Final Report: Machine Vision Pilot (MVP) and Microelectronic Authenticity and Security, Evaluation and Research (MASER)

Section 843 Machine Vision Pilot Program Report Generation and Policy Analysis (MVP)

DMEA Project Engineer: Jeff Carlile, DMEA

Microelectronic Authenticity and Security, Evaluation and Research (MASER)

DMEA Project Engineer: Jeff Carlile, DMEA

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**

Original Submission: November 30, 2020
Revised: December 30, 2020

Project Team

Defense Microelectronics Activity:

Mr. Jeff Carlile, Mr. Michael Sutherland, Mr. Daric Matthew Guimary, Mr. Phil Comer, Mr. Aaron Schaal, Mr. Kevin Hartmann, Mr. Isaac Fields, Mr. Jamesson Kaupanger

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

Contributors from SMT Corp.:

Mr. Tom Sharpe

I. Executive Summary

Section 843 of the 2018 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 2018 NDAA §843. DMEA contracted the Center for Advanced Life Cycle Engineering (CALCE) at the University of Maryland at College Park to execute the pilot program under both contracts.

The stated purpose of the pilot program was to test the feasibility and reliability of using machine-vision technologies to determine the authenticity and security of microelectronic parts in weapon systems. The primary focus of the project is the prevention and detection of counterfeit microelectronics from entering the supply chain. For the purposes of this effort, the term "Machine Vision" was defined as systems which detect signals within the electromagnetic (EM) spectrum, not only the frequencies visible to the human eye. Systems which rely on image comparison are referred to as "Image Analysis" within this effort. The program included an evaluation of two types of Machine Vision: Image Analysis, and Side Channel, and included conventional standards-based testing methods as applied to counterfeit microelectronics detection. It provided quantitative data on their effectiveness, as well as recommendations for suggested improvements to counterfeit detection methods. It included Technology Readiness Level (TRL) assessments to identify promising counterfeit detection methods that can be implemented successfully and quickly.

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.

A. Assessment of Machine Vision and related technologies for counterfeit detection and prevention

Through an assessment of the key Image Analysis (IA) and related Side Channel (SC) technologies for counterfeit detection and prevention it was found that some IA and SC technologies have shown promise. **However, in their current stage of development, Machine Vision technologies do not provide satisfactory solutions for counterfeit prevention and detection in the real-world environment (TRL 7), despite demonstrating promising results in controlled laboratory environments (TRL 4). Standards-based Conventional Testing remains the most effective form of counterfeit detection, but is time consuming. Applying Machine Vision technologies can add additional layers of risk mitigation, but no "silver bullet" currently exists to mitigate the threat of counterfeit microelectronics. Careful source selection and the application of Standards-based Conventional Testing, commensurate with the appropriate level of risk mitigation for the application, remains the industry best practice.**

Table 1: Review of Technology Readiness Level (TRL) Scale

TRL	Description
1	Basic principles observed and reported
2	Technology concept and/or application formulated
3	Analytical and experimental critical function and/or characteristic proof of concept
4	Component and/or breadboard validation in a laboratory environment
5	Component and/or breadboard validation in a relevant environment
6	System/subsystem model or prototype demonstration in a relevant environment
7	System prototype demonstration in an operational environment
8	Actual system completed and qualified through test and demonstration
9	Actual system proven through successful mission operations

Assessments of Side Channel technologies show that none have achieved a complete TRL above 5 for counterfeit detection, although some components of the systems were at a higher TRL. The companies' TRLs show that their technologies are still in an intermediate state of development. A further consideration involves the ability of companies to sustain themselves financially through the sale of products and services for counterfeit prevention. Without a robust market, customers who invest in a technology may find that

their suppliers are not willing to provide continued support over a period of several decades. This threatens their viability as long-term solutions for securing the supply chain. The Side Channel technologies should be developed for applications beyond exclusively defense microelectronics needs in order to expand and diversify demand for their products and services.

Machine Vision technologies can deliver authentication of individual parts without contact with or modification of the part. The highest TRL achieved by the Machine Vision technologies assessed was 6. They may also satisfy, at least in part, the item unique identification (IUID) requirement in DODI 5200.44, if they were fully implemented. Similar to Side Channel technologies, these companies will likely need to expand their market beyond DoD in order to grow.

If successful, these technology companies will be responsible for managing sensitive data with both national security and business implications for their customers. Threats to data integrity include the injection of spurious data, swapping of data, or mislabeling. Demonstrated methods to detect and eliminate intrusions and the ability to restore original data are essential. DoD needs to evaluate the cybersecurity capabilities of these companies before making any final choice of technology.

A demonstration of the known-good virtual golden samples concept using the Battelle Barricade system highlighted the criticality of configuration control and the maintenance of backward compatibility in systems that must remain available over the sustainment period of long life cycle programs. The Alitheon FeaturePrint system has several attractive attributes concerning its potential use for part authentication, but a number of technical and business issues need to be resolved before it should be considered ready for implementation across the DoD supply chain.

CALCE found Battelle, among the Side Channel companies, and Alitheon, among the Image Analysis companies, to have the greatest overall capability to respond to requests for part evaluation and authentication and deliver useful results in a timely manner.

The results of the Blind Study revealed that standards-based Conventional Testing is consistently accurate, though time consuming, in the detection of variations between authentic and counterfeit parts, and demonstrated the ability to determine which parts were counterfeit in the absence of an exemplar, based on detection of physical defects.

1. **The findings of the Blind Study support the recommendation that DoD should continue to rely upon standards-based testing for counterfeit detection.**
2. **The DoD should take a more active role in standards organizations that are developing anti-counterfeit standards, for both awareness within DoD as well as influencing development of standards in a way that addresses DoD's needs.**

3. **A training program on anti-counterfeit measures and supply chain security should be required for all program managers, contract officers, purchasing, maintenance, and sustainment personnel.**

As indicated by Table 2, Image Analysis and related Side Channel methods varied in accuracy but each included technologies that performed to 99% accuracy or above in their ability to discriminate between counterfeit and authentic, or to match previously registered parts specifically.

1. Short term recommendations:

The following efforts should be undertaken by the DoD as short-term investments and development efforts to develop Image Analysis and related Side Channel technologies for more effective anti-counterfeit applications. Please refer to Section V: Task 2: Evaluation of Existing Machine-Vision and AI Technologies for specific details.

1. Correlation of Image Analysis and Side Channel results with physical defects on the components
2. Development of assembly-level (PCB-level) applications of Machine Vision
3. Iteration of the Blind Study with separate homogeneous lots, or mixed lots of varying heterogeneity, and larger sample size
4. Analysis of Battelle Barricade data reference samples
5. Authentication study with more aggressive physical damage to part surfaces following registration
6. Follow-up TRL Assessments by the same team after achievement of new development milestones
7. Analysis of defects from conventional testing Blind Study to determine the consistency and effectiveness of each test method for different part types
8. Exploration of thermal methods for counterfeit detection

2. Long-term recommendations:

The following technology development concepts are also recommended for investigation and investment to improve the security of the DoD supply chain. Please refer to Section VI: Task 3: Evaluation and Development of Solutions for the Microelectronics Supply Chain for Possible Implementation by Program Managers for specific details.

1. Development of classification process for registration based systems
2. Development of defect detection capabilities using Machine Vision systems to make them compatible with standards-based testing, improve interpretability, and reduce false positives
3. Improvement of throughput for Machine Vision technologies
4. Adaptation of Machine Vision technologies from other domains

5. Identification of new technologies from other fields for securing the supply chain
6. Application of the methods used in this study to a hardware assurance study with a focus on FPGAs and tampered parts
7. Application of the methods used in this study to evaluate techniques for counterfeit materiel detection and prevention, including batteries
8. Reduction of false positives through the determination of requirements for appropriate exemplars
9. Investigation of thermal signature-based counterfeit detection methods

Awareness of counterfeit prevention policies and standards throughout DoD should be improved.

B. 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 Cost Accounting Standards (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 are 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.

1. Policy Recommendations:

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

1. 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.

2. A uniform, DoD-wide set of policies and procedures to address prevention, detection, and avoidance of counterfeiting is needed.
3. 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.
4. 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.
5. DoD should require compliance with the SAE AS6171 standards for risk-based testing to determine authenticity and reliability of electronic parts.
6. 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 Simplified Acquisition Threshold (SAT). The reporting window should be shortened, and contractors should be provided with guidance about the safe harbor for reports submitted in good faith.
7. 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.
8. Further evaluation of the civil and criminal trademark laws should be conducted to consider whether additional remedies and/or enhanced enforcement is needed.
9. 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.
10. 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.

