report/d-8294.ashx.

Business Solutions, who played an equal role in the workshops. Previously, NDIA had no real focus on counterfeiting, but was more concerned with the lifecycle management of systems. Ultimately this collaboration led to the creation of an Electronics Division within NDIA, after its Trusted Microelectronics Joint Working Group sent a report to the Office of the Secretary of Defense in 2017 containing four whitepapers with recommendations relating to DoD's access to assured microelectronics.[3]

Dr. Cohen's area of expertise is supply chain risk management, a concept that has been around for decades, but which took on new meaning in the last 15 to 20 years. In the mid-2000s, malicious attacks became a concern. This resulted in DoD Instruction 5200.44 for supply chain risk management, as well as DFARS provisions relating to the supply chain. DoD Instruction 5200.44 was issued in 2012 and had initial versions as directives dated to 2008 and 2009. It requires DoD and all of its organizational entities to manage the risk of products containing counterfeit components or malicious functions. The policy focuses on the intended harms to end users, including disruptions of potentially catastrophic magnitude, rather than the financial motivations of counterfeiters. A few years ago, the problem became more critical due to problems with certain suppliers, including Kapersky and Huawei. The Federal Advisory Security Council ("FASC") was created by the FASC Security Act of 2018 ("FASCSA") (Title II of Pub. L. 115-390) and was initially focused on the exclusion of suppliers across the federal government (like Kapersky). Huawei's products have since been banned, and U.S. suppliers were told they could not to sell to Huawei, but that proved somewhat untenable. Dr. Cohen indicated this policy is still up in the air.

We asked Dr. Cohen for his thoughts about clones and whether they are sufficiently mature to pose a significant threat at the present time. Dr. Cohen explained that there are two types of clones: reverse engineering a product in order to duplicate it exactly, and form-fit-function equivalents passed off as authentic product. In either case, if someone can clone a product, they are operating at a technology level beyond that of the original product. That means they can make the clone do things that the original product could not do. Technically, the clone might be a "conforming product," because it meets required specifications, but the part might also function in ways that the original product did not, which could be very dangerous.

Dr. Cohen mentioned that 10 years ago, China could not produce clones that met form, fit and function for products on the market, but today they can produce products that meet or exceed specifications. Traditional screening methods such as electrical testing and x-rays may not be able to identify these clones, because they are no longer substandard, nonconforming parts. Now, they may be conforming. While something extra may be added to the clone, it would not necessarily disrupt the original function of the chip. For example, a timer could be inserted that would cause the chip to fail at a certain time, or it could be programmed to fail in response to certain stimuli.

The discussion then turned to obsolescence and sustainment in military systems. Dr. Cohen explained that in the consumer market, a product can become obsolete within 18 months.

[3] See https://www.ndia.org/divisions/working-groups/tmejwg/final-team-reports.

However, in the defense industry, a product may not become obsolete for 10 years. The defense acquisition process is out of sync with the high tech parts and software that go into these systems. The government has tried to deal with this issue proactively, but it has been largely unsuccessful. Products are not designed for upgrade and requalification, since qualification typically occurs at the component (or "box") level, not at the board level.

Sustainment of government systems is handled in several ways. In some instances, the government may service a system itself at one of its depots. Line replaceable units (LRUs) such as circuit boards may be sent back to the contractor and exchanged for a functioning unit, although this means ceding some control to the contractor. In other cases, a contractor may provide logistical support and take full responsibility for sustainment. The SD-22 DMSMS Guidebook[4] outlines sustainment practices and management, which is a distributed decision-making process. For example, if a chip must be replaced due to obsolescence, it will be handled by an inventory control management organization within DoD, such as DLA. If DLA does not have a part, the depot might cut corners and remove a chip from one board (e.g., on a grounded plane) and solder it to another board. Dr. Cohen described such actions as very risky. In other cases, it may be necessary to seek assistance from the prime contractor. However, Dr. Cohen observed that industry may not be motivated to solve the government's problems, because industry is profit driven and may not propose the most cost-effective solution.

Dr. Cohen described DMEA as the expert on these types of issues. DMEA used to evaluate the costs of various alternatives. ARINC did a study that identified 25 sustainment options, ranging from requalifying a part to redesigning a board. DMEA can also reverse engineer boards and provide creative solutions, such as replacing a board containing 50 chips with one that contains only two chips.

Dr. Cohen also reflected on the option of purchasing technical data packages in what he called a "make or buy" decision. After World War II, the government would often buy the drawing and specifications for a system that it paid a prime contractor to design (e.g., a Jeep). Because the documentation was government property, the government could ask any contractor to build those systems. As systems became more complex, contractors became less willing to supply the drawings and other IP to the government, making it more difficult for the government to ask another contractor to produce parts for it. Today, the government increasingly does not buy all of the technical data needed to transfer production form one company to another. Also, it used to be the case that several companies would produce the same item; they were commodity products (e.g., 7400 Series TTL). Today, 95 to 99 percent of defense systems have only one supplier, and it is no longer practical or useful for the government to buy technical data. However, Dr. Cohen pointed out that if the government had such data, and particularly internal test data, it could use it to screen for counterfeits.

Dr. Cohen next described the evolving use of standards by the DoD. In the mid-1990s, the DoD underwent defense acquisition reform, a move away from defense standards for military

[4] See https://www.dau.mil/tools/t/SD-22-Diminishing-Manufacturing-Sources-and-Material-Shortages-(DMSMS)-Guidebook.

components. Military standards or "MIL-SPECS" for design, production, and use of components were largely eliminated, and many of these standards transferred to industry (e.g., Mil Std 883). Others were dropped. As a result, DoD could no longer call out standards in defense contracting, and Dr. Cohen indicated that DoD is still struggling with this in the area of counterfeit mitigation. The Defense Standardization Program Office maintains a database of available standards that are recognized as being useful, but they are not mandated. DFARS provisions also relate to requirements that used to be contained in military standards, but those provisions must be invoked before there is any requirement that they be followed. Defense contracts generally avoid prescriptive language and instead typically state that a contractor will use a counterfeit detection process such as AS5553 "or similar," and thus there is no requirement that the contractor actually follow the standard.

As a result, Dr. Cohen feels that standards are falling by the wayside. The Pentagon is disinclined to tell a contractor that if it follows a certain standard, it has no liability for counterfeits. It prefers to have options available so that contractors can offer solutions to counterfeit prevention, resulting in shared risk and shared responsibility. Primes will then be incentivized to be vigilant, so that their reputations are not tainted by the knowledge that they supplied counterfeit products to DoD.

Finally, we asked Dr. Cohen for about his opinions about use of machine vision technologies to screen for counterfeits. He is familiar with arguments that machine learning and deep learning could be used to identify products that do not match a known authentic part. He thinks there may be hope for that idea. Currently, such comparisons are performed manually, not by machine, and a computer could not only speed up the process but could also learn to ignore differences that may not be relevant. However, Dr. Cohen feels that machine vision alone is too narrow.

Dr. Cohen stressed that DoD should not be in the business of screening for counterfeit parts. He noted that DLA does not want to conduct screening; it has a qualified list of distributors, and it expects those suppliers to screen. Further, DoD should not be expected to screen entire systems supplied to it by its prime contractors. Instead, the primes should have responsibility for screening. Dr. Cohen suggested that DoD needs to make a business case for the use of machine vision technologies by its suppliers, not by DoD itself. He cautioned that in order to be compelling, the cost of screening and testing in general should not exceed the cost of the product itself.

Dr. Cohen pointed out that the most compelling business case is to only buy parts from an OCM or an authorized distributor. He said that people tend to ignore this solution, even though it presents a very low risk of counterfeits. If parts cannot be obtained through the authorized distribution chain, then boards should probably be redesigned in order to manage risk rather than going to the grey market. Dr. Cohen further explained that there is no need to test a part acquired from an authorized distributor. If the contractor has confidence that it's purchasing from a true authorized distributor, then it should have some confidence that there is a low incidence of counterfeits, but testing is not necessary. The contractor should demand paperwork verifying that the distributor is authorized to sell the parts being purchased.

Dr. Cohen also observed that screening methods are not foolproof. A screening method could miss a counterfeit part, or it could identify an authentic part as a counterfeit. The latter is equally problematic because it raises a red flag and stops the production process. Dr. Cohen indicated that while the incident rate of counterfeits from authorized distributors is very low, screening methods may identify those parts as counterfeits 10 to 15 percent of the time.[5] This is an extremely high error rate, and therefore Dr. Cohen concluded that additional screening is not warranted or desirable when buying from an OCM or an authorized distributor.

[5] Dr. Cohen referred us to a paper he authored on the effectiveness of testing techniques as a screening process when purchasing electronic components. See Brian S. Cohen and Kathy Lee, *On the Limits of Testing in Establishing Products Assurance*, Institute for Defense Analyses (April 1, 2014), available online at https://www.ida.org/research-and-publications/publications/all/o/on/on-the-limits-of-test-in-assuring-the-integrity-of-products.

Dan Deisz Interview Summary

Maryland Carey Law and CALCE interviewed Dan Deisz on May 29, 2020. Mr. Deisz is the Director of Design Technology at Rochester Electronics. Mr. Deisz provided an overview of the operations of Rochester Electronics, an authorized distributor and licensed manufacturer of semiconductors. Mr. Deisz explained that OCMs plan product strategies and lifetimes based on sales volume and expected revenues. OCMs have primary distribution partners but, when manufacturing becomes difficult or when a certain revenue threshold is met, the OCM will discontinue a product. However, many customers have long life systems that exceed the commercial viability and production of semiconductor products (e.g., transportation, avionics, military), and those customers want to keep shipping and/or using those same systems.

Mr. Deisz characterized Rochester Electronics as a buffer between OCMs and customers with long lifecycle systems. Rochester only deals in authorized products. It currently stocks over 12 billion finished goods in its warehouse, including active stock that is beyond its date code and obsolete parts which are left over from OCM production. [1] In addition, it has unfinished wafer stock that can be assembled and tested. Finally, Mr. Deisz's group maintains a database from which it can fabricate parts with new silicon that look like the original part ("cloning"). Parts sold by Rochester may contain the OCM's label, Rochester's label, or both. Stocked parts typically have just the OCM's label, whereas new parts manufactured by Rochester will display Rochester's label. Packaged wafer stock may contain either the OCM's label or Rochester's, or both. Customers receive a warranty from Rochester Electronics; in some cases, they may also receive an OCM warranty.

Mr. Deisz suggested that Rochester is unique in the field, since no other company fills all of the niches that Rochester occupies. The company recently started a plastic assembly line in the U.S., which is currently being qualified. He explained that globally, leadframe products are going away, and Rochester needed to set up its own leadframe assembly line in order to protect its wafer stock. Similarly, approximately four to five years ago, Rochester started doing its own hermetic assembly in response to RoHS and the elimination of lead solder. The company has partnerships with the largest assembly houses in the world and will subcontract packaging to AMKOR and others. Now, they are forced to do bonding, plating and trimming themselves for more and more products.

With respect to packaging, Rochester tries to use the most effective way to make a part a drop-in for its customer. Mr. Deisz said they pay attention to die attach material and they match electrical and thermal properties by doing teardowns and cross-sectioning. However, Rochester may not match every detail. For example, Mr. Deisz explained that sometimes there are reasons not to use the same mold compound that was used in an original product 20 years ago, which could be prone to flashing or thermal conductivity. Recent material sets may be preferred, so long as they do not materially alter the electrical and thermal properties. In addition, some

[1] Mr. Deisz acknowledged that companies which stock obsolete parts in finished form are often referred to as "authorized resellers."

material sets may no longer be available because they were found to be carcinogenic or otherwise hazardous. The pins of the devices will always be the same, though, so that customers do not have to change their systems.

Mr. Deisz stated that the "semiconductor industry today is all about the software," referring to software loaded by OEMs that runs entire systems. Changing that software can be extremely expensive. The software is enabled by the hardware and, as a result, customers will do everything they can to avoid changing certain components that are critical to ensuring that the software functions properly. Typically these are high value components such as memories and processors, which in turn are more likely to be counterfeited. Other components, such as power management and logic chips, are less critical to software functionality, and customers are more willing to change those components. As a result, those components are also less likely to be counterfeited.

Mr. Deisz explained Rochester's business model. Rochester is constantly in touch with its customers and understands what products will be needed for long term systems worldwide. When an OCM issues an end-of-life ("EOL") notice, Rochester buys some or all of the inventory (the amount varies by part and by manufacturer). For example, when Cypress exited the older SRAM business, its fab could still produce the silicon. After EOL but before the fab shut down, Rochester entered into a license agreement with Cypress to take over production, including fabrication, assembly and testing of products. In other instances, Rochester gets enabled to make a part 10 years after EOL, when only the databases remained. These decisions will also depend on whether a company is an integrated device manufacturer ("IDM") or fabless; for IDMs, it may be difficult to get access to manufacturing capability after EOL.

When Mr. Deisz's team is asked to design a part that has been out of production for 10 to 20 years, the process normally takes 9 to 18 months. In the case of form-fit-function drop-in replacements, the end result is not a device clone but will have functional equivalency, even though the fab process may be quite different. An example of this would be the most recent port of the Motorola MC6850, which was an NMOS device back in the early 1980's and with Rochester is now a CMOS device. The average cost today for a mask and six prototype wafers is approximately $40,000 for a 5-volt legacy part. There are engineering charges for Design, Assembly, Test, and Qualification beyond that for Rochester to bring a part back to market. When Rochester is enabled with the source IP from the OCM, porting a legacy 5-volt device will typically run close to $450K total to bring a product back to life. Of course, different business levels with different customers could result in the customer seeing more or less non-recurring engineering (NRE). If Rochester must totally reverse engineer the design in order to replicate the part or the design is particularly complex, total costs could be up to $1.5 million. This still is far less expensive than changing the board (including engineering costs and requalification), which could cost as much as $3 to $20 million depending on how much software must change in the system.

Rochester is currently being asked to produce parts anywhere from legacy 5v down to 180 nm in the digital domain. He explained that most obsolescence issues today arise because a customer believes it will have a new system in place by a certain time, but those systems are then

delayed (e.g., a refresh is not funded in the case of DoD). As a result, a customer needs to port a product to obtain a form-fit-function equivalent.

However, Mr. Deisz does not believe that cloning a product by porting it to a different fab is extendable into the future. He noted that product geometries are becoming increasingly complicated, and designs are locked into the fab process on which they are made. Even an OCM such as AMD can no longer move its product from TSMC to Samsung because the financial cost and time to do so would not make a business case. Clones of advanced products cannot be produced without access to the same fab (e.g., no FINFET technology can be ported or cloned somewhere else).