11. 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?

C. Adoption of Machine Vision Technologies to Evaluate the Authenticity and Security of Microelectronic Parts

Machine Vision technologies offer the possibility of improved speed, accuracy, and repeatability over manual inspection of counterfeit electronic parts for detection of defects or authentication. Current regulations do not exclude the possible use of Machine Vision technologies to screen for counterfeit parts. However, Machine Vision cannot satisfy the requirements for detailed external visual inspection ("EVI") of electronic parts indicated by industry standards. As those standards are currently constituted, Machine Vision also does not satisfy the narrow requirement of general EVI. Further, substantial questions exist about how Machine Vision might be implemented and whether there are compelling business reasons for use of Machine Vision technologies by the defense industry.

In order for Machine Vision to be implemented in counterfeit detection and authentication of electronic parts, the DoD must do the following:

1. Machine Vision technologies should be developed further to comply with industry standards on general external visual inspection of electronic parts.
2. The DoD needs to develop a better understanding of the costs and benefits of Machine Vision and how it can best be implemented.
3. The DoD needs to develop a strong business case for adoption of Machine Vision technologies by the defense industry.
4. Consideration should be given to the costs of adopting Machine Vision technologies, including capital investments, administrative overhead, security, and potential licensing costs.

Table 2: TRL Summary and Clustering Accuracy for Machine Vision Systems Evaluated

Company	Critical Technology Element	Focus of Assessment	TRL Complete (Partial)	Clustering Accuracy	Comments
Alitheon (IA)	The process of generating FeaturePrint	Software	6 – (up to 9)	0.99	Matched phase 1 registered serial numbers to phase 2 serial numbers.
Covisus (IA)	Covisus vTag scanner/DTEK system	Hardware Software	5 (up to 7) 5 (up to 7)	0.87 | 0.80	Results are reported as Echo | Kilo. Participated in the phase 1 registration process only.
Creative Electron (IA)	The FingerPrint development software	Software	4	0.83	Matched phase 1 registered serial numbers to phase 2 serial numbers.
Battelle (SC)	Barricade hardware system used to test device and collect data as well as the software algorithm which performs classification	Hardware Software	4 – (up to 8) 5 – (up to 8)	0.94	Identified suspect parts for 7 of 8 parts tested. Was not able to separate LM324N parts. Battelle purchased exemplars for each part number.
Nokomis (SC)	ADEC Hardware for electromagnetic signal capture	Hardware	4 – (up to 6)	*RNP*	No results were submitted by Nokomis.
Sandia (SC)	The process of generating and gathering the raw power spectrum (amplitude-versus-frequency plot)	Hardware	4 – (up to 5)	1.00	Performed grouping by comparing to selected reference parts.
PFP (SC)	PFP analytics software	Software	4 – (up to 7)	0.99	Overall final grouping; there are two additional values for comparison to an individual part not included in this table.

KEY:
IA: Image Analysis
SC: Side Channel
Clustering Accuracy: Identifying differences between the two date codes
RNP: Results not provided
Accuracies are provided as fractions

II. Table of Contents

IX. Appendices

Appendix 1. TRL Assessment Spreadsheets for Side Channel Technologies, and Available Product Literature

Appendix 2. Reports on Parts Used for Blind Study

Appendix 3. Reference Test Reports on Parts Used for Blind Study: SMT Corp.

Appendix 4. Blind Study Original Statement of Work: Conventional Testing

Appendix 5. Blind Study Conventional Test Report: Integra

Appendix 6. Blind Study Conventional Test Report: Micross

Appendix 7. Blind Study Conventional Test Report: CALCE

Appendix 8. Blind Study Original Statement of Work: Side Channel Testing

Appendix 9. Blind Study Test Report: Battelle

Appendix 10. Blind Study Test Report: Nokomis

Appendix 11. Blind Study Test Report: Sandia

Appendix 11A. Blind Study Test Report Addendum: Sandia

Appendix 12. Blind Study Test Report: PFP Cybersecurity

Appendix 12A. Blind Study Test Report Addendum: PFP Cybersecurity

Appendix 13. Blind Study Original Statement of Work: Machine Vision Testing

Appendix 14. Blind Study Test Report: Alitheon

Appendix 15. Blind Study Test Report: Covisus

Appendix 16. Blind Study Test Report: Creative Electron

Appendix 17. TRL Assessment Spreadsheets for Machine Vision Technologies, and Available Product Literature

Appendix 18. Company Summaries on Conventional Testing Organizations

Appendix 19. Interview Summaries for Policy Analysis

Appendix 20. Patent Landscape Table of Search Results on Machine Vision Technologies for Counterfeit Electronic Part Detection

Appendix 21. Counterfeit Subject Matter Expert Contact List

III. Introduction

A. Project Initiation

Section 843 of the 2018 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 31, 2020.[1]

The 2018 NDAA §843 identified as objectives for this pilot program the determination of the following:

"(1) The effectiveness and technology readiness level of machine-vision technologies to determine the authenticity of microelectronic parts at the time of the creation of such part through final insertion of such part into weapon systems.

"(2) The best method of incorporating machine-vision technologies into the process of developing, transporting, and inserting microelectronics into weapon systems.

"(3) The rules, regulations, or processes that hinder the development and incorporation of machine-vision technologies, and the application of such rules, regulations, or processes to mitigate counterfeit microelectronics proliferation throughout the Department of Defense."

The 2018 NDAA §843 further provided that the following entities may be consulted in the development of the pilot program:

"(1) Manufacturers of semiconductors or electronics. (2) Industry associations relating to semiconductors or electronics. (3) Original equipment manufacturers of products for the Department of Defense. (4) Nontraditional defense contractors (as defined in section 2302(9) of title 10, United States Code) that are Machine Vision companies. (5) Federal laboratories (as defined in section 2500(5) of title 10, United States Code). (6) Other elements of the Department of Defense that fall under the authority of the Undersecretary of Defense for Research and Engineering."

[1] John S. McCain National Defense Authorization Act for Fiscal Year 2019. Section 843, Public Law 115-232, 2018; referenced herein as the 2018 NDAA §843.

The Defense Microelectronics Activity (DMEA) established two contracts to carry out the tasks identified in the 208 NDAA §843. DMEA contracted the Center for Advanced Life Cycle Engineering (CALCE) at the University of Maryland at College Park (UMD) to lead the pilot program under both contracts. The DMEA Project Engineer on both contracts was Mr. Jeff Carlile, DMEA/MEXB.

The principal investigator on these contracts was Michael H. Azarian, Ph. D., a Research Scientist at CALCE in the Department of Mechanical Engineering within the A. James Clark School of Engineering at UMD. Dr. Azarian's research focuses on the detection, prediction and analysis of failures in electronic components and assemblies. Dr. Azarian is chair of the SAE G-19A Test Laboratory Standards Development Committee which is responsible for the AS6171 family of standards on detection of counterfeit electrical, electronic, and electromechanical parts. He is a member of several other SAE standards committees related to counterfeit parts, and also chairs the working group for the IEEE 1624 standard on organizational reliability capability of suppliers of electronic products.

The co-principal investigator on both contracts was Diganta Das, Ph. D., an Associate Research Scientist at CALCE in the Department of Mechanical Engineering within the A. James Clark School of Engineering at UMD. Dr. Das's expertise is in reliability, environmental and operational ratings of electronic parts, uprating, electronic part reprocessing, counterfeit electronics, technology trends in the electronic parts and parts selection and management methodologies. He has been the technical editor for two IEEE standards and is currently vice chair of the standards group of the IEEE Reliability Society. He is a sub-group leader for the SAE G-19A Test Laboratory Standards Development Committee for counterfeit part detection. For over 12 years he has served as the founder and chair of the SMTA/CALCE Symposium on Counterfeit Parts and Materials, held at the University of Maryland, College Park.

To generate the necessary reports and perform the policy analysis associated with the pilot program, DMEA established a program entitled "Section 843 Machine Vision Pilot Program Report Generation and Policy Analysis". This project is referred to herein as the "MVP" project. To conduct the policy analysis under this contract, CALCE engaged as a sub-contractor the University of Maryland Carey School of Law at the University of Maryland in Baltimore (referred to herein as Maryland Carey Law). The principal investigator on the sub-contract was Patricia E. Campbell, J.D., LL.M., a Law School Professor and Director of the Intellectual Property Law Program at Maryland Carey Law. Professor Campbell has been involved in research relating to counterfeiting for a number of years, as an author, conference presenter, symposium organizer, and lecturer to DoD.