Currently, Rochester has no problem with availability of fab technologies, and Mr. Deisz indicated that he has a few fabs he can utilize. Problems typically arise with technology in the 45 to 90 nm range, when parts are not portable to another fab process. Mr. Deisz stated that these products cannot be cloned. He noted, however, that IBM's Power PC 750, made with 180 nm technology at IBM, was the fastest 180nm process in the world, and even it could not be ported. As a result, Mr. Deisz believes that in the future, most counterfeits will be used parts sold as new, not clones.

When Rochester acquires the intellectual property for a part, it may include patents, design drawings, mask works, databases, and test programs. Mr. Deisz noted that test programs may contain a great deal of device-specific proprietary information, equivalent to tens of man-years of effort. The masks are not particularly valuable to Mr. Deisz's team because they are specific to the fab; instead, the physical design database (GDS2, or Gerber Design System 2) that is used to create the design has great value, since it details the layers in the part. Proprietary spice decks (models of the electrical performance of a circuit) are also extremely valuable. If spice models are not available, then Mr. Deisz's team must create them by characterizing the silicon. Point of sale data can also be helpful, since it allows Rochester to market its redesigned parts to other original customers who may have a similar need.

In Mr. Deisz's experience, IP packages vary tremendously between OCMs. He commented that it is surprising how much information some OCMs lose. Sometimes databases for active production products have already been lost, and archived materials vary significantly. In addition, the testing data, physical designs, and foundry test models for a part are rarely located in the same geographical area or the same plant. As a result, the IP is not readily accessible by one person and can be very difficult to reassemble.

Rochester may obtain an IP package from an OCMs through either a license agreement or an outright purchase of the rights. Rochester always enters into a written contract with the OCM, authorizing it to make the desired part, but the terms vary greatly. One constant is that the OCM usually requires an upfront, cash payment, not a royalty dependent upon success of redesign or future sales. In some instances, Rochester has concerns about overlapping IP rights. For example, if an ARM processor is embedded in a product, Rochester will be required to pay royalties to both ARM and the OCM. If the OCM does not alert Rochester about an ARM

processor core, Rochester is likely dealing with old IP and there is low risk. However, if Rochester clones an ASIC, it will seek indemnification from the OCM.

Rochester's competitors include many unauthorized businesses who try to create clones (i.e., "counterfeits"). No other company's operations are enabled by OCMs. Tekmos also makes drop-in replacements, but Mr. Deisz does not believe it is fully authorized by OCMs. Global Foundries, on the other hand, is a foundry that competes with companies like TSMC and Samsung. Mr. Deisz understands that the U.S. government has invested substantial sums of money in Global Foundries, and it serves as an ITAR facility for the U.S. government. However, Global Foundries does not manufacture products based on reverse engineering.

We asked Mr. Deisz for his view relating to machine vision technology when it comes to counterfeit detection mechanisms. He categorized machine vision as falling into two categories: (1) track and trace, and (2) known good library. Track and trace technology involves marking parts and tracking them using a database. The known good library, such as Batelle type systems, capture data on known authentic parts, stores it in the cloud, and then the device under test ("DUT") is compared to that library. While these systems may be able to determine that a part is authentic, Mr. Deisz stressed that authenticity is not equivalent to reliability. It provides no information about how the part has been stored, including environmental problems such as moisture absorption and temperature change, and how it has affected internal structures of the part such as the die attach. Further, Mr. Deisz pointed out that there will always be escapes since it is not possible to have a perfect library of known good parts. That is, there may be no way to account for all good versions of a part, since some were fabricated in multiple locations. He also believes that while surface analysis can identify some counterfeits, it will not catch them all, even if machine vision technologies work as promised.

Mr. Deisz indicated that Rochester's reverse engineering process has a machine vision component. His group images and tears down parts in order to reverse engineer them for cloning. However, using imaging for cloning is not easy, and they cannot simply take an image and go directly to manufacturing. Instead, a great deal of engineering is required in order to make the part perform in the same way as the original. Therefore, imaging would not be an effective strategy for counterfeiters, and it would also be prohibitively expensive.[2]

Mr. Deisz also described his involvement with SIA and its Anticounterfeiting Task Force, where he began collaborating with Intel, Texas Instruments, and Analog Devices in the early 2000's. Counterfeiting came to the forefront when semiconductor companies started seeing returns. At that time, Lonnie Hurst, Andrew Olney, and a few others wanted to get together to compare notes and potentially influence policy. Customs and Border Protection and the Department of Homeland Security began providing training on counterfeit semiconductors. The IPR Center and its Microelectronics Working Group also previously focused on anticounterfeiting efforts for the semiconductor industry, and it provided approximately 10 days

[2] Regarding clones, Mr. Deisz noted that counterfeiters could potentially insert random failures or data dependent failures into parts. He commented that the worst malicious insertion would be an unpredictable failure.

of classes every quarter. Mr. Deisz served as the SIA representative. Mr. Deisz mentioned that Martin Robl at Infineon in Europe provided similar anticounterfeiting training in Europe.

However, Mr. Deisz observed that the IPR Center and Homeland Security seem to have lost interest in counterfeit semiconductors and other electronic part counterfeits in the last three years. He believes that the monetary value of counterfeit semiconductors isn't high enough to capture their interest, and particularly compared to the value of counterfeit handbags and similar items, even though counterfeit handbags do not present the same safety risks as counterfeit semiconductors. More recently, Homeland Security has also been focused on problems like fentanyl and, since the Covid pandemic, counterfeit PPE.

Robin Gray Interview Summary

Maryland Carey Law and CALCE talked with Robin Gray on June 3, 2020. Mr. Gray is the Chief Operating Officer and General Counsel of the Electronic Components Industry Association ("ECIA"). In his role as COO, Mr. Gray runs the day-to-day operations of ECIA, including finance and human resources, as well as working on technical standards. As General Counsel, Mr. Gray serves as corporate secretary for the nonprofit, and he represents the organization when it meets with government officials, regulatory agencies, and other companies, particularly in the counterfeiting arena.

Mr. Gray emphasized that while ECIA files public comments on regulatory issues, it does not engage in lobbying activities and has no interaction with Congress unless specifically asked to do so. However, ECIA meets regularly with law enforcement officers regarding counterfeiting issues. Sometimes the association is also consulted about peripheral matters such as recycling, trade issues, privacy laws, and hazardous substances and RoHS. Mr. Gray observed that many individuals with whom he meets have legal backgrounds, and some committees such as SAE include both legal and technical people

ECIA is focused on business optimization and developing best practices for improving relationships between Original Components Manufacturers (OCMs) and authorized distributors. The organization brings together distributors and manufacturers to discuss problems they may have, including issues such as reduction of costs and streamlining the distribution process. However, ECIA does not involve itself in relationships with customers. In addition, ECIA is involved in the development of technical standards for electronic components. Mr. Gray explained that JEDEC handles semiconductor technical standards, while ECIA is involved with passive component technical standards.

ECIA also maintains a website, TrustedParts.com (formerly known as ECIAauthorized.com), where member distributors can post lists of authorized inventory that is available for purchase. The website is a sales aggregator: interested parties cannot make purchases through the website, but they can determine which genuine parts are available from authorized distributors. Membership in ECIA is not required to participate in the site. However, participating distributors that are not members of ECIA are restricted to only listing the ECIA member manufacturers' products for which they are authorized. That is, a member manufacturer is permitted to have all its authorized distributors list only that manufacturer's inventory, regardless of whether the distributor is a member of ECIA. ECIA thereby assures that 100 percent of the published line card is authorized.[1] Before listing inventory, the ECIA member must provide proof of authorization. ECIA staff will then check the manufacturer's website to ensure that the distributor is listed; if it is not, ECIA will ask for a copy of the distributor's agreement with the OCM or correspondence from the OCM confirming that the distributor is authorized. In addition, ECIA sends monthly reports to manufacturers, thereby giving OCMs the

[1] Mr. Gray noted that three or four existing members were grandfathered in when this requirement was adopted approximately seven years ago, and those few members may not fully meet the requirement.

opportunity to notify ECIA if a distributor is no longer authorized. Some authorized distributors also police others, again ensuring that only genuine, authorized components are listed on the website.

We asked Mr. Gray how ECIA deals with authorized distributors which also sell unauthorized inventory, as well as companies that are only authorized to sell in certain parts of the world. Mr. Gray acknowledged that this can be a challenging problem, since some manufacturers have broad product lines and will divide up authorizations, so that no distributor is authorized for all of that manufacturer's products. ECIA checks authorizations for specific regions, but its database does not break down that information by part number.

Mr. Gray also stressed that a company which is "authorized to sell" is not the same as an authorized distributor. An authorization to sell, or to buy and resell, only means that company is a customer, not a distributor. The onus is on the buyer to make sure that it is really purchasing from an authorized distributor and that the OCM's warranty will be conveyed with the sale. ECIA provides widgets and links that its members can place on their websites, showing that they are authorized distributors. Independent distributors are not eligible to become ECIA members. However, Mr. Gray pointed out that there is really no such thing as a fully authorized distributor, since all companies will sell product to their customers for which they are not authorized, based on a customer's specific request. Further, authorized distributors may sell components from multiple manufacturers that are competitors, although they must agree to abide by storage and handling requirements contained in their distribution agreements.

Mr. Gray indicated that one of ECIA's priorities is branding advocacy. For several years, ECIA was involved in a B2B advertising campaign about the benefits of buying through the authorized supply chain. Approximately 20 years ago, ECIA funded a study at Texas A&M that quantified the value of using distributors from the viewpoints of both customers and manufacturers. The study showed that it is more cost effective to buy from authorized distributors than to make direct purchases from OCMs. Mr. Gray mentioned that ECIA is updating the study at this time.

ECIA is also involved in anti-counterfeiting standards activity in SAE. Mr. Gray co-chaired the committee responsible for AS6496, and he has participated in other SAE committees as well. ECIA also collaborates with other organizations such as SIA and its Anticounterfeiting Task Force. ECIA co-signs public comments on Department of Defense and TSA regulations relating to anti-counterfeiting efforts, and it meets with Homeland Security and Customs and Border Protection. The organization has participated in DOJ's Microelectronics Work Group. DOJ also holds an annual Counterfeiting & Intellectual Property Theft meeting including general counsels from all industry sectors (e.g., entertainment, pharmaceuticals, electronics, consumer goods), along with government agencies such as the FBI and FDA. ECIA and SIA typically represent the electronics sector at these meetings, while DoD and its prime contractors are not usually in attendance.

Mr. Gray mentioned that while the dollar value of counterfeit electronics is quite high, the impact and consequences of the failure of counterfeit electronic components is extremely

significant and costly. To his knowledge, there has been little or no litigation initiated by OCMs. The MIL-AERO industry is more focused on protecting the supply chain than on punishing violators. Meanwhile, the government is more concerned about higher value consumer products such as Nike sneakers and Louis Vuitton handbags, so there is little criminal enforcement of electronics counterfeiters.

Mr. Gray further explained that for DoD, counterfeit electronics frequently enter the supply chain during maintenance and repair of legacy systems. The military uses long lifecycle systems and, while parts may have become obsolete, DoD may not want to incur the cost of requalification. Mr. Gray suggested that counterfeiters look for any scarcity in the marketplace, including parts that are no longer in production as well as items that are temporarily unavailable or that have long lead times. Mr. Gray stated that "scarcity equals opportunity."

ECIA submitted comments to DFARS Case 2014-D005, a proposed rule that addresses required sources of electronic parts for defense contractors and subcontractors. The final rule was enacted as DFARS Section 252.246-7008 (Sources of Electronic Parts) in May 2018. Mr. Gray observed that the final rule creates a three-tier system that requires contractors to obtain parts from (1) original manufacturers and their authorized suppliers; (2) suppliers that buy exclusively from OCMs and authorized distributors; and (3) contractor-approved suppliers, when parts are not otherwise available. Mr. Gray expressed concern that the provision authorizing contractors to buy from suppliers that obtain parts exclusively from the original manufacturers or their authorized suppliers creates a huge loophole that raises a number of questions: How can a contractor know that a supplier is really buying exclusively from OCMs and authorized distributors, and not from other sources? Does the manufacturer's warranty flow through? Have the parts been handled properly? Even if the parts are tested and appear to be authentic, are they reliable? Mr. Gray said this provision was intended as a set-aside for small businesses, but he believes it is highly problematic. He recommends that the provision should either be eliminated or, at the very least, it should be moved down a tier and should only be an option when parts are no longer in production and are not available from an OCM or authorized distributor. He also pointed out that many authorized distributors are, in fact, small businesses.

When asked about testing, Mr. Gray indicated there is a place for testing in the supply chain, but he also believes that testing increases dependence on the gray market. Buyers should consider whether the test lab is independent of the seller and should also ask what the lab is testing against. Mr. Gray said there is no gold standard for testing, because OCMs will not provide exemplars and will not share their "secret sauce" with testing labs or anyone else. He mentioned that Honeywell conducted a test a few years ago where it sent a mixture of counterfeits and authentic parts to the ten best test labs, and they missed 20 percent of the counterfeits. Buyers also have to consider whether all parts on a reel are being tested, since counterfeits may be comingled with authentic parts on a reel. A particularly problematic area is RoHS testing, which is usually destructive and quite costly. Mr. Gray also pointed out that some sellers will not accept returns of product that has been tested, even if it has been identified as suspect counterfeit.

We asked Mr. Gray for his views on use of machine vision technologies to screen for counterfeit parts. He told us that industry's position is that it is not necessary to incur this cost when buying from an OCM or an authorized distributor. Further, even if machine vision technologies can prove that a part is genuine, they cannot show how it was stored and handled or whether it has been tampered with or tainted with malware. As a result, Mr. Gray believes that machine vision technologies would only benefit the grey market, not OCMs. Indeed, he feels they could actually encourage purchases from unauthorized sources, especially where a customer needs parts quickly to avoid shutting down production or otherwise does not care whether it buys from an authorized distributor.

Returns are also a concern. Counterfeit parts can be included with returns, which are often co-mingled with other parts. Mr. Gray noted that SAE has strict standards on returns, but some authorized distributors have subsidiaries who can sell returns. Mr. Gray suggested that active semiconductor products should be nonreturnable by customers. Contract manufacturers are another source of co-mingled inventory, and parts become untraceable when they sell off excess unused inventory. Mr. Gray characterized contract manufacturers as a "black hole of information."

Mr. Gray also discussed his work as co-chair of the SAE committee that developed the AS6496 standard. The standard is up for its five-year review, and it is possible that a revised version of the standard will address gaps in the DFARS. However, Mr. Gray again stressed that buyers need to focus on individual transactions and ask whether, at the time of sale, the seller is performing authorized distribution. Buyers should not be asking whether a company is an "authorized distributor," but whether they are performing authorized distribution at the time of a particular sale. Definitional differences between the prime standard and AS6496 may also be addressed in the upcoming review, although Mr. Gray noted that the review has not yet been formally opened.

Mr. Gray ended our discussion by sharing his views on legal and policy issues relating to counterfeits. First, he observed that the approved vendor list for DLA includes several unauthorized distributors. The authorized market almost always has some inventory available, and he feels that procurement officers should devote more effort to sourcing parts from an authorized source. He noted that this problem occurs more at DLA than with prime contractors, who now have diligent anticounterfeiting procedures in place. In addition, Mr. Gray restated his concerns about the definition of "exclusively buy from" in DFARS Section 7008, and he again suggested that any small business set aside should be directed to authorized distributors and/or that the provision should be moved to a lower tier. Finally, Mr. Gray concluded by saying that better testing and certification of test labs is needed. He also noted that there needs to be a broader effort of certifying testing labs, such as the lab accreditation being considered in SAE AS6171.

Faiza Khan Interview Summary

Maryland Carey Law and CALCE spoke with Faiza Khan on May 11, 2020. Ms. Khan is the Executive Director of IDEA (the Independent Distributors of Electronics Association). IDEA is an association of independent distributors that promotes quality initiatives in the supply chain. It focuses on disseminating information to its member and other independent distributors with the goal of "stamping out counterfeit components." IDEA provides Responsible Procurement Solutions™, a process for procurement of electronic components, inspection, and disposition of suspect counterfeits.[1] Ms. Khan stated that IDEA's mission is to ensure that what goes in an independent distributor's door and then goes out to a purchaser should never be substandard.

IDEA has created a set of standards by which its members must abide. Ms. Khan explained that, prior to IDEA, the reputation of independent distributors in the supply chain was extremely poor. IDEA's members joined together to develop standards for purchasing and handling of electronic components, thereby letting the industry know that the member companies don't wish to be linked with unethical distributors who do not care about their businesses or their customers.

Ms. Khan compared the business models of authorized and independent distributors. An authorized distributor is franchised to purchase parts directly from manufacturers, although she noted that some authorized distributors also buy from sources other than OEMs and OCMs. Some independent distributors may be franchised for particular parts, but much of their business (approximately 80 percent) is brokering parts. That is, generally independent distributors don't own a substantial amount of inventory; instead, they buy parts from other distributors. Some of their purchases may be from franchisees, but a lot of it is not.

Ms. Khan discussed IDEA's standards at length. Currently, IDEA has two standards: IDEA-STD-1010 (Acceptability of Electronic Components Distributed in the Open Market) and IDEA-QMS-9090 (Quality Management System Standard for Independent Distributors of Electronics Association Members). In addition, the organization is working on a purchasing standard, but its release has been delayed. The new standard will expand the purchasing guidelines relating to procurement in IDEA-QMS-9090, meaning that it will be more directed to buyers than IDEA-QMS-9090.

According to Ms. Khan's understanding, IDEA-STD-1010-A was the first standard developed and released by the association.[2] However, it was clear that additional work was needed, and about three years later IDEA-STD-1010-B was released. IDEA is currently working on another revision, although she is not sure when IDEA-STD-1010C will be introduced. Ms. Khan enthusiastically commented that there is "no document around like 1010-B," due to its photo comparisons and the level of detail it contains. The next revision, 1010-C, is currently under development and should be available towards the end of 2021. She believes it will be "a

[1] See https://www.idofea.org/about.html.
[2] Ms. Khan was not employed at IDEA when the 1010 standard originally issued.

significant update over an already great document." At approximately the same time that 1010-B was issued, IDEA also introduced its IDEA-QMS-9090 Quality Management System Standard, as well as the IDEA-ICE-300 Professional Inspector Certification Exam.

Ms. Khan explained that the 1010 standard relates to visual inspection and distinguishes between counterfeit and substandard parts. IDEA defines a "counterfeit" as any part that is being represented as another. While some people also include refurbished parts as counterfeits, IDEA classifies refurbished parts as "substandard," meaning that inspection has identified something that needs to be looked at more closely. Ms. Khan indicated that IDEA does not want to use the "counterfeit" label too loosely.

Ms. Khan stated that all parts must be visually inspected, even though this may be burdensome and take time. Some customers demand 100 percent visual inspection, while others may require less. Nevertheless, most independent distributors conduct some form of visual inspection. Independent distributors do not assume they can trust the label on a part, since all companies have been "burned" too many ties. While the 1010 standard requires a thorough visual inspection, which could include x-ray and XFM characterization as well as decapsulation, some customers require other forms of testing also. For example, the DoD requires electrical testing of its parts. However, for most customers, thorough visual inspection eliminates the need to send all parts to electrical testing.

If a company identifies a counterfeit or suspect counterfeit part, they will not send it to a customer. If the inspection identifies some other anomaly (e.g., an incorrect date code), then the distributor allows the customer to decide if it is willing to accept the parts. The distributor will consider the data, and if the data points to a part being counterfeit or suspect, then it would be labeled that way.

IDEA-ICE-3000, the Professional Inspector Certification Exam, is not a standard, but instead is an online examination administered by IDEA. The exam covers 10 topics pulled from the 1010 standard. It is an open-book exam and has a 95 percent pass rate, but it requires experience in order to pass. Ms. Khan indicated that the questions can be "tricky" and require practical knowledge of inspection techniques.

IDEA-QMS-9090, the Quality Management System Standard, is intended for internal use by IDEA members, although other independent distributors also use it as guidance. The standard addresses issues relating to storage and shipment of parts, such as moisture sensitivity, storage conditions, limiting access to the warehouse, escrow payments, and use of drop shipments. IDEA conducts an annual audit to ensure that members are following these guidelines and adhering to a code of ethics. The member first submits information to IDEA, which is then followed by a telephone call with IDEA. Ms. Khan explained that IDEA is to small to conduct site visits as part of the audit process.

While IDEA members are required to practice the 1010 and 9090 standards, other nonmembers use them as well. Ms. Khan commented that all respectable independent distributors use the techniques in the 1010 standard to inspect their products, but not all use the

9090 standard. Some nonmembers may take ideas from the 9090 standard but, in many cases, they are already ISO certified and therefore they do not need to strictly follow the 9090.

We asked Ms. Khan for her views on the use of machine vision technologies to identify counterfeit parts. She told us that she does not fully understand machine vision, although she knows that it is useful in the manufacturing industry to verify uniformity. However, she believes that for part inspection, machine vision technologies need further development before they will be truly useful. For example, automated X-ray inspection is currently used, but there are concerns about false failures when inspecting parts on a reel. If the parts are turned slightly on the tape, then a human inspector would have to intervene and use his or her personal judgment to decide whether there has been a false failure. Ms. Khan indicated that IDEA would be open to including machine vision inspection in the 1010 standard, but it would have to account for false failures and would have to include cautionary language about use of the technology.

Ms. Khan mentioned her involvement in other standards setting organizations, such as the G-19D committee and the SAE 6081 standard. IDEA has also been involved with the Component Obsolescence Group (COG), a subgroup of IIOM, headquartered in Germany. Ms. Khan explained that IDEA is largely North America-centered, and it is essential to have an international network since parts come from Asia and global sourcing is the norm.

Ms. Khan ended our conversation by sharing her views on counterfeit electronic parts in the marketplace. She described the situation as “very scary” and believes that counterfeiting has not yet peaked. She thinks it is a problem that is not going away and, in fact, she expects it to get worse. She observed that counterfeits are becoming increasingly sophisticated, and she expressed particular concern about clones. Ms. Khan mentioned that she is interested in learning more about use of Blockchain for counterfeit prevention, including length of time to adoption, expense, and whether others would buy into its use. Ms. Khan concluded by stating that customers also have a responsibility to be very specific about what they expect from independent distributors, since some unscrupulous distributors work out of their garages and don’t inspect product.

Andrew Olney Interview Summary

Maryland Carey Law and CALCE spoke to Andrew Olney on May 13, 2020. Mr. Olney is the General Manager of Technology Development at Analog Devices, Inc. He became a member of the Anticounterfeiting Task Force ("ACTF") of the Semiconductor Industry Association ("SIA") in 2006, and he chaired the ACTF from 2011 to 2013. Analog discontinued its SIA membership in 2018, after ADI acquired Linear Technology Corporation in 2017. However, Mr. Olney remains very active in anticounterfeiting efforts.

Mr. Olney described SIA as an association that represents approximately 80 percent of the semiconductor industry (including companies with fabs and those that are fabless). The organization engages in lobbying activities, including those relating to anticounterfeiting, and it develops policies intended to strengthen the industry. Mr. Olney suggested that we talk with someone at SIA for additional information about the organization, and he also directed us to the SIA website.

During the time that Mr. Olney chaired SIA's ACTF, one of the most significant outcomes was a 2013 white paper entitled "Winning the Battle Against Counterfeit Semiconductor Products," on which he was the principal author.[1] Mr. Olney indicated that he worked with representatives of 10-12 other companies, who assisted in editing the white paper; those individuals are credited in the Acknowledgements on page 27. As a result, the paper represents the views of the group.

Mr. Olney stressed that, although the white paper was prepared in 2013, he believes it is still fully applicable today. For example, the white paper contains a definition of counterfeiting that was agreed upon by six worldwide semiconductor associations: "Semiconductor counterfeiting is considered the act of fraudulently manufacturing, altering, distributing, or offering a product or package that is represented as genuine."[2] Mr. Olney indicated that the definition took time and effort to develop, and he believes it is still accurate today.

Mr. Olney commented that there have not been many major counterfeiting cases since the whitepaper was written in 2013. One exception was the case against Rogelio Vasquez from PRB Logics Corporation, prosecuted by Assistant US Attorney Lisa Feldman in the Central District of California. Mr. Vasquez was sentenced to 46 months in prison for selling counterfeit integrated

---

[1] See https://www.semiconductors.org/wp-content/uploads/2018/06/SIA-Anti-Counterfeiting-Whitepaper-1.pdf. Mr. Olney provided us with a copy of the white paper in advance of our conversation.

[2] *Id.* at 3. The white paper also recites the definition of counterfeit electronic part contained in the January 2010 report of the Bureau of Industry Security (a counterfeit electronic part is "one that is not genuine because it: is an unauthorized copy; does not conform to original OCM design, model, or performance standards; is not produced by the OCM or is produced by unauthorized contractors; is an off-specification, defective, or used OCM product sold as "new" or working; or has incorrect or false markings or documentation, or both.") See id. at 2-3.

circuits from China, which were purchased by military suppliers.[3] Mr. Olney explained that semiconductor companies support the government in these kinds of cases. Analog, Mr. Olney's employer, conducts counterfeit testing for law enforcement and for Customs and Border Protection ("CBP"), because it wants to assist government agencies that investigate and prosecute companies that sell counterfeit parts. In return, the semiconductor companies may receive restitution for cases where they have assisted law enforcement, although it could be a very small amount of money.

Conversely, Mr. Olney observed that Analog will not perform counterfeit testing for companies that have purchased parts from brokers or independent distributors. Analog provides no support to those companies because, even if Analog verified the authenticity of the parts, there is no way of knowing how the parts have been handled and stored. Such parts could have terrible quality and reliability, due to exposure to electrostatic discharge, high temperatures, and other conditions. Instead, Analog would politely tell the customer to buy from authorized distribution channels, since Analog audits its authorized distributors to ensure that parts are handled and stored correctly.

Mr. Olney discussed Analog's policies and procedures for dealing with counterfeiters. If Analog sees a broker using the Analog logo, it will send a cease and desist letter to that broker. Other semiconductor companies follow the same practice, and the companies also share information with one another. Upon receipt of a cease and desist letter, the vast majority of brokers in the U.S. will stop displaying the Analog logo. However, Mr. Olney acknowledged that it is more difficult stopping trademark infringement in other countries, especially China. Even in the U.S., a few brokers may simply set up another company with a new name and then continue using the Analog logo and trademarks.

In addition, Analog records its registered trademarks with CBP. CBP monitors shipments coming into the U.S. from China and other suspect areas. CBP may take high-resolution photos of suspect parts and, based on these photos, Analog can then determine if the parts are authentic. Mr. Olney explained that Analog looks for certain trade secret features in the photos, which allows it to make an accurate determination of authenticity in 98 to 99 percent of cases. Again, however, Mr. Olney noted that authenticity does not equate to reliable operability.

Throughout our conversation, Mr. Olney repeatedly stated that purchasing from authorized distribution channels is the only solution to the counterfeiting problem. He noted that this is even truer today than it was in 2013 when SIA's ACTF issued its whitepaper on counterfeit semiconductor products.

We asked Mr. Olney for his views on the use of machine vision technologies to detect counterfeit parts. He clearly stated that Analog sees absolutely no value in machine vision, because operators do not have the expertise to make accurate authentication determinations. Indeed, he believes they are wrong approximately 50 percent of the time. Similarly, Mr. Olney

[3] Mr. Olney provided us with a May 30, 2019 press release from the U.S. Department of Justice, containing more information about the case against Mr. Vasquez. A copy of the press release is attached to this interview summary.

sees no value in a database of registered parts. He noted that previously DLA tried to use DNA marking to identify authentic parts, but that program did not go well at all. Mr. Olney indicated that in order for a system to make accurate authenticity determinations, proprietary information from Original Component Manufacturers (OCMs)s would be required, and he does not believe manufacturers will supply that information.

Mr. Olney stated that DMEA and defense contractors sometimes still turn to unauthorized sources, despite the fact that he and others continue counseling them to use authorized suppliers only. He does not believe that obsolescence provides an excuse for purchasing from unauthorized sources. Analog very rarely obsoletes parts that go into government systems; the company has parts dating back to the 1970s. It continues to manufacture parts specifically so that the government will not have to purchase from unauthorized sources. Mr. Olney acknowledged that some companies do obsolete parts, particularly parts containing lead solder that have been made obsolete because of environmental regulations. In those circumstances, the government can still purchase parts from Rochester Electronics (an authorized distributor and licensed manufacturer) and authorized resellers that distribute legacy products. However, Mr. Olney believes that the government sometimes chooses to buy from unauthorized sources because "they can get the parts cheaper there."

In conclusion, Mr. Olney's message is clear: the only way to avoid counterfeit parts is to purchase from authorized sources. He quoted the SIA whitepaper, which states, "The key to winning the battle against counterfeit semiconductors is elegantly simple: exclusively buy semiconductor products either directly from the Original Component Manufacturer (OCM) or from the OCM's Authorized Distributors/Resellers."[4]

[4] See SIA white paper at 24.