To apply subject matter expertise in addressing, performing research, and summarizing the current status of Microelectronic Authenticity and Security challenges and solutions, DMEA established a program entitled "Microelectronic Authenticity and Security, Evaluation and Research". This project is referred to

herein as the "MASER" Project. Under MASER, CALCE designed and led a blind study of the effectiveness of techniques for counterfeit detection and part authentication, including Machine Vision technologies. CALCE also evaluated the Technology Readiness Levels (TRL) of such tools. To assist in the performance of the blind study, CALCE enlisted the support of SMT Corporation and Mr. Tom Sharpe, Vice President, as a Subject Matter Expert (SME) regarding advanced counterfeit components and clones. The Senate Armed Services Committee (SASC) invited SMT Corporation to participate in the 2011 Counterfeit Electronic Parts Hearing and the 2012 SASC Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain, as a subject matter expert. Mr. Sharpe has been a regular contributor and presenter on advanced counterfeit threats at numerous industry conferences for more than a decade. SMT Corporation provided known advanced counterfeit components and clones for use in the study, along with corresponding authentic parts, and it provided detailed test reports on both types of parts that confirm their identity as either counterfeit or authentic.

1. Expected benefits of this project include:

- Evaluation of Image Analysis, Side Channel, and conventional testing methods as applied to counterfeit microelectronic detection will provide quantitative data on their effectiveness, as well as recommendations for suggested improvements to counterfeit detection methods.
- The work will inform the Defense Microelectronics Activity (DMEA), the Department of Defense (DoD), and other US government agencies on how to employ detection methods to secure the supply chain and thus help to protect the nation's national security interests.
- The TRL assessments will help to identify promising counterfeit detection methods that can be implemented successfully and quickly.
- The policy analysis will identify potential impediments to effective implementation of existing laws and regulations, and indicate steps that can enhance the effective application of such rules, regulations, or processes to mitigate counterfeit microelectronics proliferation throughout the DoD.

The findings of this report are expected to be of value across DoD at all levels for prevention and detection of counterfeit microelectronics and to support efforts to secure the supply chain. It may also assist administrators within DoD and other branches of the U.S. government in setting policy and proposing related legislation. This report should be shared with the groups within the DoD who are active in the area of counterfeit prevention, including: Naval Surface Warfare Center (NSWC) Crane; Army Materiel Command; the Air Force Research Laboratory; the Defense Microelectronics Activity (DMEA); the Joint Federated Assurance Center (JFAC), including the ASSESS working group; the Missile Defense Agency

(MDA); the Defense Logistics Agency (DLA) Land and Maritime; and DLA GIDEP, as well as U.S. Government agencies outside of the DoD.

B. Key Concepts

The stated purpose of the pilot program was to test the feasibility and reliability of using machine-vision technologies to determine the authenticity and security of microelectronic parts in weapon systems. The primary focus of the project is the prevention and detection of counterfeit microelectronics from entering the supply chain. The interpretation and definition of the term "counterfeit" varies greatly across standards, civil and criminal codes, and other government documents. This topic is addressed in greater depth in the Policy Analysis portion of the report, in Section VIII. Counterfeit electronic part has been defined in the DFARS as: "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."[2]

For the purposes of the technology evaluation and blind study, the emphasis was placed on "conventional counterfeits" (including parts that have been remarked or recycled) and "clones." A clone is defined in SAE AS6171 as "a reproduction of a part produced by an unauthorized manufacturer without approval or design authority that replicates the authorized manufacturer's part."[3] Counterfeiters can obtain the information needed to design and produce clones through reverse engineering of authentic parts, access to bare die, or intellectual property theft. Unsophisticated clones might resemble their authentic counterparts in form or fit, but not function. If the functional differences extend to electrical characteristics specified on a datasheet, their detection could be relatively straightforward using standards-based electrical testing. Similarly, a functional resemblance that does not extend to physical or material design characteristics would allow straightforward detection through materials analysis or visual or x-ray inspection. On the other hand, the semiconductor design and fabrication capability and packaging technology available to foreign governments and industrial organizations is highly advanced, and can enable production of high quality reproductions that could be very difficult to detect using conventional means. Some of the technologies and testing discussed in this report have broader applicability to hardware

[2] 48 C.F.R. 202.101, eff. May 6, 2014.

[3] SAE AS6171, Revision A, "Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts."

security and assurance (e.g., clones or tampered parts that may contain stealthy or malicious functionality). However, the parts that were available for the blind study did not allow evaluation of the detection of tampered parts.

A strict technical interpretation of "Machine Vision" is a technology that involves methods for automated image acquisition and processing using computer algorithms. Machine Vision involves the use of software and/or hardware-based automation for capturing and storing one or more images, which includes some or all of the following:

- positioning an object within the field of view of an image sensor, which can be accomplished through hardware (e.g., robotics), software (i.e., image manipulation) or a combination thereof;
- adjusting the illumination conditions to obtain consistency in the appearance of the object; and
- determining the image acquisition conditions (for such parameters as magnification, exposure time, sensitivity, filtering, resolution, etc.).

Machine Vision systems typically include one or more of the following steps applied to the acquired images:

- processing the image (performing a set of transformations to the image or associated data to optimize its suitability for the intended analysis);
- identifying relevant features in 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/or
- 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 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. 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. On the other hand, the automation of the imaging process also hinders the application of subject matter expertise, the opportunity for subjective evaluation, and consideration of factors that were not explicitly addressed in the development of the software that are introduced by human involvement.

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 (see https://www.visiononline.org/vision-standards-details.cfm?type=7) and an archive of webinars.

Conventional imaging involves use of the visible part of the electromagnetic spectrum, typically in the range of about 380 to 700 nm wavelength. Other forms of imaging, that make use of regions of the spectrum that do not contain visible light, are well known. Examples include X-ray radiography, magnetic resonance imaging, terahertz imaging, and imaging or mapping of signals using infrared radiation (e.g., infrared thermography or Fourier Transform Infrared Radiation, or FTIR, mapping); Raman spectroscopy; or X-ray radiation generated by interaction with electrons (Energy Dispersive X-ray Spectroscopy, or EDS) or through fluorescence of incident X-ray radiation (X-ray Fluorescence Spectroscopy, or XRF). By extension, therefore, it is useful to consider authentication technologies that are based on techniques for extracting features or images of microelectronic devices using energy outside of the visible part of the electromagnetic spectrum.

In most of this report, "Machine Vision Technologies" is therefore interpreted more broadly than the strict technical description provided above, to include the entire electromagnetic spectrum: methods employing X-ray imaging, analysis of radiated electromagnetic emissions, and analysis of electrical power consumption, some of which make use of recent advances in image processing, such as neural networks and other machine learning technologies. The policy analysis section of the report, Section VIII, includes an analysis of patents and standards that employs an interpretation of Machine Vision as methods that involve the formation of images using automated image acquisition and processing using computer algorithms.

C. Summary of Tasks and Content of Report

This report addresses four main tasks that are associated with the MVP and MASER projects, as identified by DMEA:

- Task 1 – Evaluate existing advanced counterfeit detection systems

  1a: Determine Technology Readiness Level (TRL) for each system

  1b: Determine current effectiveness of each system based on blind study with known counterfeits/clones and known good test articles

- Task 2 – Evaluate existing application of machine-vision and AI technologies to IC and PCB hardware assurance

  2a: Determine TRL of each technology

  2b: Evaluate effectiveness and limits of each technology

2c: Recommend which technologies should be further developed

- Task 3 – Evaluate and develop specific solutions to IC supply chain risk

  3a: Demonstrate near-term solutions; e.g., Known Good Virtual Golden Samples Demonstration

  3b: Study and develop long-term solutions

- Task 4 – Review applicable laws, regulations, policies, and DoD Instructions with respect to machine-vision and the counterfeit threat

  4a: Identify current roadblocks

  4b: Recommend changes to current regulations, policies, etc.

  4c: Recommend new regulations, policies, etc.

The remainder of the report has been structured to reflect this task breakdown. Supporting information, test reports, and related work product has been included in a series of Appendices.

IV. Task 1: Evaluation of Existing Advanced Counterfeit Detection Systems

A. Task 1a: Technology Readiness Assessment of Side-Channel Detection Systems

CALCE performed a Technology Readiness Assessment[4] (TRA) using the U.S. Department of Defense Technology Readiness Assessment Deskbook[5] to analyze and identify each participating system's Technical Readiness Level[6]. Only aspects of the TRA Deskbook relevant (Appendix A: a template for a TRA, Appendix B: guidance on identifying Critical Technology Elements, Appendix C: guidance on assessing technology maturity) to the pilot program are used. CALCE established specific metrics for the assessment and generated a series of reports detailing the Critical Technology Elements and the Technical Readiness Level of each participating system. Those individual reports and the comparative conclusions are included in this report to DMEA.

This use of the TRL information can vary depending on the goals of the user. The US DOD and other government agencies can evaluate the return on investment in the context of research funding goals by assessing commercialization, availability, wide acceptance including standards, and IP use by the

[4] An assessment of how far technology development has proceeded. It provides a snapshot in time of the maturity of technologies and their readiness for insertion into the project design and execution schedule.

[5] U.S. Government Accountability Office, "Technology Readiness Assessment Guide," 2016.

[6] A metric used for describing technology maturity. It is a measure used by many U.S. government agencies to assess maturity of evolving technologies (materials, components, devices, etc.) prior to incorporating that technology into a system or subsystem.

government. It is also possible that DoD would recommend using the tool to various agencies and prime contractors based on the usability in a DoD or contractor facility. The timeline and cost considerations will be different based on the use, such as inventory review, purchase from an unauthorized distributor, investigation of failure incidents (acceptability at internal adjudication, the building of cases, acceptance at the court of law). In all these cases, if the government asks a contractor to use a particular technology, the government may be committing to paying the cost, and the government may be indemnifying the company from future problems. One system may be more ready for a particular use while being unsuitable for different use. For uniformity, we made the following use assumption for TRL:

- For the Side Channel tools, the system's application is the inspection of components for counterfeit detection at the point of purchase or acceptance.
- For the Image Analysis tools, the assumption is that the system can identify the registered parts at any time after registration. Those parts can be loose, in their packaging (e.g., tubes, trays), on assembled boards, or taken off the boards for investigation.

Usability factors include coverage of parts and technology by functionality, package type, and required information to perform the counterfeit detection. The cost considerations include the cost of the equipment, the cost of personnel to run the equipment and analyze the data, and non-recurring engineering (NRE) costs. The NRE cost includes programming, fixtures, and machine learning training. Whether or not a method is useful also depends on the lead time and numbers and types of samples required.

A traditional technology readiness assessment evaluates technology on a stand-alone basis. For this evaluation, there is an element of comparison with the established tools and methodologies. These technologies are meant to replace (or complement) the traditional method of detection using analytical and visual tools. As a result, the technology needs to be compared among each other and the traditional methods. No TRL is available or calculated for the traditional methods for comparison. Hence, the comparison will traditional methods will need to include accuracy, cost, and time.

Another factor in the assessment is the organizations' business goals and mission. The TRL is estimated based on the assumption that a product is meant for commercialization by the developers. However, depending on the organization, the goals can include finding IP users and licensees, commercializing and selling the product for use by others, commercializing and providing detection as a service, or just publishing the findings as an academic exercise.

We have used the NASA TRL calculator (available as an open-source tool from the Defense Acquisition University (DAU). The questionnaire emphasizes an assessment of flight preparedness. For our assessment, we have considered the use conditions defined earlier to be equivalent to flight preparedness.

Since all the systems assessed have multiple subsystems and associated development items, a critical technology element[7] (CTE) for each counterfeit detection method is selected for the assessment. The TRL handbook defines that to be considered "critical," a technology must meet both of the following requirements: the system must depend on the technology to meet operational requirements and the technology element or its application must be "new or novel or in an area that poses major technological risk during detailed design or demonstration." The CTEs can be hardware or software.

In a traditional technology readiness assessment, CTE's maturity during the acquisition process through each milestone of the acquisition process because knowledge of technology's maturity evolves. In this assessment, there is no active acquisition process. This TRL assessment assumes that this assessment will inform future decision making. In the absence of an active acquisition process, the suggested participants of a TRL estimation provided in the handbook do not exist, and the research team at CALCE performed the assessment. The CALCE team has used the following sources of information in this assessment:

- Company information
    - Company website
    - Company literature or literature about the company
    - Company presentations
        - Conferences
        - Public releases
    - Images or videos of the system
- Interviews by CALCE
    - Interviews with users and specialists
        - DoD
        - Subject matter experts, including members of the development team
    - Communications with company members
- Academic sources
    - Journals on the area of the technology
        - Conference papers and presentations
        - Archival journals

[7] A technology element is "critical" if the system being acquired depends on the technology element to meet operational requirements (with acceptable development, cost and schedule; and with acceptable production and operations costs) and if the technology element or its application is either new or novel.

        - Trade magazines
- Patent landscape
    - Patent applications
    - Patents issued to companies as well as related patents

The TRL scale takes into account the operational environment defined as "Environment that address all the operational requirements and specifications required of the final system" and the relevant environment "Testing environment that simulates both the most important and most stressing aspects of the operational environment." Most test labs do not employ a "one-size-fits-all" approach but rather aggregate multiple tests, each one designed to detect a specific type of counterfeiting. For this assessment, we assume that one single tool is used for the detection, and the technology is evaluated in isolation. Table 3 lists the definitions of the TRLs.

Table 3: Review of TRL Scale

TRL	Description
1	Basic principles observed and reported
2	Technology concept and/or application formulated
3	Analytical and experimental critical function and/or characteristic proof of concept
4	Component and/or breadboard validation in a laboratory environment
5	Component and/or breadboard validation in a relevant environment
6	System/subsystem model or prototype demonstration in a relevant environment
7	System prototype demonstration in an operational environment
8	Actual system completed and qualified through test and demonstration
9	Actual system proven through successful mission operations

1. Battelle Barricade

The Barricade system by Battelle is used to sense static power consumption of ICs or electronic parts at different voltages measuring the current and frequency responses. The testing is done on parts at steady state and provided with a constant voltage supply. The part is also connected to an external clock signal which changes over time. As the external clock signal changes, the intrinsic random properties of the component affect the signal being sensed. The current draw on the supply voltage changes as the external clock signal transitions which can be measured with an ammeter and oscilloscope. The Barricade system can also be used to perform classification. A set of test vectors are applied to the device under test at

different frequencies. The current draw is measured during the tests after which a power waveform is plotted and compared to known authentic parts or classes of components enrolled in the system. The Barricade system can be used to cluster and classify parts from different date/lot codes and differentiate between authentic and counterfeit parts.

Battelle is a non-profit research institution which uses the money obtained from products to further their work and research. Battelle markets the Barricade system on its website as a commercial product, however no direct sale opportunities are presented.

a. Basic information on the developers and technology:

- **Location:** Headquartered in Columbus OH
- **Battelle Leadership:** President and CEO: Lewis Von Thaer (Battelle)
- **Barricade Leadership:** Thomas Bergman, Katie Liszewski
- **The size and portability of the method or device**: The system can be made portable if a laptop computer is used. The testing system (no including computer) is 13" x 9" x 4.5" and weights 14 lbs. The black box in Figure 1 shows the Barricade system.
- **Cost for the product**: Unknown
- **Resources and infrastructure required for testing**: A computer with network connection to remote database (provided by Battelle) is required to use the system. Software provided with the hardware testing system is also required. Process for testing and enrollment is included in Figure 2.
- **Preparations needed before testing can be performed**: The user needs a Xeltek SUPERPRO 5000/5004GP series socket compatible with the part to be tested. If part is already in the system, the profile can be selected otherwise a new entry would be required. Information needed includes the pin layout of the part, including the pin locations of power and ground pins, and the normal operating voltage of the part.
- **Numbers of samples needed**: The number of parts required to train the system to authenticate other parts is not clear, although Battelle indicated that at least 10-50 parts are preferred.
- **The skill level and training of personnel required to operate equipment, to analyze data, and to interpret results**: If the part under test has been entered into the system and a profile exists, the skill required is minimal. Simply place the device in the socket and run the test. The software will interpret and provide and analysis of the results. The skill required to train the system on an unseen part is not well described. Figure 2 suggests that destructive testing may be required to authenticate untrusted parts prior to enrollment.