Kevin Sink Interview Summary

Maryland Carey Law and CALCE spoke with Kevin Sink on May 8, 2020. Mr. Sink is the Vice President of Total Quality at TTI, Inc. He described TTI as an authorized distributor of electronic components such as resistors, capacitors, and connectors (i.e., the types of components that make up about 80 percent of a typical PC board's population). Mr. Sink said that TTI is distinct in the market because, while it sells these types of electronic "nuts and bolts," TTI does not sell integrated circuits. According to Mr. Sink, TTI has over 20,000 customers. Last year, it sold 252,000 different SKUs or part numbers, shipping them out on over 2 million unique line items.

In his role as Vice President of Total Quality, Mr. Sink works with military and aerospace customers on problems they are experiencing with products they purchased and working with suppliers to resolve those problems. Approximately 90 percent of those problems relate to defects in material. Mil-aero customers represent approximately 20 to 25 percent of TTI's business today, but that sector represents about 80 to 85 percent of the work of his group.

As an authorized distributor,[1] TTI has contracts with original component manufacturers (OCMs) that include both responsibilities and benefits. TTI is required to market the OCM's products, promote them, and get customers to use these products in their designs. TTI also provides logistics for OCMs: it must purchase the OCM's products and maintain them in inventory. This allows customers to obtain parts more quickly; ordering directly from the OCM could result in a delay of 8 to 28 weeks before parts are received, whereas authorized distributors keep the parts readily available. However, TTI is required to inventory parts in a manner that is consistent with the OCM's storage practices, including climate control and protection from electrostatic discharge and moisture. The OCM audits TTI to make sure that proper storage procedures are followed. By safely warehousing and handling parts, TTI can pass the manufacturer's warranty along to its customers. The relationship also creates a known chain of custody for the parts, from the OCM to the authorized distributor to the customer.

OCMs conduct audits of their authorized distributors, although the frequency of those audits varies by manufacturer. Some OCMs conduct audits annually, while others audit distributors only every three to five years, or only when the authorized distribution contract is originally signed. OCMs who have more military business typically conduct audits more frequently. These audits look at whether inventory is being handled and stored correctly, but they do not physically verify where the parts originated from. OCMs analyze this through the review of specific reports. They verify the quantity of pieces shipped to customers by the distributor (point of sale) against the quantity of pieces sold to the distributor (point of acquisition). For

[1] Mr. Sink indicated that "authorized distributor" is a relatively new term that has come into use over the past ten years. Previously, authorized distributors were referred to as "franchised distributors." Today, that term is falling out of favor in the U.S., since it does not meet the commonly understood definition of a "franchise" as we might understand say with hamburger chains. While "Authorized distributor" is also used in Europe and Asia, it is still likely to hear the term "Franchised distributor" in those geographies.

example, if TTI sold a million pieces of a particular part but only bought 200,000 of that item from the manufacturer, that would raise questions about where TTI obtained its inventory.

TTI also receives certain benefits from its contract with the OCM. It receives special pricing, and it also has the ability to return some inventory that is not selling. Authorized distributors may also receive a scrap allowance in lieu of a return allowance, which would allow TTI to destroy unsold product instead of returning it to the manufacturer. Manufacturers do expect the product to be "scrapped," though they may or may not require a formal "scrap certificate" from their distribution partner. Distributors want to scrap products that are not selling in order to free up inventory dollars. Mr. Sink observed that returns and scrap allowances encourage TTI to take new products even if it is not sure the items will sell.

TTI's scrap is sent to a destruction facility, where it is ground up and then melted down. TTI uses a company that provides certified destruction so that TTI can be sure the product has been destroyed, rather than being recycled in an irresponsible way (e.g., e-waste shipped to third world countries) or resold. Scrap is not sold into the independent distribution chain.[2] Mr. Sink explained that OCMs do not want to do business with a distributor that used its scrap allowance and claims it destroyed product, when it actually sold that product to an independent distributor (i.e., the gray market). TTI has never sold product into the gray market. Instead, every quarter the company scraps about $1 million in inventory, and it recoups approximately $25,000 for the gold and silver that is recovered when the scrap is melted down.

In order to prevent counterfeits from entering its distribution chain, TTI cannot purchase products from the open market. For example, if a manufacturer of electronic devices (e.g., cellphones) has a large surplus of components, it may put those parts on the market at a drastically reduced price. TTI is ethically and contractually precluded from purchasing such parts and offering them for sale as if they came from the OCM; it can only buy parts directly from the OCM.[3] An independent distributor, on the other hand, can buy from the open market, as well as from an OCM or from another distributor (authorized or independent).

TTI does not sell any parts for which it is not authorized, although other distributors may sell a combination of authorized and unauthorized parts. Often those companies start out as brokers, then they move up in the supply chain as they acquire customers and a good reputation. They may develop a mix of authorized lines and independent distribution. Some very large companies also have authorized and independent lines, which they are required to keep separate.

Mr. Sink also discussed the length of time that parts can be held in inventory by TTI. Some parts have a shelf life, such as those with adhesive that may degrade over time. However, only about 500 products out of 250,000 have an actual shelf life. Otherwise, there are no significant restrictions on shelf life. Mr. Sink recalled that there used to be concerns about shelf

[2] Mr. Sink further explained that authorized distributors naturally do not want to sell product to independent distributors, because independent distributors take sales away from authorized distributors.
[3] Mr. Sink indicated that in some instances, an authorized distributor can also purchase parts from another authorized distributor. One authorized distributor might purchase parts from another in order to fill a customer's order. However, Mr. Sink stated that TTI is unlikely to purchase parts from another distributor and typically refers the customer to the other authorized distributor for that purchase.

life of soldered parts, but he explained that component plating and termination have improved so that is no longer a concern. Even so, some customers retain a policy that they will not buy parts over two years old, while others will not buy parts over five years old. Again, these policies relate to concerns about solderability.

OCMs, on the other hand, make decisions about when to end production of a part depending upon their assessment of the market and how quickly they expect customers to move to a new replacement part. When the OCM issues a product change notice or an end of life notice, TTI may purchase some of the discontinued parts so that it will have the parts in inventory when other distributors do not. Some customers may also purchase one to five years' worth of production through TTI, but in that instance the customer would be responsible for storage. Mr. Sink mentioned that currently, TTI does not purchase five years' worth of inventory and store it; there are specialty companies that operate in that space.

Mr. Sink explained that it is very important to its customers that TTI is an authorized distributor. Reputable companies buy product through authorized channels, and today, customers in the MIL-AERO space are required to purchase electronic parts from authorized distributors. As part of small/disadvantaged business targets of federal contracts, prime contractors are supposed to give some portion of their business to small companies, which they often do by purchasing from brokers who bought parts from authorized distributors. Mr. Sink explained that the DFARS requires that parts in production be purchased from an OCM, its authorized distributor, or an entity that purchases parts from the OCM or an authorized distributor. He believes this requirement leave the door open to purchases from brokers.

Mr. Sink observed that there is also an economic incentive to purchase from authorized distributors, since they offer better pricing than brokers. He noted that if a broker is offering a lower price on a part than the authorized distributor, a purchaser should be wary because there should be an extra layer of markup, making the broker's pricing more expensive than the authorized distributor. Most companies do not want to accept that risk.

When TTI ships parts to a customer, the customer receives a packing slip with a certificate of conformance ("COC"). The COC states that the part was built according to the specifications of the manufacturer or military specifications. However, Mr. Sink stated that every defective part he has dealt with at TTI has had a COC. As a result, focus on COC's as part of counterfeit prevention is inordinate. Mr. Sink explained that manufacturers produce so many parts like capacitors that there is no way anyone can look at each part with any degree of scrutiny. Instead, he suggested that what's really needed is traceability. Some prime contractors in the defense industry will request a certificate of traceability, but most customers only want a COC.

Mr. Sink discussed the definition of a "counterfeit" part. He defines a "counterfeit" as a part that the manufacturer determines that it did not make. He expressed dissatisfaction with other definitions of "counterfeit." For example, there is a long history of the DoD labeling things as "counterfeit" when they are actually fraudulent or nonconforming parts. Specifically, Mr. Sink believes that old parts sold as new are fraudulent, not counterfeit, because they are genuine parts from an OEM or OCM. He also expressed frustration with the practice of labeling

something that doesn't work right as a "counterfeit" or "suspect counterfeit," even though it too is a genuine part. Further, AS6496 contains a definition that is now inconsistent with the G-19T definition, but he believes that is the result of timing and expects that the AS6496 committee will likely adopt the G-19T definition in the future. This reflects an evolution of the internal debate over the appropriate definition of "counterfeit," and it is important to look at the most recent documents to get a picture of where people are currently on the definition. Mr. Sink further explained that the G-19T definition has been repeated by numerous committees as they try to align with the government's definitions while also being applicable globally, where the U.S. government's definition is less relevant.

If a customer notifies TTI that it has parts that are not working properly, TTI will send samples of those parts to the manufacturer, which then tests the parts and can determine whether it made the parts or not. Some parts are flagged as suspect counterfeits when they do not look like other authentic parts that TTI has in stock, do not appear to meet specifications, or do not contain information that TTI has requested to appear on the label. An authorized distributor usually has a specific tag or marking on the products that it sells, although Mr. Sink noted that fake labels are more likely when dealing with expensive products or one that are hard to find. TTI will also determine whether a product was returned in TTI's packaging or in customer packaging.

Mr. Sink observed that usually when a customer returns parts to TTI as suspect counterfeits, there is something about those parts that looks suspicious. However, manufacturers sometimes remark their products, and the parts turn out to be authentic. Similarly, parts are made at a certain tolerance, and some parts simply are not within that tolerance. However, Mr. Sink acknowledged that "once in a blue moon" TTI receives a return where the markings are bad, and the part is determined to be counterfeit. In each of these cases, it was determined that the customer did not obtain the part from TTI. Instead, they came from a broker or another source, and the customer then intermixed its inventory and returned the part to TTI by mistake.

When TTI does identify a counterfeit electronic part, the part is placed in quarantine at TTI's facility. TTI quarantines parts by placing them in a locked cabinet in the same type of atmosphere as its warehouse (e.g., air conditioning, other controls). Counterfeit parts are not returned to the customer, and the customer does not get credit for the return. Mr. Sink does not feel that it is burdensome for TTI to quarantine parts since it requires only a small space in the warehouse. In fact, TTI still has all of the parts it has ever placed in this quarantine.

The OCM decides whether to report the counterfeit parts to GIDEP, since the manufacturer has the expertise to decide whether a part is counterfeit. Mr. Sink indicated that TTI will not report instances of counterfeits to ERAI, because ERAI supports the broker community and TTI does not want to do anything that would assist the competing business model of independent distribution. Nevertheless, Mr. Sink believes that ERAI has better data than GIDEP. Likewise, the manufacturer decides whether to pursue a case against the counterfeiters. Many OCMs feel that they do not lose enough money to counterfeit parts to make it worthwhile to file a civil suit or request criminal prosecution. In Mr. Sink's experience, law enforcement has never asked for parts that TTI is holding in quarantine. Individuals have

been prosecuted for counterfeiting parts, but they are charged with adjacent crimes like wire fraud, not a specific violation of the 2012 NDAA.

Finally, Mr. Sink discussed TTI's involvement with industry standards. He identified SAE's AS6496 as the leading standard relating to authorized distributors. Currently, there is no requirement that authorized distributors be accredited under that standard. He explained that when AS6496 was adopted, authorized distributors did not want to have a separate accreditation since AS9120 and ISO 9001 were already in effect. He observed that most companies have not rushed to obtain AS6496 accreditation, because the required audits are intensive and time consuming, and very few customers demand AS6496 accreditation. In his experience, TTI's customers are satisfied by the fact that TTI is an authorized distributor. Despite the fact that they do not seek accreditation, many companies follow the processes and measures set forth in AS6496 and other standards, which are viewed as best practices that are expected by customers including major defense contractors.

Mr. Sink and TTI have been involved with other SAE standards also, including AS6081 for independent distributors and the G19T terms and definitions standard. Mr. Sink was previously active in ECIA (formerly "NEDA" or the National Electronic Distributors Association), the original group that put together a position paper that ultimately became AS6496.

Mr. Sink concluded our discussion by observing that the FY 2012 NDAA and resulting regulations were "game-changers." Previously, only those who had first-hand experience with counterfeits expressed any real concern. After DoD created these new rules, the market started taking counterfeits more seriously, and customers started caring about whether they were doing the right thing. Usage of brokers, and the distinction between authorized distributor and independent distributor, became more relevant concerns. TTI saw an increase in the number of smaller businesses buying from authorized distributors in order to avoid counterfeits. However, beyond military and aerospace, Mr. Sink feels that there is far less awareness of the risk posed by counterfeits. He believes that the auto industry in particular is lagging, although he recognizes that auto manufacturers usually buy directly from parts manufacturers because they buy in such quantity. The same is true of the medical field.

When asked about machine vision technologies, Mr. Sink indicated that they have promise if only a camera and a database are required. In order to be attractive, these technologies must be low cost and cannot require that anything extra be added to the part. He feels that machine vision could potentially be better than added DNA or other taggants which require additive production steps and specialized readers. He stressed that companies do not want to spend extra money for add-ons.

Richard Smith Interview Summary

On April 17, 2020, Maryland Carey Law and CALCE spoke with Richard Smith. Mr. Smith is the Vice President of Business Development at ERAI, Inc., an information services organization that maintains a database of suspect counterfeit and nonconforming electronic parts and high-risk suppliers. Mr. Smith provided a demonstration of the capabilities of the ERAI database, and he also answered numerous questions about ERAI's services and training.

ERAI was founded in 1995, and Mr. Smith recalled that it received its first report of a suspect counterfeit part in 2001, shortly after China joined the World Trade Organization. ERAI's global membership include contractors, manufacturers and distributors from the medical, defense, aerospace, and nuclear fields, as well as governmental agencies and industry organizations. ERAI receives its information from test labs, prime contractors, and distributors, among others. Reports can be submitted by members and non-members, although only members can access reports in the ERAI database.

ERAI works with Homeland Security, Customs and Border Protection, the IPR Center, the DoD agencies, and even local law enforcement. For example, Mr. Smith mentioned that there were 49 reports or alerts submitted to ERAI relating to VisionTech Components, and in 2010 a federal indictment was issued against Shannon Wren, the owner of the company. Such indictments are included in the ERAI database and can be searched by members.