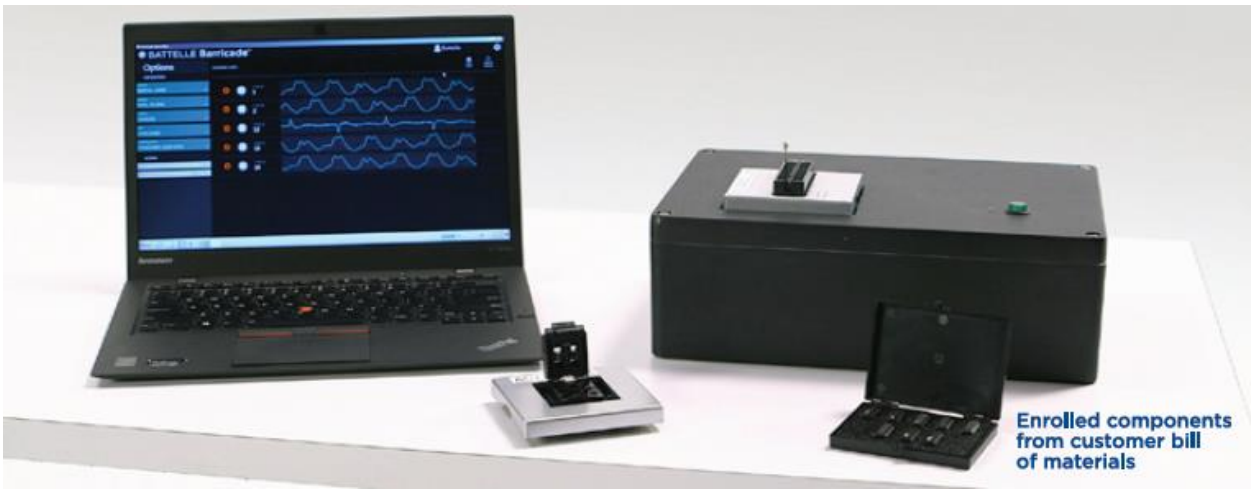


Figure 1: Barricade System with Computer

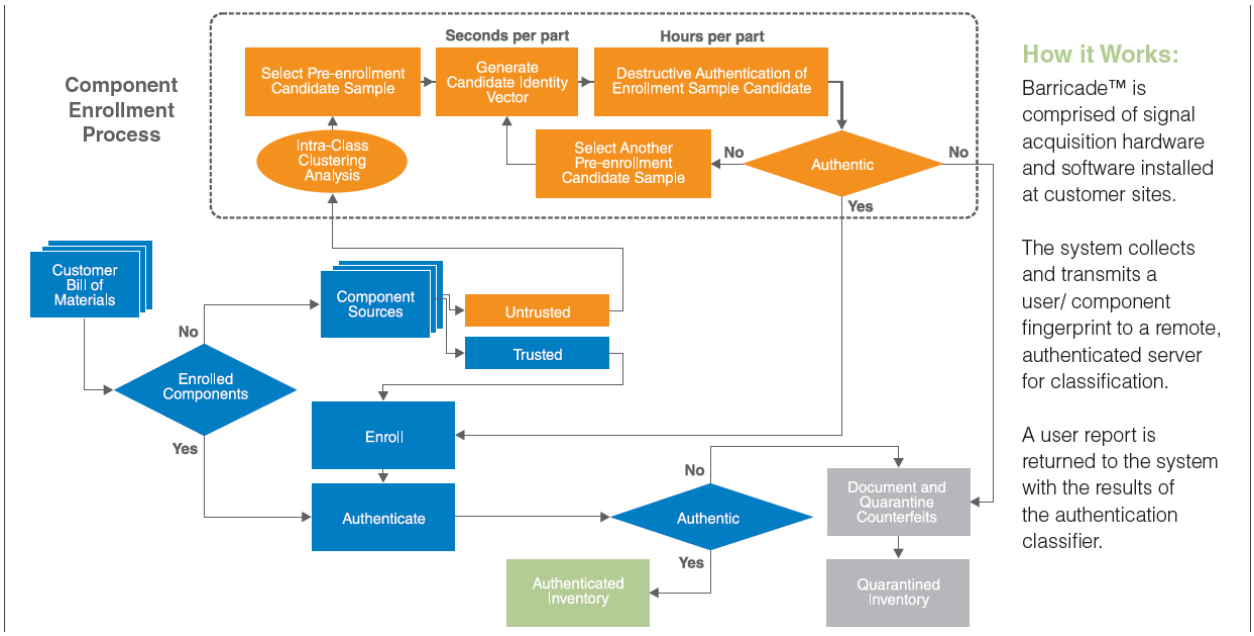


Figure 2: Component Enrollment Process

Steps in use of the Barricade System:

1. A part is loaded into the system
2. Test vectors are manually selected and applied to the part, and the features of the power consumption of the device are established and stored in the system.
3. Barricade's classification algorithm divides the parts in the system into multiple categories. PCA is used to transform the final feature vector of the part.
4. Parts are tested on at a time and classified by the system based on the measured features and those stored.

The test vectors are applied at different frequencies. The test vectors are selected to be appropriate for the type of part under test. The power consumption of the part is measured by recording the current. The Barricade system provides a power waveform on the user interface of a connected computer.

The classification process depends on whether parts have been enrolled prior to testing. If known authentic parts have been enrolled, then the system can compare the PCA features to those stored. Parts can then be classified. The application of multiple test vectors provides the opportunity to improve the classification results. Barricade tends to show the first two principal components after Band filtering; however, it is not clear if only the first two principal components are always used for analysis. The Barricade system is also capable of classifying different date/lot codes of the same part. It appears that this process would require each part to be enrolled into the system if not already done.

Table 4: Parts Evaluated by the Barricade System

Functionality	Package Type	Part Number	Tests Performed
EPROM	DIP	M2732A-2F1 (ST Microelectronics)	Discriminating authentic and counterfeits.
EPROM	SOIC	AT28HC256-90SU (Microchip Technology)	Date lot discrimination.
3-bit Decoder	DIP	DM74LS138N (Fairchild, National) SN74LS138N (Motorola, TI)	Discrimination between different manufacturers.
8-bit shift register	DIP	SN74HC164N (TI)	Discriminating authentic and clones.
Quad NAND gate	DIP	SN74S00N (TI)	Date lot discrimination.
Hex Schmidt inverter	DIP	CD40106BE (TI)	Discriminating authentic and clones.
Hex inverting buffer	DIP /SOIC	CD4049 (TI)	Discriminating authentic and clones from multiple date/lot codes.
Microcontroller	-	MC68HC908EY	Discrimination between commercial and military grade.
Microcontroller	-	MC68HC908GZ MC68HC908GR	Discrimination between date/lot code and microcontroller types.
Microcontroller	-	MC68HC908GR	Discrimination between modified and unmodified parts.
Microcontroller	-	MSP430	Discrimination between variants of microcontroller.

b. **Patents:**

- L. House and D. Engelhart, “Electronic Component Classification,” United States of America Patent US 10,416,219 B2, 17 September 2019.
- L. House and D. Engelhart, “Electronic Component Classification,” United States of America Patent US 10,054,624 B2, 21 August 2018.
- L. House and D. Engelhart, “Electronic Component Classification,” United States of America Patent US 10,054,624 B2, 12 September 2017.
- K. Liszewski and M. Brewer “System and Method for Generating Test Vectors,” United States of America Patent Application 20180/307654 A1, 25 October 2018.

c. **Presentations:**

- T. Bergman and K. Liszewski, “Battelle Barricade: Authentication Testing of Integrated Circuits through Power Consumption Waveform Analysis,” in CALCE/SMTA Symposium for Counterfeit Parts and Materials, College Park, MD, June 2017.
- T. Bergman, “Authentication Testing of Integrated Circuits through Power Consumption Waveform Analysis,” in CALCE/SMTA Symposium for Counterfeit Parts and Materials, College Park, MD, June 2018.
- L. J. House, “Battelle Barricade: Electronic Component Authentication Technology,” in Counterfeit Microelectronics Working Group Meeting, Arlington, VA, February 2015.

d. **Articles:**

- T. D. Bergman and K. T. Liszewski, “Battelle Barricade: A Nondestructive Electronic Component Authentication and Counterfeit Detection Technology,” in Proceedings of the 2016 IEEE Symposium on Technologies for Homeland Security (HST), Waltham, Massachusetts, May 2016.
- K. T. Liszewski and T. D. Bergman, “Battelle Barricade: Microelectronic Device Authentication and Counterfeit Detection Utilizing Power Analysis,” in Proceedings of the 2017 International Symposium for Testing and Failure Analysis (ISTFA), Pasadena, California, November 2017.

e. **Marketing:**

- Battelle Barricade, “Are Counterfeit or Clone Chips in Your Systems?” 2017.

Table 5: Additional Information about Battelle

Question	Answer
How many units are manufactured?	Roughly 20 systems, most of which are at Battelle.
Are units in stock or are they built against order?	It is presumed that they are made to order.
Do the units include software and database? Do the users have to subscribe for getting those features?	The software and database are included with the system based on the information provided in the brochure. It is assumed that a subscription is not required given it is listed as provided with the hardware.
Do you have a product data sheet?	There seems to be no public data sheet, however some general system information is provided in the brochure.
Do you offer support service?	This is not addressed.
Do you offer repair or upgrades?	This is not addressed.
What is the lead time to buy one?	This is not addressed.
What is the price of the unit?	This is not addressed.
What are you selling to customers?	Hardware and software system.
Are the units built outside of the company?	It appears that Battelle makes them all in house.

For the purpose of this assessment, the hardware system used to test device and collect data as well as the software algorithm which preforms classification are considered Critical Technology Elements (CTE). The TRA is performed for this CTE. Both hardware and software were considered for the assessment. It is found that the hardware side of the system has achieved TRL of 4 completely and has met some of the aspects up to TRL 8. It was also found that the software side of the system achieved a TRL of 5 completely and has met some of the aspects up to TRL 8.

While manufacturing TRL assessment was not performed, some information regarding the status of the product is provided in

Table 5. The information presented in the table is obtained by direct communication and from publicly available literature.

2. Nokomis: Advanced Detection Of Electronic Counterfeits (ADEC)

Radiated electromagnetic emissions (REME) form the basis for the ADEC System developed by Nokomis, Inc. If the current through a conductor changes with time, the amount of charge enclosed by the conductor will also change. Thus, the electromagnetic radiation from that conductor will be time-variant. Generalizing this to a complete microelectronic device indicates that the device's overall electromagnetic radiation will change with time. Ideally, these variations will be the direct result of changes in the device's

operation over time, rather than the result of noise or electromagnetic fields in the environment. This provides a means for the characterization of the operation of a device based on measurements of radiated electromagnetic emission (REME), typically in the radio frequency or microwave part of the spectrum. Such emissions are measurable using antennae and may be affected by the operating characteristics of the device, its configuration, materials, and other physical characteristics, as well as external factors including environmental conditions (e.g., temperature and humidity), mechanical excitations (e.g., shock or vibration), location relative to the antenna, and local electromagnetic environment. Thus, the electromagnetic emissions of a microelectronic device are characteristic of the device under consideration assuming these other factors can be controlled. The age, materials, and layout all contribute to a unique "signature" for each device.

Electromagnetic Side Channel attacks are the exploitation of electromagnetic emissions to compromise the confidentiality of data in an electronic system. REME can be exploited to reveal information about the functioning of the device. The signals produced by this variation can be analyzed statistically in order to reveal characteristics of the device, such as encryption algorithms used to process data. In principle, the same concept can be used to verify the absence of unexpected code or circuitry in a device, if it is operated in the same manner as a "golden" part to which its REME spectra are compared.

Gandolfi, Mourtel, and Olivier[8] found that this theoretical principle can be applied to smart cards and used to establish practical results. They found that electromagnetic signals collected during their experiment were noisy, but transmit information. Further, coupled with proper data processing techniques, the authors claimed that their results are more accurate than a power analysis would have been; their algorithm generated no false alarms due to signal errors generated during data processing. Other studies have explored the use of near- and far-field probes to collect the electromagnetic signals given off by a device These investigations demonstrated that the electromagnetic Side Channel can be used to reveal information about the operation of a device.

Nokomis Inc. has developed the Advanced Detection of Electronic Counterfeits (ADEC) system to exploit the use of electromagnetic emissions to analyze the authenticity of components and printed circuit boards.

[8] K. Gandolfi, C. Mourtel and F. Olivier, "Electromagnetic Analysis: Concrete Results," in *Cryptographic Hardware and Embedded Systems*, Berlin, Heidelberg: Springer, 2001, pp. 251-261.

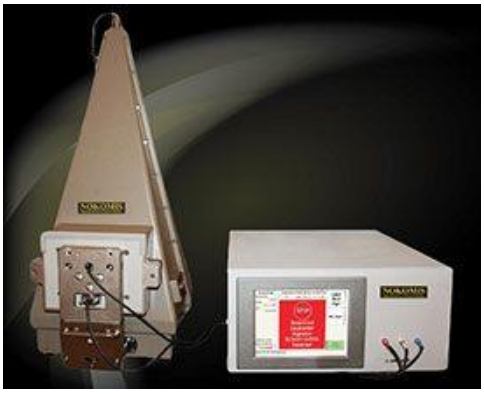


Figure 3. ADEC System by Nokomis (from http://www.nokomisinc.com)

a. **A summary of their corporate information, patent portfolio, and DoD research funding follows.**

- **Incorporation:** October 2002 in Pennsylvania
- **Headquarters:** 310 5th St., Charleroi, PA 15022
- **Address of incorporation:** 6510 Brownsville Rd., Pittsburgh, PA 15236
- Advanced Electronic Diagnostics Division is located at 353 E. Lincoln Ave., McDonald, PA 15057
- Test Range Facility is located at 209 Country Club Rd., Mather, PA 15346

  This address is sometimes listed as Waynesburg, PA
- **Officers and Directors**
  - Walter Keller, Jr. – President
  - Eli Polovina – VP of Operations, Director
  - Vincent Joyce – Director of IT
  - Gena Disimoni – Director of Advanced Technology
- **Financial Information**
  - Annual revenue of $5.5m according to ZoomInfo in June 2020
  - Annual revenue of $3.6m according to Dun & Bradstreet in June 2020
- **Company size**
  - 28 employees according to ZoomInfo in June 2020
  - 15 employees according to Worldbase in May 2020
- **Business Analysis**
  - Given a medium-high business delinquency risk score by Experian

        - Trending positively
    - Given a low business stability risk score by Experian
        - Trending positively
- **Principal investigators**
    - Walter Keller, (724) 483-3946, wkeller@nokomisinc.com
    - Andrew Portune (no longer with the company as of 2020)
- **Public website:** http://www.nokomisinc.com/

b. Intellectual Property Related to the Technology Under Assessment:

Patents and Patent Applications

- US8825823B2
    - System and method for physically detecting, identifying, diagnosing and geolocating electronic devices connectable to a network
    - 01/06/2012 priority date
- US9562962B2
    - System and method for physically detecting, identifying, diagnosing and geolocating electronic devices connectable to a network
    - 07/11/2014 priority date
    - A continuation of US8825823B2
- US9059189B2
    - Integrated circuit with electromagnetic energy anomaly detection and processing
    - 03/02/2012 priority date
    - EP2820675A1 is the European Patent Office equivalent
    - JP2019062207A is the Japanese Patent Office equivalent which has not yet been granted
    - WO2013131031A1 is the WIPO equivalent which has not yet been granted
- US9887721B2
    - Integrated circuit with electromagnetic energy anomaly detection and processing
    - 05/04/2015 priority date
    - A continuation of US9059189B2
- US9851386B2
    - Method and apparatus for detection and identification of counterfeit and substandard electronics
    - 03/02/2012 priority date

        - EP3114490A1 is the European Patent Office equivalent
        - WO2015134148A9 is the WIPO equivalent which hasn't been granted yet
    - US10571505B2
        - Method and apparatus for detection and identification of counterfeit and substandard electronics
        - 12/19/2017 priority date
        - This is a continuation of US9851386B2
    - US10475754B2
        - System and method for physically detecting counterfeit electronics
        - 03/02/2012 priority date
        - EP2820595A1 is the European Patent Office equivalent
        - JP2019009455A is the Japanese Patent Office equivalent which has not yet been granted
        - WO2013131073A1 is the WIPO equivalent which has not yet been granted
    - US20200144204A1
        - System and method for physically detecting counterfeit electronics
        - 10/31/2019 priority date
        - This patent application was filed a few months after US10475754B2 was granted (possibly a continuation)
    - US20170245361A1
        - Electronic device and methods to customize electronic device electromagnetic emissions
        - 1/6/2017 filing date
    - US9772363B2
        - Automated analysis of RF effects on electronic devices through the use of device unintended emissions
        - 2/26/2015 priority date
    - US9285463B1
        - Method and apparatus for battle damage assessment of electric or electronic devices and systems
        - 12/12/2012 priority date
    - US9797993B2
        - Advance manufacturing monitoring and diagnostic tool
        - 12/27/2013 priority date