ERAI also enjoys a good rapport with GIDEP, although Mr. Smith said he believes that ERAI has far more data than GIDEP. In part, he believes this is due to the fact that, unlike GIDEP, reporting companies can report anonymously to ERAI. He suggested that companies may be more willing to report suspect counterfeits if they do not have to disclose their identity, which he said could be problematic or awkward. In addition, ERAI reports may be filed against a part number, as opposed to the supplier of the part. This feature allows the community to be made aware of suspect counterfeit parts in the supply chain without identifying the source.

Although ERAI focuses on electronics, Mr. Smith explained that it can list any part that has a part number. For example, Mr. Smith said that he recently gave a presentation to the Nuclear Regulatory Commission, and now members of the nuclear industry have started reporting to ERAI. He showed us reports of Baumer gauges and related counterfeits that were subsequently submitted to ERAI. In addition, the database contains some bearings and other non-electric parts. However, ERAI does not have a way to share information on materiel that does not have a part number (e.g., chemicals, bulk steel), or where there is nothing with which to compare the problem part. Similarly, materials that are authentic but contain hazardous ingredients (e.g., drywall) cannot be reported. Mr. Smith noted that ERAI is certainly capable of expanding beyond electronics, although some industries are highly risk adverse and view reporting as leading to potential liabilities.

Mr. Smith discussed ERAI's process for reporting suspect counterfeit parts. Reporting parties are asked to submit a description of the non-conformance, along with photos or other digital images illustrating the problem. Testing data can also be attached to a report. ERAI then

conducts an investigation to determine the validity of the report, and it contacts the company against which the alert was filed so the accused company can respond to the complaint. If the accused company disputes the complaint, ERAI reviews the situation and may attempt to mediate a resolution between the parties. If a resolution cannot be reached, or if the accused company does not respond, the report is included in the ERAI database. ERAI does not conduct any testing itself; instead, it relies on what is reported to it. Reports from non-members are accepted and vetted in the same manner as reports from members.

Mr. Smith observed that today, the supply chain is doing a much better job of eliminating counterfeit parts before they reach the prime contractors. As a result, most reports to ERAI are submitted by distributors and brokers, not by defense contractors. However, the use of COTS parts has had a negative effect. Mr. Smith noted as an aside that when GIDEP reporting became mandated, purchasing agents altered their contractual arrangements to purchases contingent on a non-counterfeit finding, meaning that they would never take possession of suspect counterfeit parts and were thereby alleviated of the requirement to report to GIDEP. ERAI also receives reports from labs when they conduct testing for companies, since they consider this to be good advertising for the test lab. In other instances, test labs will not provide their reports to ERAI, but the company that hired the lab will file an alert with ERAI.

Mr. Smith commented on the difference between the "nonconforming" versus "suspect counterfeit" designations in the ERAI database. "Suspect counterfeit" reports contain sufficient evidence to show that a part is not authentic (e.g., evidence of blacktopping). "Nonconforming" means that here is not enough evidence to clearly conclude that a part is not authentic, or the part may be authentic but there are other problems that nevertheless make it risky to use that part (e.g., corroded leads, failed electrical testing due to improper handling).

In addition to maintaining the High Risk and Counterfeit Database, ERAI also provides education for its members and non-members. A new division called InterCEPT offers training and certification programs on inspection and testing of electronic parts. Other offered services include risk mitigation tools and real time alerts, a database of photographs of nonconforming parts, and electronic components sourcing services.

Appendix 20.

Patent Landscape Table of Search Results on Machine Vision Technologies for Counterfeit Electronic Part Detection

Name	Type	Feature	Owner	Patent #	Status	Column1	Expiration	Gov't Funding	Abstract
Method and a system for verifying authenticity safe against forgery	Identification of Relevant Features	Fingerprint	DASY INTER SA	US4218674	Expired	9/9/75	8/19/97		This invention relates to a method and system for verifying authenticity safe against forgery of an object releasing a function said object being of base material having random imperfections in or on the same, comprising measuring random imperfections in or on the base material of said object in a predetermined measuring track over the surface of said object of base material having random imperfections in or on the same by means of a detector for detecting said random imperfections, said random imperfections optionally being supplied to said base material, converting said measured random imperfections into pulses, supplying said pulses together with timing pulses to an AND gate, whereby only simultaneously arriving pulses are passed, supplying said passed pulses to a shift register shifting with said timing pulses to obtain a binary code, comparing said binary code with a previously stored binary code of the same object, whereby the function is released if said binary codes are identical; as well as a system for carrying out the method.
Locating regions in a target image using color matching, luminance pattern matching and hue plane pattern matching	Analyze Features	Measure Features	National Instruments Corp	US6944331	Active	10/26/01	6/30/23		A system and method for locating regions in a target image that match a template image with respect to color and pattern information. The template image is characterized with regard to pattern and color. The method comprises performing a first-pass search using color information from the color characterization of the template image to find one or more color match candidate locations. For each color match candidate location, a luminance, i.e., gray scale, pattern matching search is performed on a region proximal to the location, producing one or more final match regions. For each final match region a hue plane pattern match score may be calculated using pixel samples from the interior of each pattern. A final color match score may be calculated for each final match region. A weighted sum of luminance pattern match, hue pattern match, and color match scores may be calculated, and the scores and sum output.
Authentication method and system	Image Processing	Manipulating Digital Image	CoPilot Ventures Fund III LLC	US10089478	Active	9/4/02	9/4/23		The present invention provides a method and apparatus for the production and labeling of objects in a manner suitable for the prevention and detection of counterfeiting. Thus, the system incorporates a variety of features that make unauthorized reproduction difficult. In addition, the present invention provides a system and method for providing a dynamically reconfigurable watermark, and the use of the watermark to encode a stochastically variable property of the carrier medium for self-authentication purposes.
Security markers for determining composition of a medium	identification of Relevant Features	Fingerprint	NCR	US7256398	Active	6/26/03	6/10/24		A method of determining a component of a medium comprises illuminating the medium to excite a marker associated with the component. Detected photoluminescent emission from the marker in response to the excitation is compared with one or more emission profiles. The component is identified based on a match between the detected photoluminescent emission and at least one of the emission profiles.
Random-type identifying material, 3-D identifying system and method using the same	Identification of Relevant Features	Fingerprint	Kwang-Don Park	US7576842	Expired - fee related	7/4/03	N/A		The present invention relates to a random type recognition object for an identification apparatus wherein identification particles are distributed irregularly within a 3D shape and a positional value and a characteristic value of the identification particles distributed within the 3D shape in one or plural directions are recognized by separate recognition means, and an identification apparatus and method using a random type recognition object whose reproduction is impossible. Furthermore, the present invention relates to a product authentication system and method in which a purchaser transmits data extracted from a recognition object distributed together with a product using a recognition apparatus to an authentication system in order to determine whether purchased product is genuine, the authentication system transmits information on a product coincident with the received data to the purchaser, and the purchaser compares the purchased product with the information on the product received from the authentication system to determined whether the product is genuine.
Mobile hand held machine vision method and apparatus using data from multiple images to perform processes	Image Processing	Object Manipulation	Cognex Corp	US9798910	Active	12/22/04	8/8/27		A method and apparatus for performing a process associated with an item to be imaged is disclosed. The process requires data associated with a plurality of required features of the item to be imaged. A handheld device is used to obtain a sequence of images. For at least a subset of the obtained images, a camera field of view is directed toward the item from different relative juxtapositions while obtaining the images. At least a subset of the obtained images are examined to identify the required features. Images are obtained until each of the required features are identified in at least one image. Feedback is provided to a user indicating at least one additional required features to be imaged, required features that have already been imaged and guidance indicating how to manipulate the handheld device to obtain images of additional required features.
Idiosyncratic emissions fingerprinting method for identifying electronic devices	Identification of Relevant Features	Fingerprint	Barron Assoc Inc	US7420474	Active	5/13/05	11/23/25	U.S. Air Force Research Laboratory	A method of producing idiosyncratic electronic emissions fingerprints from an electronic device is disclosed wherein emissions produced by the electronic device are collected and converted into one or more digital electronic fingerprints. The method contemplates a variety of emissions, such as electromagnetic emissions (including radio frequency emissions) and vibrational emissions (including audio emissions). The emissions fingerprints of various types extracted from an electronic device can be combined into more complex emissions signatures, and/or they can be combined with conventional electronic fingerprints or other idiosyncratic identifying data. A drift-test method for compensation and correction of emissions fingerprint drift is also disclosed.

Name	Type	Feature	Owner	Patent #	Status	Column1	Expiration	Gov't Funding	Abstract
Method for extracting random signatures from a material element and method for generating a decomposition base to implement the extraction method	Identification of Relevant Features	Fingerprint	SIGNOPTIC TECHNOLOGIES	US8989500	Active	12/23/05	8/11/27		The present invention concerns a method for extracting a random signature from a subject material element, comprising: a phase to generate at least one acquisition vector of structural characteristics of at least one region of the subject material element, a phase to generate at least one random signature vector from the acquisition vector, the random signature vector comprising: at least one random component having a stable nature so that its value may be found on each implementation of the method on one same region of the subject material element, and/or at least one random component having an unstable nature so that its value is likely to vary random fashion on each implementation of the method on one same region of the subject material element, use of the random signature vector as random signature.
Sensing data from physical objects	Analyze Features	Measure Features	Digimarc	US9384390	Active	1/23/06	1/19/27		Directional albedo of a particular article, such as an identity card, is measured and stored. When the article is later presented, it can be confirmed to be the same particular article by re-measuring the albedo function, and checking for correspondence against the earlier-stored data. The re-measuring can be performed through us of a handheld optical device, such as a camera-equipped cell phone. The albedo function can serve as random key data in a variety of cryptographic applications. The function can be changed during the life of the article. A variety of other features are also detailed.
Amorphous alloy member and its application for authenticity determining device and method, and process for manufacturing amorphous alloy member	Identification of Relevant Features	Texture	Fuji Xerox Co Ltd	US8325987	Active	9/28/06	12/11/31		An amorphous alloy member including an irregular region having a center line average roughness Ra of about 0.1 μm to about 1000 μm on a surface, at least the irregular region including an amorphous alloy having an amorphous phase at a volume ratio of about 50% to about 100%. A process for manufacturing the amorphous alloy member, and an authenticity determination device and an authenticity determination method using the amorphous alloy member.
Detecting counterfeit electronic components using EMI telemetric fingerprints	Identification of Relevant Features	Fingerprint	Oracle	US8341759	Active	10/16/07	10/16/27		One embodiment of the present invention provides a system that non-intrusively detects counterfeit components in a target computer system. During operation, the system collects target electromagnetic interference (EMI) signals generated by the target computer system using one or more antennas positioned in close proximity to the target computer system. The system then generates a target EMI fingerprint for the target computer system from the target EMI signals. Next, the system compares the target EMI fingerprint against a reference EMI fingerprint to determine whether the target computer system contains a counterfeit component.
Method and device for identifying a printing plate for a document	Identification of Relevant Features	Defect Detection	Advanced Track and Trace	US8472677	Active	6/2/08	12/6/29		A method for identifying a printing plate for a document includes: printing at least one document with the plate, capturing, at high resolution, at least one image of at least one part of the document, extracting a geometric characteristic of at least one captured image, storing the geometric characteristic extracted, for a candidate document where one seeks to determine whether the printing plate was used to print it, capturing, at high resolution, an image of the part of the candidate document corresponding to the part of the document for which a geometric characteristic has been stored, extracting the geometric characteristic of the image of the candidate document corresponding to the stored geometric characteristic; and determining whether a correlation measurement of the geometric characteristic for the candidate document and the stored geometric characteristic is greater than a pre-defined limit value.
Device and method for detection of counterfeit pharmaceuticals and/or drug packaging	Analyze Features	Measure Features	US Department of Health and Human Services	US10101280	Active	3/31/09	3/31/30	HHS	Featured are a device (20) and method for the detection of counterfeit pharmaceuticals and/or packaging therefore. Counterfeit pharmaceuticals are detected by visual inspection upon exposing a suspected counterfeit pharmaceutical to one or more light sources having different wavelengths, and observing the differences in color and/or brightness between the suspected counterfeit and a genuine pharmaceutical/packaging. In further embodiments, a image acquisition device acquires an image showing color and/or other visual effect(s) brightness of the suspect counterfeit and this image is compared to an image of a authentic pharmaceutical/packaging.
Counterfeit detection system	Image Processing	Manipulating Digital Image	HP	US8798313	Active	7/9/09	7/14/30		A counterfeit detection system is disclosed herein. The system includes an image reduction system for minimizing size of at least one original image using a plurality of different reduction strategies to generate a plurality of minimized images. The system further includes a classification system which includes a first sub-system for generating at least one accuracy comparative assessment metric for each of the plurality of minimized images, a second sub-system for comparing the at least one accuracy comparative assessment metric for each of the plurality of minimized images with an accuracy assessment metric for the at least one original image, and a third sub-system for determining if at least one of the plurality of minimized images can be transmitted with improved or equivalent classification accuracy at a reduced bandwidth when compared to the original image are also part of the system.
System and method for physically detecting counterfeit electronics	Identification of Relevant Features	Fingerprint	Nokomis	US10475754	Active	3/2/11	12/10/35		A system for inspecting or screening electrically powered device includes a signal generator inputting a preselected signal into the electrically powered device. There is also an antenna array positioned at a pre-determined distance above the electrically powered device. Apparatus collects RF energy emitted by the electrically powered device in response to input of said preselected signal. The signature of the collected RF energy is compared with an RF energy signature of a genuine part. The comparison determines one of a genuine or a counterfeit condition of the electrically powered device.

Name	Type	Feature	Owner	Patent #	Status	Column1	Expiration	Gov't Funding	Abstract
Systems and methods for tracking and authenticating goods	Identification of Relevant Features	Fingerprint	Covectra Inc	US8908920	Active	6/23/11	6/31/2032		Systems and methods for identifying, tracking, tracing and determining the authenticity of a good are described herein. In some embodiments, a system includes an imaging system, a database, and an authentication center. The imaging system is configured to capture an image of a unique signature associated with a good at the good's origin. The unique signature can be, for example, a random structure or pattern unique to the particular good. The imaging system is configured to process the image of the good to identify at least one metric that distinguishes the unique signature from unique signatures of other goods. The database is configured to receive information related to the good and its unique signature from the imaging system; and is configured to store the information therein. The authentication center is configured to analyze the field image with respect to the information stored in the database to determine whether the unique signature in the field image is a match to the captured image stored in the database.
High Speed, Non-Destructive, Reel-to-Reel Chip/Device Inspection System and Method Utilizing Low Power X-rays/X-ray Fluorescence	Image Processing	Object Manipulation	Creative Electron Inc	US20130022167	Abandoned	7/22/11	1/1/13		A reel-like format for transporting devices under test (DUT) into low power x-ray inspection system allows for high speed transportation and inspection that is several orders of magnitude faster than conventional systems. The system can be configured with a conveyor belt for handling of non-reel suitable DUTs. A stabilizing control mechanism precisely and accurately brings the tape (with components) into the x-raying window, that allows spatial displacement of a portion of the to-be-viewed tape.
Object identification and inventory management	identification of Relevant Features	Fingerprint	Alitheon Inc	US9646206	Active	9/15/11	11/28/32		A method/apparatus for identifying an object based on a pattern of structural features located in a region of interest wherein the pattern of features comprises at least one fingerprint feature. The region may be recognized and used to identify the object. A first feature vector may be extracted from a first image of the pattern and may be mapped to an object identifier. To authenticate the object, a second feature vector may be extracted from a second image taken of the same region later in time than the first image. The two feature vectors may be compared and differences between one or more feature vector values determined. A match correlation value may be calculated based on the difference(s). The differences may be dampened if associated with expected wear and tear. Thus the impact on the match correlation value of such differences may be reduced. The differences may be enhanced if associated with changes that are not explainable as wear and tear. Thus the impact on the match correlation value of such differences may be increased.
Characterization of a physical item	Identification of Relevant Features	Texture	Chromologic	US10341555	Active	12/2/11	12/29/35	U.S. Army Research Office	The present invention is directed to a method and apparatus that involves improved characterization of an object based on its surface roughness and other unique features without having to necessarily define a fixed and predetermined region of interest. In accordance with one aspect, the present invention provides a method for characterizing an object based on a pattern of the object's surface roughness. The method comprises the steps of obtaining a unique image of a feature on the surface of the object, converting the image obtained into certain electrical signals and processing the electrical signals so they are associated with the object and thereby provide a characterization of the object that is used to generate a unique identifying signature for the object.
Pill identification and counterfeit detection method	Analyze Features	Measure Features	EyeNode LLC	US8712163	Active	2/14/12	12/14/32		Disclosed is a computer-implemented method of pill analysis including the steps of acquiring a pill image having an image frame and detecting contrast shifts within the image frame to locate at least one object with an object outline. A first value for the object(s) is determined, where the value is an area, a position, a length, a width, an angle, a color, a brightness, a code, a shape, a crystal pile size, a crystal geometry, a substance identity, or a character identity. Based on the first and second values, the computer outputs a result to a user.
Digital fingerprinting object authentication and anti-counterfeiting system	identification of Relevant Features	Fingerprint	Alitheon Inc	US9443298	Active	3/2/12	4/4/32		Improvements are disclosed for authentication of an object, verification of its provenance, and certification of the object as compliant with manufacturing standards. Or, an object may be reported as a suspected counterfeit. In one embodiment the system compares a digital fingerprint of the object, based in image capture, to digital fingerprints previously stored in a database and determines if the object has been registered before and is thus authentic. An object feature template may be created which has a list of features and attributes that are relevant for authenticating particular classes of objects. The object feature template can also be used to examine unregistered objects for signs of counterfeiting.
Photo forensics using image signatures	Analyze Features	Reference comparison	Truepic Analyze LLC	US9031329	Active	5/2/12	3/11/33		Evaluating an image is disclosed. A plurality of attributes of the image is analyzed. A determination is made that a portion of the attributes of the image imperfectly matches a reference attribute signature corresponding to a device. It is distinguished whether the imperfect match likely corresponds to a modification of the image.
Detecting defects on a wafer using defect-specific information	Identification of Relevant Features	Defect Detection	KLA Corp	US9721337	Active	10/15/12	10/15/32		Methods and systems for detecting defects on a wafer using defect-specific information are provided. One method includes acquiring information for a target on a wafer. The target includes a pattern of interest formed on the wafer and a known DOI occurring proximate to or in the pattern of interest. The information includes an image of the target on the wafer. The method also includes searching for target candidates on the wafer or another wafer. The target candidates include the pattern of interest. The target and target candidate locations are provided to defect detection. In addition, the method includes detecting the known DOI in the target candidates by identifying potential DOI locations in images of the target candidates and applying one or more detection parameters to images of the potential DOI locations.
Product, image, or document authentication, verification, and item identification	Analyze Features	Reference comparison	Authentiform LLC	US9053364	Active	10/30/12	10/30/33		The present disclosure provides methods, reagents, and apparatus for authenticating and identifying products. Methods of the disclosure are easy to implement but difficult to replicate, simulate, alter, transpose, or tamper with. In some embodiments, the present disclosure relates to a method of authenticating products using a product authentication code defined by a frequency array of a population of entities, and an item identifier defined by the specific manifestation of the product authentication code.

Name	Type	Feature	Owner	Patent #	Status	Column1	Expiration	Gov't Funding	Abstract
Method and apparatus for detection and identification of counterfeit and substandard electronics	Identification of Relevant Features	Fingerprint	Nokomis	US10571505	Active	3/6/13	3/6/34	United States Navy	An apparatus for detecting a condition or authenticity of one or more electronic devices includes an enclosure having an antenna integrated therewithin, a fixture mounted within a hollow interior of the enclosure, the fixture being configured to receive the one or more electronic devices and connect one or more signals to each of the one or more electronic devices and a sensor and controller assembly connected to the antenna and configured to process a signature of an emission of a radiofrequency (RF) energy from of one or more electronic devices having the one or more signals connected thereto.
Supervised autonomous robotic system for complex surface inspection and processing	Image Processing	Object Manipulation	Carnegie Mellon University	US9796089	Active	3/15/13	3/17/34	US Air Force and Army	The invention disclosed herein describes a supervised autonomy system designed to precisely model, inspect and process the surfaces of complex three-dimensional objects. The current application context for this system is laser coating removal of aircraft, but this invention is suitable for use in a wide variety of applications that require close, precise positioning and maneuvering of an inspection or processing tool over the entire surface of a physical object. For example, this system, in addition to laser coating removal, could also apply new coatings, perform fine-grained or gross inspection tasks, deliver and/or use manufacturing process tools or instruments, and/or verify the results of other manufacturing processes such as but not limited to welding, riveting, or the placement of various surface markings or fixtures
Apparatus and method for integrated circuit forensics	Image Processing	Machine Learning	US Secretary of Navy	US9885745	Active	6/24/13	9/25/13	United States Navy	A test system including an embodiment having a sensor array adapted to test one or more devices under test in learning modes as well as evaluation modes. An exemplary test system can collect a variety of test data as a part of a machine learning system associated with known-good samples. Data collected by the machine learning system can be used to calculate probabilities that devices under test in an evaluation mode meet a condition of interest based on multiple testing and sensor modalities. Learning phases or modes can be switched on before, during, or after evaluation mode sequencing to improve or adjust machine learning system capabilities to determine probabilities associated with different types of conditions of interest. Multiple permutations of probabilities can collectively be used to determine an overall probability of a condition of interest which has a variety of attributes.
System and method for counterfeit ic detection	Analyze Features	Reference comparison	IEC Electronics	US9646373	Active	9/7/13	11/26/34		A method for counterfeit IC detection includes: providing a computer, an optical and an X-ray imager; optically imaging a package of one or more ICs; pattern matching the package image to identify an IC type; selecting one or more reference images from a reference library; X-ray imaging one or more ICs; performing in any order: comparing an internal lead frame structure of the one or more ICs to images from the reference library to determine a first numerical indicator; and determining a composition of the lead frame of the one or more ICs and to a corresponding composition from the reference library to determine a second numerical indicator; calculating an indication of authenticity based on the first numerical indicator and the second numerical indicator; and accepting or rejecting the one or more ICs based on the indication of authenticity. A system for counterfeit IC detection is also described.
Counterfeit microelectronics detection based on capacitive and inductive signatures	Identification of Relevant Features	Fingerprint	US Secretary of Navy	US9959430	Active	2/5/14	6/20/36	United States Navy	Systems and methods for detecting counterfeit integrated circuits are provided. One exemplary embodiment of a method can include: providing an integrated circuit for testing; and characterizing capacitive and inductive loading of the integrated circuit power for a specified frequency range; wherein the characterizing step further comprises applying a low level alternating current to a power pin while measuring for capacitance characterization conditions created by the integrated circuit's internal capacitance and inductance responses, wherein by sweeping the alternating current signal across a specified frequency range one or more capacitance related device signature can be created and used to identify a component as originating from a trusted source or not. A system can include components and machine readable instructions for operating the components using exemplary methods. Exemplary embodiments can include automated systems that can also be used with the device signature on a production line or in a supply chain verification location.
System and method for authentication	Analyze Features	Reference comparison	ClearMark Systems LLC	US10127447	Active	3/12/14	3/12/35	Department of Energy	Described are methods and systems for determining authenticity. For example, the method may include providing an object of authentication, capturing characteristic data from the object of authentication, deriving authentication data from the characteristic data of the object of authentication, and comparing the authentication data with an electronic database comprising reference authentication data to provide an authenticity score for the object of authentication. The reference authentication data may correspond to one or more reference objects of authentication other than the object of authentication.
Image recognition device, image sensor, and image recognition method using feature	Identification of Relevant Features	Fingerprint	Omron Corp	US10055670	Active	3/14/14	5/31/34		An image recognition device includes an identification unit configured to compare a feature point in an input image and a feature point in every model image to compute a first degree of similarity between the input image and the model image, and to identify the input image on the basis of said first degree of similarity. To compute the first degree of similarity for a model image, the identification unit adds to a score based on a matching feature point for each feature point in the model image matching a feature point in the input image. The score based on the matching feature point is a value that increases as the number of model images including the matching feature point decreases.
Authenticating physical objects using machine learning from microscopic variations	Image Processing	Machine Learning	Entrupy Inc	US20170032285	Pending	4/9/14	1/1/17		A method for classifying a microscopic image includes receiving a training dataset (306) including at least one microscopic image (305) from a physical object (303) and an associated class definition (304) for the image that is based on a product specification. Machine learning classifiers are trained to classify the image into classes (308). The microscopic image (305) is used as a test input for the classifiers to classify the image into one or more classes based on the product specification. The product specification includes a name of a brand, a product line, or other details on a label of the physical object.

Name	Type	Feature	Owner	Patent #	Status	Column1	Expiration	Gov't Funding	Abstract
Non-contact electromagnetic illuminated detection of part anomalies for cyber physical security	Identification of Relevant Features	Fingerprint	Nokomis	US10149169	Active	6/9/14	4/23/35		An apparatus for testing, inspecting or screening an electronic device for electrical characteristics, modified or unmodified hardware, or firmware modifications including Malware, Trojans, improper versioning, and the like, includes a transmitting antenna positioned at a distance from the electronic device and a electromagnetic energy receiver or sensor for examining a resulting unintentional derived electromagnetic energy from the electronic device. The receiver collects unintentional RF energy components emitted by the device and includes a processor and executable instructions that perform analysis in a response to the acquired electromagnetic energy input. The characteristics of the collected RF energy may be compared with RF energy characteristics of an exemplary device. The analysis determines one of a modified, unmodified or score of certainty of discerned condition of the device.
Fibers with multicomponent fibers used for coding	identification of Relevant Features	Fingerprint	Eastman Chemical Co	US9972224	Active	6/27/14	3/24/36		Disclosed are fibers which contains identification fibers. The identification fibers can contain a plurality of distinct features, or taggants, which vary among the fibers and/or along the length of the identification fibers of the fibers, a fiber band, or. The disclosed embodiments also relate to the method for making and characterizing the fibers. Characterization of the fibers can include identifying distinct features, combinations of distinct features, and number of fibers with various combinations of distinct features to supply chain information. The supply chain information can be used to track the fibers, fiber band, or yarn from manufacturing through intermediaries, conversion to final product, and/or the consumer.
Determination method, determination system, determination device, and program	Analyze Features	Reference comparison	NEC	US20190279377	Pending	9/1/14	1/1/19		The present invention addresses the problem of providing a technique for determining the authenticity of a product without requiring a special device such as an integrated circuit (IC) tag. A means for solving this problem according to the invention is characterized by determining the authenticity of a target product on the basis of the validity of the association between the body of the product and a surface-treated component that is mounted to the body and that has been validated.
System and method for detecting the authenticity of products	identification of Relevant Features	Fingerprint	Guy Le Henaff	US20200065577	Pending	11/21/14	1/1/20		System and method for detecting the authenticity of products by detecting a unique chaotic signature. Photos of the products are taken at the plant and stored in a database/server. The server processes the images to detect for each authentic product a unique authentic signature which is the result of a manufacturing process, a process of nature etc. To detect whether the product is genuine or not at the store, the user/buyer may take a picture of the product and send it to the server (e.g. using an app installed on a portable device or the like). Upon receipt of the photo, the server may process the receive image in search for a pre-detected and/or pre-stored chaotic signature associated with an authentic product. The server may return a response to the user indicating the result of the search. A feedback mechanism may be included to guide the user to take a picture at a specific location of the product where the chaotic signature may exist.
Methods and systems for low-energy image classification	Analyze Features	Measure Features	Microsoft	US10055672	Active	3/11/15	6/21/35		Examples of the disclosure enable efficient processing of images. In some examples, one or more interest points are identified in an image. One or more features are extracted from the identified interest points using a filter module, a gradient module, a pool module, and/or a normalizer module. The extracted features are aggregated to generate one or more vectors. Based on the generated vectors, it is determined whether the extracted features satisfy a predetermined threshold. Based on the determination, the image is classified such that the image is configured to be processed based on the classification. Aspects of the disclosure facilitate conserving memory at a local device, reducing processor load or an amount of energy consumed at the local device, and/or reducing network bandwidth usage between the local device and the remote device.
Methods and arrangements for configuring industrial inspection systems	Image Processing	Object Manipulation	Digimarc	US10593007	Active	6/11/15	6/18/36		In computer vision systems that need to decode machine-readable indicia from captured imagery, it is critical to select imaging parameters (e.g., exposure interval, exposure aperture, camera gain, intensity and duration of supplemental illumination) that best allow detection of subtle features from imagery. In illustrative embodiments, a Shannon entropy metric or a KL divergence metric is used to guide selection of an optimal set of imaging parameters. In accordance with other aspects of the technology, different strategies identify which spatial locations within captured imagery should be successively examined for machine readable indicia, in order to have a greatest likelihood of success, within a smallest interval of time. A great variety of other features and arrangements are also detailed.
Method and system of using image capturing device for counterfeit article detection	identification of Relevant Features	Fingerprint	Datalogic	US9672678	Active	6/15/15	8/6/35		A device, system, and method of detecting counterfeit articles are provided. The method includes receiving article identifying information associated with a test article, using the article identifying information to retrieve an authentic article image associated with the test article from an image storage database, scanning the test article to capture one or more images of the test article under different wavelength illuminations, and displaying the one or more test article images and the authentic article image to allow comparison of the test article and the associated authentic article. Additionally, multiple wavelength emitting elements may be located within an image-capturing device, to provide alternate illuminations of the test article, allowing alternating capture of images highlighting different security features for providing a superimposed image. A system of counterfeit article detection is also provided.
On-chip aging sensor and counterfeit integrated circuit detection method	Identification of Relevant Features	Fingerprint	University of California	US10298236	Active	10/29/15	11/2/36		An on-chip aging sensor and associated methods for detecting counterfeit integrated circuits are shown. In one example, the on-chip aging sensor is integrated within a chip. In one example, the on-chip sensor includes both an on-chip age sensor, and an antifuse memory block including static information unique to the chip.