- EP3201821A4
    - Detection of malicious software, firmware, IP cores and circuitry via unintended emissions
    - 10/03/2014 priority date
    - WO2016054626A9 is the WIPO equivalent
    - EP3201821A1 is the European Patent Office equivalent
    - **US10395032B2** is the patent in the United States
        - Priority date for the US is 03/19/2015
- US9642014B2
    - Non-contact electromagnetic illuminated detection of part anomalies for cyber physical security
    - 03/19/2015 priority date
- US10149169B1
    - Non-contact electromagnetic illuminated detection of part anomalies for cyber physical security
    - 03/13/2017 priority date
    - A continuation of US9642014B2
- US10416213B2
    - Ultra-sensitive, ultra-low power RF field sensor
    - 10/29/2015 priority date
- US10149169B1
    - Non-contact electromagnetic illuminated detection of part anomalies for cyber physical security
    - 03/13/2017 priority date

c. **Funding from DoD: Multiple contracts from 2012 to present**

- Navy RIF: N00024-12-C-4516
- MDA SBIR Phase II: HQ0147-14-C-7019
- MDA 12-026
- Air Force SBIR Phase II: FA8222-15-C-0006
- Air Force RIF: FA8222-15-C-0008
- Air Force SBIR Phase II: FA8750-15-C-0268
- Air Force SBIR Phase II: FA8650-17-C-1035
- DMEA SBIR Phase II: HQ0727-17-C-0004

- Nokomis website information: Nokomis has current DCAA audit certification for execution on contracts up to $100M.

d. **Presentations:**

- B. Pathak and G. Johnson, “Advanced Detection of Electronic Counterfeits (ADEC); DFARS Case 2012-D055, Detection and Avoidance of Counterfeit Electronic Parts,” June 28, 2013, presented at public meeting hosted by DoD for discussion of DFARS Case 2012-D055, available online at https://www.acq.osd.mil/dpap/dars/publicmeeting/presentations/Nokomis_Presentation.pdf. See also Section VIII-A-2-a of this report.
- B. Pathak, “Advanced Detection of Electronic Counterfeits (ADEC),” in *ERAI Executive Conference*, Orlando, FL, 2013.
- W. Keller, “Advanced Detection of Electronic Counterfeits (ADEC),” in *Counterfeit Electronic Parts & Electronic Supply Chain Symposium - East*, College Park, MD, 2013.
- W. Keller, "Advanced Detection of Electronic Counterfeits," in *Symposium on Counterfeit Parts and Materials*, College Park, MD, 2014.
- A. Portune, “Supply Chain Assurance Using ADEC Technology,” in *Symposium on Counterfeit Parts and Materials*, College Park, MD, 2015.
- W. Keller, “Maintenance Depot Counterfeit Detection Assessments Utilizing Electromagnetic Emission,” in *Symposium on Counterfeit Parts and Materials*, College Park, MD, 2016.
- A. Portune, “Advanced Detection of Electronic Counterfeits for Enhanced Supply Chain Assurance Against Sophisticated Counterfeits," in *Symposium on Counterfeit Parts and Materials*, College Park, MD, 2017.
- A. Brant, “Nondestructive Detection of Counterfeit Radiation Hardened Electronic Parts via radiated Electromagnetic Emissions (REME) Analysis,” in *Symposium on Counterfeit Parts and Materials*, College Park, MD, 2018.
- Nokomis, “ADEC Presentations,” 30 May 2019. [Online]. Available. http://www.nokomisinc.com/adec-presentations.html. [Accessed 19 February 2020].

Nokomis has tested a wide array of parts using their system. Many of these tests were performed for government-funded programs in whose reports the results may be found. A few such parts that could be found from public literature, presentations, patent applications, and granted patents have been listed in Table 7.

Table 6. Parts Tested using ADEC[9]

Functionality	Package Type	Part Number	Tests Performed
DC to DC Converter	SOIC	ADUM5421ARZ (Analog Devices)	General authenticity
Microcontroller	PDIP PLCCTQFP	AT89S52 (ATMEL)	General authenticity

A larger list of tested parts was provided to CALCE by Nokomis, and has been reproduced in **Error! Reference source not found.**7.

Table 7. List of Parts Tested Using ADEC System as Reported to CALCE by Nokomis.

NSN	MFG Part Number	MFG
5962012640083	CY7C225A-40DMB	Cypress
5962013601549	54LS193	E2V/QP Semi
5962012640083	SNJ54LS244J	TI
5962012629453	SN54LS374J	TI
5962013036132	PALC22V10-25DMB	Cypress
5962013036132	PALC22V10-25DMB	QP Semi
5962013267536	SNJ54LS156J	TI
5962012384928	80C31BH/BQA	QP Semi
5962011495443	AM9016DPC	AMD
5962012489359	SN54ALS169BJ	TI
5962012489472	SN54LS174J	TI
5962012862245	AM27S29/BRA	AMD
5962012410647	JM38510/65602BRA	TI
5962010708976	54S174	TI
5962010748048	M38510-01701BEB	Nat Semi
5962010748867	14536B/BEAJC	Motorola
5962010748867	CD4536BF/3A	TI
5962013574794	TDC1046B8V	QP Semi
5962012543904	SN54S74J	TI
5962012639192	SN54LS109AJ	TI
5962012400498	54L74/BCA	Rochester
5962013934937	AT22V10L-25DM/883	Atmel
5962013934937	AT22V10L-25DM/883	QP Semi
5962013492199	PALC22V10-40DMB	Cypress
5962013492199	PALC22V10-40DMB	QP Semi
5962012858222	SL54163/BEA	Signetics
5962011888744	M38510/50401BRA	TI
5962011046417	54S374/BRA	Signetics
5962012886902	54LS112A	TI
5962012912900	54F74	TI
5962012912900	M38510/34101BCA	Rochester
5962012912900	JD54F74BCA	QP Semi
5962013176621	DM28C256-150/B	Xicor
5962013176621	AT28C256-15DM/883C	Atmel
5962013065557	AM29705A/BXA	AMD
5962012878541	SNC54S174J	TI
5962012856514	93S16DMQB	Nat Semi
5962012318507	54ALS74A	TI
5962012504384	SNJ54HC273J	TI
5962012608674	IDT7164S70DB	IDT
5962011007994	CD4040BCN	Nat Semi
5962011007994	CD4040BMJ/883	QP Semi
5962013595486	CY7C225A-35DMB	Cypress
5962015739840	GEM40301QEA	SRI

NSN	MFG Part Number	MFG
5962013266057	JM38510/11302BEA	Analog Devices
5962013266057	M38510/11302BEA	QP Semi
5962012456812	JD54F163BEA	QP Semi
5962012966828	PAL16R6B-4	MMI/AMD
5962012488630	SN54LS191J	TI
5962004302600	M38510/01307BCA	Lansdale
5962004302600	5490/BCA	Rochester
5962013187889	P4C1256L-100DWMB	Pyramid
5962014430935	AT28C256-15UM/883	Atmel
5962012622712	TIBPAL16R8-20MFKB	TI
5962013169109	JM38510/66304BEA	TI
5962013035762	SNJ54HCT374J	TI
5962012801453	JM38510/32702BCA	TI
5962012801453	JM38510/32702BCA	TI
5962012801453	SN54LS393J	TI
5962012801453	JM38510/32702BCA	Motorola
5962012648166	SN54LS175J	TI
5962012622720	TIBPAL16R6-30MJB	TI
5962011882933	HM1-6514	Intersil/Harris
5962013231861	SMJ27C512-25JM	TI
5962013231861	SMJ27C512-25JM	Micross
5962014700021	SNJ54ALS374AJ	TI
5962013236962	AT28C256-25FM/883	Atmel
5962PLJ00925F	29651ADMB	Raytheon
5962010685245	SN54LS163AJ	TI
5962012088567	SNJ54ALS569AJ	TI
5962012044547	SN54F244J	TI
5962012223905	JM38510/38303BRA	TI
5962012223905	54ALS244AJ/883	Nat Semi
5962013014863	IDT54FCT374LB	IDT
5962013014863	54FCT374LMQB	QP Semi
5962012645223	AM27S07A/BFA	AMD
5962011975030	54F240	TI
5962011975030	JM38510/33201BRA	Motorola
5962013397104	PALC22V1030DMB	Cypress
5962013397104	PALC22V10-30DMB	QP Semi
5962014538879	PALC16R6-30DMB	Cypress
5962012793741	AD565SD	Analog Devices
5962012863678	M38510/07102BEB	TI
5962012940102	CD54HCT377F3A	TI
5962012288376	SNJ54HC74J	TI
5962012124322	54F109/BFA	Signetics
5962011020627	SN74LS273N3	TI
5962003697641	M38510/01306BEA	Lansdale
5962010681044	M38510/31513BEA	Motorola
5962010681044	54LS190/BEA	Rochester