Name	Type	Feature	Owner	Patent #	Status	Column1	Expiration	Gov't Funding	Abstract
Method and Apparatus For Authentication of a 3D Structure	Identification of Relevant Features	Texture	ALPVISION SA	US20180268214	Pending	11/10/15	1/1/18		New authentication features are proposed that are visible, can be authenticated with a mobile equipment and yet are challenging to counterfeit. In a possible embodiment, the surface of the authentication feature may have three-dimensional characteristics, which can be recognized by a handheld camera, such as a smartphone camera, while it cannot be easily reproduced by a simple scan and print procedure. In a further possible embodiment, at least two different viewpoints of the authentication feature may be acquired using a smartphone camera and the resulting images may be analyzed using the smartphone processor to identify the three-dimensional characteristics of the authentication feature. The manufacturing of the feature may be performed at a low cost by embossing the three dimensional structure on a surface. The authentication feature may be carried by a self-adhesive label or directly embedded on the product packaging.
Methods and apparatuses for identifying anomaly within sealed packages using power signature analysis counterfeits	Identification of Relevant Features	Fingerprint	Power Fingerprinting Inc (PFP Cybersecurity)	US20170160320	Pending	12/2/15	1/1/17		Some embodiments described herein include an apparatus having a memory and a processor operatively coupled to the memory. The processor is configured to receive, in response to an excitation signal and from the power signature detector, a power signature signal associated with a target electronic device disposed within a sealed package. The processor is configured to extract a characteristic of the power signature signal and compare the characteristic of the power signature signal with a characteristic of a reference power signature signal associated with at least one reference device to determine a counterfeit status of the target electronic device. The at least one reference device is a pre-determined trusted device or a pre-determined counterfeit device. The processor is configured to send, to a communication interface, a notification signal associated with the counterfeit status of the target electronic device.
Detection of counterfeit electronic items	Analyze Features	Object Manipulation	Optimal Plus Ltd.	US9767459	Active	3/14/16	3/14/36		Disclosed are methods, systems and computer program products where an item may or may not be determined as counterfeit based on result(s) of a comparison between test data for the item, and test data for items that are associated with manufacturing data in the cluster that is most likely to include manufacturing data that is associated with attribute data obtained for the item. In some embodiments, such methods, systems and computer program products may allow automated, universal non-destructive, and/or non-invasive detection of counterfeit electronic items. In some embodiments, counterfeit detection may be integrated into existing supply chains, including high volume manufacturing supply chains, and may be performed for a large variety of items without a need for a major adjustment to manufacturing. However, the counterfeit detection in some embodiments may not necessarily be integrated into manufacturing and may occur at any time, even when an item is in use.
Avionics protection apparatus and method	Identification of Relevant Features	Fingerprint	Nokomis	US10235523	Active	5/10/16	8/31/36		An apparatus for a network of electrical and/or electronic devices coupled to a data bus comprises a sensor coupled to the data bus and configured to capture information content communicated through the data bus in a form of electromagnetic emissions being at least one of differential mode electromagnetic emissions, common mode electromagnetic emissions, coupled radiated electromagnetic emissions, and data bit streams; one or more processors or logic devices, and a non-transitory computational medium comprising executable instructions. The apparatus measure a feature value in at least one region of a time domain or a frequency domain of the captured electromagnetic emissions, calculates a difference value between the measured feature value and one or more baseline feature values, and determines, based on the calculated value, a presence or an absence of anomalies indicative of at least one of cyber intrusion attempt, cyber attack, cyber-physical attacks, malware, etc.
Controlled authentication of physical objects	identification of Relevant Features	Fingerprint	Alitheon Inc	US10614302	Active	5/26/16	11/7/37		A physical object is scanned and a digital image of the object is generated from the scan. At least one subset of the image, known as an “authentication region” is selected. A plurality of feature vectors, arising from the physical structure of the object, are extracted from certain locations of interest within an authentication region and combined to generate a unique identifier or “digital fingerprint” for that object. Preferably, authentication regions for feature vector extraction are automatically selected by a software process. To identify or authenticate an object, a system may compare a digital fingerprint of an object to digital fingerprints previously stored in a database. Digital fingerprint data may specify a set of features (also termed “locations of interest”) which may be referenced in the creation of a “fingerprint template” which is a template of certain locations of interest and/or attributes selected for authenticating a particular class of objects.
Automated model-based inspection system for screening electronic components	Image Processing	Machine Learning	Raytheon	US10586318	Active	10/17/16	4/4/37		A method includes obtaining data associated with an electronic component. The method also includes conducting a multi-tier inspection process to verify a conformance of the electronic component. Each of the tiers includes a different type of identification test, and at least one of the tiers is configured to provide fuzzy outputs. The method further includes analyzing the data associated with the electronic component using one or more first tests associated with a first of the tiers to determine whether the electronic component conforms to a pre-specified requirement. In addition, the method includes generating an output based on the analysis and determining whether additional testing is required using one or more next-level tests associated with another of the tiers.
Detection of counterfeit and compromised devices using system and function call tracing techniques	Identification of Relevant Features	Fingerprint	Florida International University	US10027697	Active	4/28/17	4/28/37	Department of Energy	Frameworks, methods, and systems for securing a smart grid are provided. A framework can include data collection, call tracing techniques, and preparing call lists to detect counterfeit or compromised devices. The call tracing techniques can include call tracing and compiling all system and function calls over a time interval. The framework can further include data processing, in which a genuine device is identified and compared to unknown devices. A first statistical correlation can be used for resource-rich systems, and a second statistical correlation can be used for resource-limited systems. Threats of information leakage, measurement poisoning and store-and-send-later can be considered.

Name	Type	Feature	Owner	Patent #	Status	Column1	Expiration	Gov't Funding	Abstract
Counterfeit integrated circuit detection by comparing integrated circuit signature to reference signature	Identification of Relevant Features	Fingerprint	Global Circuit Innovations Inc	US10460326	Active	10/24/17	2/23/38		A method is provided. The method includes connecting an integrated circuit to a curve tracer, displaying a device signature corresponding to the integrated circuit on a screen of the curve tracer, and comparing the device signature to a reference signature to determine if the integrated circuit is counterfeit.
Method and System to Automatically Inspect Parts Using X-Rays	Image Processing	Machine Learning	Guilherme Cardoso (Creative Electron)	US20190219525	Pending	1/16/18	1/1/19		A system and method for automating programming of an industrial use x-ray inspection machine, utilizing an artificial intelligence (AI) engine in both a navigator level and planner level stage of an x-ray parts inspection machine, the AI engine performing at least one of identifying and classifying a sample, assessing location(s) to be inspected on the sample, and implementing a test criteria for each assessed location on the sample. The AI engine removes the typical interactions and setup procedures performed by the machine operator, thus enabling a higher degree of system automation and accuracy.
Systems and methods for enhancing machine vision object recognition through accumulated classifications	Image Processing	Machine Learning	Capital One Services LLC	US20190279329	Pending	3/2/18	1/1/19		The disclosed technology includes systems and methods for enhancing machine vision object recognition based on a plurality of captured images and an accumulation of corresponding classification analysis scores. A method is provided for capturing, with a camera of a mobile computing device, a plurality of images, each image of the plurality of images comprising a first object. The method includes processing, with a classification module comprising a trained neural network processing engine, at least a portion of the plurality of images. The method includes generating, with the classification module and based on the processing, one or more object classification scores associated with the first object. The method includes accumulating, with an accumulating module, the one or more object classification scores. And responsive to a timeout or an accumulated score exceeding a predetermined threshold, the method includes outputting classification information of the first object.
System and method to protect items associated with additive manufacturing	Identification of Relevant Features	Texture	General Electric Co	US20190286102	Pending	3/16/18	1/1/19		According to some embodiments, a lossless protection procedure may be applied to control distribution of a print geometry of an industrial asset item. For example, an item definition data store may contain electronic records defining a geometry of the industrial asset item. A signature identifier encoder platform may determine a unique signature identifier associated with the industrial asset item and modify the geometry of the industrial asset item to encode therein information about the unique signature identifier. In some cases, for example, this may be done by adjusting a scanning pattern of a fill region (e.g., stripe, checkerboard, etc.) or a support structure of the industrial asset item. An authentication platform may then receive, from a sensor (e.g., an X-ray), a measured characteristic parameter of an item to be authenticated and determine a signature identifier of the item (which can be used to authenticate the item).
Systems and methods to prevent counterfeiting	Identification of Relevant Features	Fingerprint	Avery Dennison	WO2020028288	Pending	7/31/18	1/1/20		System and method for using one or more entropically configured distinct physical features (a "IDENTROPY") for establishing trust, accountability, and transparency with respect to physical items are disclosed. Such system and method are useful, among other things, for detecting counterfeit physical items.
IC device authentication using energy characterization	Analyze Features	Measure Features	SAIC	US10585139	Active	2/14/19	2/14/39	Defense Ordnance Technology Consortium	Systems, methods, and apparatuses are described for verifying the authenticity of an integrated circuit device. An integrated test apparatus may use quiescent current and/or conducted electromagnetic interference readings to determine if a device under test matches the characteristics of an authenticated device. Deviations from the characteristics of the authenticated device may be indicative of a counterfeit device.
Artificial intelligence based monitoring of solid state drives and dual in-line memory modules	Image Processing	Machine Learning	Intel	US20190189236	Pending	2/21/19			In embodiments, a memory controller (MC) includes an output interface, and an execution engine (EE) to identify, based on field test results of a die coupled to the MC, initial test results of the die using an artificial neural network (ANN) trained to identify the die from a set of NVM dies based on initial test results of the set of NVM dies obtained at a time of manufacture of the set of dies. The initial test results include a first useful life prediction and the field test results include a second useful life prediction, and the initial test results are regenerated by the ANN to protect their confidentiality. In embodiments, the MC is further to compare the second useful life prediction with the first useful life prediction, to determine a deviation between the two, and output, via the output interface, the deviation to a user.
Integrated circuit with electromagnetic energy anomaly detection and processing	Identification of Relevant Features	Defect Detection	Nokomis	US9059189	Active	3/2/11	11/4/32		An integrated circuit includes an antenna, a die manufactured from a semiconducting material, an RF energy collection and processing device disposed on or within the die and including at least a receiver and a processing device, an input configured to supply power to said RF energy collection and processing device and an output for operative communication by said RF energy collection and processing device. The integrated circuit is configurable and operable to provide at least one of electromagnetic emission anomaly detection, tamper detection, anti-tamper monitoring, degradation monitoring, health monitoring, counterfeit detection, software changes monitoring, firmware changes monitoring and monitoring of other RF energy anomalies.
Scanning method for screening of electronic devices	Analyze Features	Measure Features	NTES of Sandia	US10094874	Active	12/1/11	10/18/32	Department of Energy	A visualization method for screening electronic devices is provided. In accordance with the disclosed method, a probe is applied to a grid of multiple points on the circuit, and an output produced by the circuit in response to the stimulus waveform is monitored for each of multiple grid points where the probe is applied. A power spectrum analysis (PSA) produces a power spectrum amplitude, in each of one or more frequency bins, on the monitored output for each of the multiple grid points. The PSA provides a respective pixel value for each of the multiple grid points. An image is displayed, in which image portions representing the multiple grid points are displayed with the respective pixel values.

Name	Type	Feature	Owner	Patent #	Status	Column1	Expiration	Gov't Funding	Abstract
Defect screening method for electronic circuits and circuit components using power spectrum anaylysis	Identification of Relevant Features	Defect Detection	NTES of Sandia	US10145894	Active	12/1/11	11/24/32	Department of Energy	A method involving the non-destructive testing of a sample electrical or electronic device is provided. The method includes measuring a power spectrum of the device and performing a Principal Component Analysis on the power spectrum, thereby to obtain a set of principal components of the power spectrum. The method further includes selecting a subset consisting of some of the principal components, and comparing the subset to stored reference data that include representations in terms of principal components of one or more reference populations of devices. Based at least partly on the comparison, the sample device is classified relative to the reference populations.
Digital fingerprinting track and trace system	Identification of Relevant Features	Fingerprint	Alitheon Inc	US9582714	Active	3/2/11	3/2/32		Methods and systems for tracking a physical object to identify or authenticate it utilizing digital fingerprints which are based on natural features extracted from a digital image of the object. Digital fingerprints do not require or rely on any labels, tags, integrated materials, unique identification characters, codes or other items that may be added to the object specifically for the purpose of identification. Consequently, the disclosed digital fingerprint techniques help to detect or prevent unauthorized alterations of documents, apparel, drugs and pharmaceuticals, etc. Further digital fingerprints can be used to better track and trace a wide variety of objects throughout the distribution chain to demonstrate their provenance and to detect counterfeit objects.
Authentication-based tracking	Identification of Relevant Features	Fingerprint	Alitheon Inc	US20180053312	Pending	8/1/16			Methods and systems integrate digital fingerprint authentication-based identification and location tracking into a single, continuous process in which an authentication-integrated tracking system is simultaneously aware of both the identity and location of each physical object at all times as they move along a conveyance system. Insertion or removal of an object is quickly detected and reported. Rapid reestablishment and continuation of authentication-integrated tracking is enabled in the event of any temporary interruption or failure of tracking in the system. An exemplary system comprises plural tracking units networked together, each tracking unit including a camera or scanner to observe a corresponding field of view, the tracking units arrange to realize a continuous field of view of a physical conveyance system.
Multi-level authentication	Identification of Relevant Features	Fingerprint	Alitheon Inc	US10621594	Active	2/19/16	7/7/38		Apparatuses and methods associated with multi-level authentication are disclosed herein. In embodiments, a method includes authenticating a physical object of a plurality of physical objects that together form an aggregate physical object; storing in a database system relationship information reflecting a relationship between the aggregate physical object and the plurality of physical objects; attempting to authenticate a target physical object; responsive to matching the target physical object to the aggregate physical object based on the attempt to authenticate the physical target: identifying in the database system a database record corresponding to the aggregate physical object; storing in the database record authentication data reflecting the match between the target physical object and the aggregate physical object; and storing an indication of a re-authentication of the physical object in the database system based on the relationship information. Other embodiments may be disclosed or claimed.
Deterrence of device counterfeiting, cloning, and subversion by substitution using hardware fingerprinting	Analyze Features	Reference comparison	NTES of Sandia	US8848905	Active	7/28/10	9/14/32		Deterrence of device subversion by substitution may be achieved by including a cryptographic fingerprint unit within a computing device for authenticating a hardware platform of the computing device. The cryptographic fingerprint unit includes a physically unclonable function ("PUF") circuit disposed in or on the hardware platform. The PUF circuit is used to generate a PUF value. A key generator is coupled to generate a private key and a public key based on the PUF value while a decryptor is coupled to receive an authentication challenge posed to the computing device and encrypted with the public key and coupled to output a response to the authentication challenge decrypted with the private key.
Electronic component classification	Identification of Relevant Features	Fingerprint	Battelle Memorial Institute	US10054624	Active	12/13/13	12/12/34		A system and method of electronic component authentication or component classification can reduce the vulnerability of systems (e.g., satellites, weapons, critical infrastructure, aerospace, automotive, medical systems) to counterfeits. Intrinsic deterministically random property data can be obtained from a set of authentic electronic components, processed, and clustered to create a classifier that can distinguish whether an unknown electronic component is authentic or counterfeit.

Appendix 21.

Master List of Contacts with Expertise Related to Counterfeit Parts

Preface:

This is a list of contacts in government, industry, academia, and elsewhere of individuals with expertise in the field of counterfeit electronics.

Standards Organizations, Conferences, and Other Organized Groups

There are a number of organizations, conferences, and working groups whose membership and attendance rosters would provide a much more exhaustive source of contact information. Their rosters are not reproduced here in order to avoid the violation of trust given to their members.

- SAE G-19 Committee (including G-19A, G-19D, and G-19CI)
  - Counterfeit Electronic Components Committee
  - Chartered to address aspects of preventing, detecting, responding to and counteracting the threat of counterfeit electronic components.
    - G-19A Test Laboratory Standards Development Committee
    - G-19AD Authorized Distributor
    - G-19C Standard Compliance Verification
    - G-19CI Continuous Improvement
    - G-19D Distributor
    - G-19DR Distributor Risk Characterization
    - G-19T Terms and Definitions
- SAE G-21 Committee
  - Counterfeit Materiel Committee
  - Chartered to address aspects of preventing, detecting, responding to and counteracting the threat of counterfeit materiel.
    - G-21B Counterfeit and Substandard Battery Risk Mitigation
    - G-21R Counterfeit Refrigerants
- SAE G-32 Committee
  - Cyber Physical Systems Security (CPSS) Committee
  - Chartered to further CPSS, including analyses of the system operating environment defined by the operational, functional, and architectural systems engineering elements.
- SMTA-CALCE Symposium on Counterfeit Parts and Materials
  - Providing a forum to cover all aspects of changes in the electronic parts supply chain on how an organization performs part selection and management through whole life cycle of the parts.
- Counterfeit Microelectronics Working Group,
  - National IPR Coordination Center/DOJ
- GOMACTech (Government Microcircuit Applications & Critical Technology Conference)
  - Conference focuses on advances in systems being developed by the Department of Defense and other government agencies.
- DMSMS (Diminishing Manufacturing Sources and Material Shortages)
  - Focusing on DoD DMSMS issues resulting from, the loss, or impending loss, of manufacturers or suppliers of items, raw materials, software or parts obsolescence.

- HOST (IEEE International Symposium on Hardware Oriented Security and Trust)
  - An event for researchers and practitioners to advance knowledge and technologies related to hardware security and assurance.
- CMSE (Components for Military & Space Electronics)
  - An event focused on the design, reliability, and application of electronic components for use in avionics aerospace, military & commercial space systems.
- Various DoD Working Groups:
  - Joint Federated Assurance Center (JFAC)
    - Promotes and enables software assurance (SwA) and hardware assurance (HwA).
  - ASSESS Working Group
  - Counterfeit Risk Management (CRM)
    - Army Materiel Command Industrial Base
      - Coordinates a counterfeit avoidance effort for Army system engineers.
      - Provides a website containing counterfeit prevention materials across services.
      - DoD Integrated Project Team (IPT) includes participants from across DoD.
  - Joint Artificial Intelligence Center (JAIC)
    - To help operationally prepare the DoD for AI, the JAIC integrates technology development, with the requisite policies, knowledge, processes and relationships to ensure long term success and scalability.
  - Navy - Trusted PCB (Printed Circuit Board)
    - Remains one of the only truly trusted sources for printed circuit boards in the DoD supply chain.
  - Air Force - AFWERKS Supply Chain
    - Encourages a community of intrapreneurs, industry, academia, and non-traditional contributors to develop innovative approaches to protect the supply chain.

Alphabetical List of Subject Matter Experts

Angelle, Joy
Industry
joy.angelle@aerocyonics.com,
401-365-6100 Ext. 1003
Aerocyonics, Inc.

Arno, Sally
Industry
sally@freedomsales.com
Director of Quality, Freedom Sales

Azarian, Michael
Academia
mazarian@umd.edu
(301) 405-5323
Center for Advanced Life Cycle Engineering (CALCE)
Univ. of Maryland College Park
Chair, SAE G-19A, Test Laboratory Standards Development Committee

Baker, Don
Industry
dbaker@ctrends.com
CEO and Founder, CTrends, Inc.
Executive Board Member of IDEA

Baldwin, Kristen
Department of Defense
Deputy Director for Strategic Technology Protection and Exploitation

Berger, Glenn
Department of Defense
glenn.a.berger@navy.mil,
(812) 854-8549
Division Chief Engineer of the Trusted Microelectronics Division
Microelectronics Design Chief Engineer
Naval Surface Warfare Center, Crane Division, (NSWC Crane)

Bodemuller, Robert
Industry
Robert.a.Bodemuller@lmco.com,
(972) 603-0033
Lockheed Martin Missiles and Fire Control

Bogert, Gerald
Industry
gerald.bogert.contractor@unnpp.gov
Bechtel Plant Machinery Inc.

Bramschreiber, Kelsey
Department of Defense
Kelsey.bramschreiber@navy.mil
Leader of JFAC Hardware Assurance Technical Working Group,
Naval Surface Warfare Center, Crane Division, (NSWC Crane)

Calvete, Thomas
Industry
tcalvete@harris.com
Component Engineer, Harris Corporation

Campbell, Patricia
Academia
pcampbell@law.umaryland.edu
(410) 706-2569
Law School Professor
Director, Intellectual Property Law Program
Director, Maryland Intellectual Property Legal Resource Center
University of Maryland Carey School of Law

Cardoso, Bill
Industry
bcardoso@creativeelectron.com
CEO, Creative Electron, Inc

Church, Jeff
Department of Defense
jeff.t.church.civ@mail.mil,
(804) 734-2425
Defense Contract Management Agency

Cohen, Brian
Independent Contractor
brianscohen@cybertechsol.net
CyberTech Solutions, LLC.
formerly IDA

Coleman, Dave
Industry
David.Coleman@elbitsystems-us.com
(817) 234-6615
Elbit Systems of America

Das, Diganta
Academia
diganta@umd.edu
(301) 405-5323
Center for Advanced Life Cycle Engineering (CALCE)
Univ. of Maryland College Park
Technical Committee Chair, *SMTA-CALCE Symposium on Counterfeit Parts and Materials*
SAE G-19A, Assembly Subgroup Chair

Deisz, Daniel
Industry
ddeisz@rocelec.com
Director of Design Technology, Rochester Electronics

Dimase, Dan
Industry
daniel.dimase@aerocyonics.com
CEO, Aerocyonics, Inc.
Former Chair, SAE G-19A, Test Laboratory Standards Development Committee

Farragher, Jeff
Department of Homeland Security
Jeffrey.R.Farragher@ice.dhs.gov
Homeland Security Investigation

Franklin, Eustice
Department of Defense
efranklin@gidep.org
Government-Industry Data Exchange Program

George, Paula
Department of Defense
Paula.George@dla.mil
Defense Logistics Agency

Gray, Robin
Industry
rgray@ecianow.org
Chief Operating Officer and General Counsel,
Electronic Components Industry Association

Guin, Ujjwal
Academia
Ujjwal.guin@auburn.edu
(334) 844-1835
Department of Electrical and Computer Engineering
Auburn University

Hallman, Jeff
Academia
Jeff.Hallman@gtri.gatech.edu
Principal Research Engineer
Georgia Tech Research Institute - GTRI

Hamako, Kevin
Department of Homeland Security
Kevin.M.Hamako@ice.dhs.gov
U.S. Department of Homeland Security, Special Agent, Commercial Trade Fraud / IPR

Hammond, Robb
Industry
Robb.Hammond@aeri.com
President and CEO, AERI

Hauch, Adam
Department of Defense
adam.hauch@dss.mil
Defense Intelligence Agency
Trusted and Assured Microelectronics

Heebink, Joel
Industry
joel.heebink@honeywell.com
Program Manager for Counterfeit Prevention, Honeywell International Inc.

Hilaro, Julie
Department of Homeland Security
julie.e.hilario@ice.dhs.gov
Current lead (assumed), Counterfeit Microelectronics Working Group

Hoover, Eric
Department of Defense
eric.d.hoover2.civ@mail.mil
Army Materiel Command Industrial Base

Hughitt, Brian
National Aeronautics and Space Administration
brian.hughitt-1@nasa.gov
Technical Fellow, Quality Engineering, retired

Jackson, Lamar
Department of Homeland Security
Lamar.A.Jackson@ice.dhs.gov
Supervisory Special Agent, US Department of Homeland Security

Johnson, Karen
Industry
kdjohnso@ida.org
Institute for Defense Analyses

Khan, Faiza
Industry
fkhan@idofea.org
Executive Director, Independent Distributors of Electronics Association (IDEA)

Koepsel, Kirsten
Independent Contractor
kirstenpatents@mac.com
formerly AIA
Co-chair, SAE G-19D, Distributor Committee

Lilani, Sultan Ali
Industry
Sultan.Lilani@integra-tech.com
Director, Technical Sales Support, Integra Technologies
Former Co-Chair, SAE G-19A, Test Laboratory Standards Development Committee

Linderman, Eric
Department of Defense
eric.w.linderman.civ@mail.mil
Office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology(ASA (ALT))

Livingston, Henry
Industry
henry.c.livingston@baesystems.com
Technical Director and BAE Systems Engineering Fellow at BAE Systems

Maestas, Lisa
Industry
lisam@ti.com
Director Central Quality Services & Ant-Counterfeit Program,
Texas Instruments

Mantese, Joseph
Industry
mantesjv@utrc.utc.com
United Technologies Research Center

Martell, Steven
Industry
steven.martell@nordsonsonoscan.com
Manager Technical Support Services, Nordson Sonoscan
Vice-Chair, SAE G-19A, Test Laboratory Standards Development Committee

Martinez, Gerald
National Aeronautics and Space Administration
gerald.m.martinez@jpl.nasa.gov
Jet Propulsion Laboratory

Meshel, David
Industry
David.C.Meshel@aero.org
Branch Chief Mission Assurance, Aerospace Corporation.

Olney, Andrew
Industry
Andrew.Olney@analog.com
Director of Quality at Analog Devices
Former head of SIA anticounterfeiting group

Ott, Richard
Department of Defense
richard.ott.3@us.af.mil
(937) 713-8979
Validation and Verification Lead
JFAC ASSESS Working Group Lead
Air Force Research Lab

Panaguiton, Peter
Department of Defense
ppanaguiton@gidep.org
(951) 262-7277 Ext. 239
Government-Industry Data Exchange Program

Pecht, Michael
Academia
pecht@umd.edu
(301) 405-5323
Director, Center for Advanced Life Cycle Engineering (CALCE),
Univ. of Maryland College Park

Poncheri, Anne
Industry
aponcheri@resion.com
Resion LLC., InterCEPT

Popick, Paul R.
Independent Contractor
paul.popick@incose.org
formerly Johns Hopkins University APL

Reed, Melinda
Department of Defense
melinda.k.reed4.civ@mail.mil
Director for Resilient Systems in the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) Office of Strategic Technology Protection and Exploitation (STP &E)
formerly Office of the Deputy Assistant Secretary of Defense for Systems Engineering

Resler, Brian J.
Department of Justice
brian.resler2@usdoj.gov,
(202) 616-3298
Assistant Deputy Chief for Litigation, Computer Crime and Intellectual Property Section, U.S. Department of Justice

Richard, Stephen
Department of Defense
stephen.p.richard4.civ@mail.mil,
309-782-0899
Army Materiel Command Industrial Base

Schipp, Fred
Department of Defense
frederick.schipp@navy.mil
812-854-5848,
NSWC Crane

Scofield, William
Industry
william.h.scofield@boeing.com
Engineer at The Boeing Company

Sharpe, Thomas
Industry
tsharpe@smtcorp.com
(203) 270-4705
Vice President, SMT Corp.

Sink, Kevin
Industry
Kevin.Sink@ttiinc.com
Director of Total Quality, TTI Inc.

Smith, Kebharu
Department of Justice
Kebharu.Smith@crm.usdoj.gov
Senior Trial Attorney, Computer Crime and Intellectual Property Section

Smith, Richard
Industry
rsmith@erai.com
Vice President, Business Development, ERAI

Snider, Kristal
Industry
ERAI
ksnider@erai.com
(239) 261-6268
Vice President, Founder

Snider, Mark
Industry
ERAI
mark@erai.com
(239) 261-6268
President, Founder

Sood, Bhanu
National Aeronautics and Space Administration
Bhanu.Sood@Nasa.Gov
NASA Goddard Space Flight Center
SAE G-19A, DDPA and Defect Taxonomy Subgroup Chair

Tehranipoor, Mohammad
Academia
tehranipoor@ece.ufl.edu
Chair Professor in Cybersecurity at the Department of Electrical and Computer Engineering, the University of Florida
Co-founder, IEEE Int. Symposium on Hardware-Oriented Security and Trust (HOST)

Tipton, Robert
Industry
bobtipton99@aol.com
Wyle (may have retired)

Tsang, Jenny
Department of Homeland Security
JENNY.U.TSANG@cbp.dhs.gov
US Customs and Border Protection Laboratory, Asst Director.

Zulueta, Phil
Academia
phillipzulueta@gmail.com
Independent contractor, formerly JPL