NSN	MFG Part Number	MFG
5962013628122	AT28HC256-90UM/883	Atmel
5962014156543	16V8D-20LD/883	QP Semi
5962014080586	CD54HC138F3A	TI
5962014116183	IDT72401L10DB	IDT
5962013337436	SL10631/BEA	Lansdale
5962013548223	CY7C167A-45DMB	Cypress
5962012622710	TIBPAL16L8-20MFKB	TI
5962012622722	TIBPAL16R4-30MJB	TI
5962012678991	SN54F241J	TI
5962012726295	SNJ54F109J	TI
5962012674869	SNJ54LS337J	TI
5962012837123	M38510/00202BDA	Lansdale
5962013137194	SNJ54LS138FK	TI
5962013173178	IDT71256L45DB	IDT
5962012886900	SL82S129/BEA	Signetics
5962012858216	54L73/BDA	Rochester
5962012701947	Z0800206LMB	Zilog
5962012661479	AD570SD/883B	Analog Devices
5962005476683	SNJ54S112J	TI
5962010661151	JANB54LS74AW	TI
5962013154989	8403609LA	IDT
5962013633446	WS27C010L-15DMB	WSI
5962013818096	M38510/20304BFA	QP Semi
5962PLJ00047F	25LS2569DM/B	Rochester

[9] W. Keller, "Advanced Detection of Electronic Counterfeits," in *Symposium on Counterfeit Parts and Materials*, College Park, MD, 2014

Their system uses a radio frequency receiver to measure the radiated electromagnetic emissions that are characteristic of a microelectronic part. The ADEC RF subsystem is the Nokomis Hiawatha sensor, which achieves a -170 dBm sensitivity and uses multiple independent channels for data throughput. This Hiawatha receiver is also a Nokomis product. Hiawatha is configured to receive signals in the frequency range between 30 MHz and 3 GHz.

Nokomis has prioritized the sensitivity of REME detection in their hardware design, providing access to features in the detected spectra that might otherwise not be discernable. During communications with Nokomis, they indicated that a signal-to-noise ratio of -70 dB at room temperature was possible for certain features or portions of the spectrum.

Electromagnetic radiation is generated by a device when it is powered on. In order to power on the device, a voltage necessary to energize the device's basic function is provided to one power input. In order to further evoke an electromagnetic response in the device, a time varying signal is provided to another input. In the case of integrated circuits and other complex components, rather than providing this signal to a power input, it can be provided to a clock input so that more complex operations of the device are not triggered.

According to Nokomis,[10] ADEC has two configurations: automated screening and analytical testing. Automated screening requires reference parts in order to develop a signature file. These reference parts should ideally be known authentic parts (also known as exemplars or golden parts). Using the "best available" components is also possible but introduces increased risk that the reference parts are not authentic. Analytical testing does not require a reference part or signature file.

Both configurations require that the device under test be powered. The part under test is brought to a "minimal functionality" state. Only manufacturer-specified inputs are provided.

The process steps for testing devices using the ADEC system has been provided to CALCE by Nokomis and is as follows:

1. The device is loaded into the test chamber
2. The device produces unintended electromagnetic emissions when powered on
   - Inputs are provided according to the part's data sheet, typically power, clock, and ground
   - Additional inputs may be necessary based on the part's specifications
3. ADEC provides one voltage, one clock, and ground to the DUT
4. The ADEC RF receiver subsystem is used to acquire and analyze the electromagnetic signature

[10] A. Portune, email communication, Dec. 9, 2019.

- Typically, specific frequency regions of interest are captured for the DUT for analysis
- N number of signature metrics are determined for M frequency regions, creating a matrix of quantitative values used to assess the part

5. Classification using a reference part:

- The reference parts' signatures must be established before the operator can proceed
- The operator selects the believed identity of the part from a list of previously tested parts
- A binary classification is then performed as follows:
  - A Bayesian network is utilized, acting upon the N signature metrics measured in M frequency regions to detect characteristics that are outside expected bounds
  - For an algorithmically determined confidence level, the part is deemed real or suspicious
  - Testing with a reference part typically takes between 5 seconds, although longer scan times are possible to allow for additional confidence and signal processing

6. Classification when a reference part is unavailable

- N signatures are measured for each device under test using the same inputs
- Signature metrics for each part are extracted in each frequency region
- The operator can perform qualitative and/or quantitative analysis on extracted metrics and raw emission signature data
- High fidelity data acquisition (1 Hz RBW scan from 30 MHz – 1 GHz) typically requires ~ 1 hr per scanned component
- Once frequency regions of interest have been identified, scan time can be reduced to under 5 minutes per part

Classification can be performed by comparing the device under test to a reference part, or to a set of logged parts if no references are available. In the case where references are available, their signatures must be established before the operator can proceed. Once these have been logged in the system, the operator loads the suspected counterfeit device into the test chamber and selects the expected identity of the part from a list of previously tested parts. Classification proceeds by comparing spectral features from the device under test (DUT) to those of known authentic or golden part to determine whether the DUT is or is not a match. This can be accomplished using computer-based machine learning algorithms, or by inspection by a trained operator. Based on communications with Nokomis, they are in the process of developing an artificial neural network (ANN)-based classification algorithm to automate the training and classification operations. At present, the classification operation is largely performed by a trained human operator, which substantially increases the time required for the training process, increases variability, and requires an operator with specialized training. This reduces the suitability of the current system for deployment to end-use locations such as supply/maintenance depots or other installations where throughput is a high priority and highly trained technical personnel may not be available.

Consider a situation where the signatures of several authentic integrated circuits are stored in the system. If the operator has a part which he believes to be of the same manufacturer, date/lot code, etc. as one of the stored circuits, and he has a test board available that was used previously to scan the reference

parts, he can load the circuit under test into the chamber, select the second circuit from the menu, and begin the scan. The ADEC system will deliver a result of the scan within approximately five seconds.

When a reference part is unavailable, an operator can indicate this set of circumstances in the user interface and the classification takes the form of clustering. However, in this circumstance a test board that is suitable for use with the part may be unavailable, unless the part package and I/O layout corresponds to a common configuration that was previously tested. In the absence of a test board, based on Nokomis's responses to CALCE's inquiries concerning the blind study, it may require several weeks to develop the capability to test any of the parts. Another of the potential drawbacks with the Nokomis system is the amount of time it can to analyze the electromagnetic spectrum of an electronic device using ADEC in the absence of known-authentic reference samples. In communications with Nokomis it was learned that classification of such devices can take significantly longer than the process using reference parts. This was independently verified by Nokomis as reflected in the process steps listed above.

For the purposes of the Technology Readiness Level assessment, the Critical Technology Element (CTE) that was the basis for assessment was the hardware used to extract the REME signals from the DUT, marketed as the Nokomis ADEC system. The main components of this system are an electromagnetic isolation chamber in the form of a gigahertz transverse electromagnetic (GTEM) cell containing an RF sensor, and a measurement unit for collecting, processing, and analyzing the signals in the range of 30 MHz to 3 GHz.

The NASA TRL worksheet was used for the initial assessment and has been reproduced in Appendix 1. In addressing the requirements for the TRL assessment, the following assumptions or observations affected the assessment:

Scaling requirements are assumed to have been defined but do not conform to end use requirements across DoD. Modeling and Simulation are assumed to have been performed under some operating conditions, but not necessarily across the full range of relevant operating environments for end use deployment. Operating environment is assumed to have been defined but is not adequate in terms of range of environmental conditions and associated reliability and measurement accuracy, and therefore not final. Modeling and Simulation assumed to have been performed under some operating conditions, but not necessarily across the complete range of relevant operating environments.

It is noteworthy that in June 2013, during a public meeting hosted by DoD for discussion of DFARS Case 2012-D055, Nokomis made a presentation on the ADEC system and stated "ADEC should be a

requirement for a DoD-approved operational system to detect and avoid counterfeit parts."[11] For more discussion of this presentation and the context surrounding it, see Section VIII-A-2-a of this report.

A table with additional questions concerning Nokomis's ADEC system was sent to Dr. Walter Keller, the CEO of Nokomis, by email but was returned without any entries having been completed. Dr. Keller stated in the email, dated Dec. 4, 2020, that he believed the TRL of the ADEC system was 9, and he provided the following statement as justification for this: "It is used for counterfeit detection and as a general diagnostics tool. It is used to assess and analyze operational electronic parts on a daily basis at several sites." Based on information obtained from the literature and publicly available sources, and through other communications with Nokomis personnel, the following additional information was considered:

Table 8. Additional Information About Nokomis

Question	Answer
How many units have been manufactured?	Not known exactly, but most or all systems have been deployed largely to research laboratories, as opposed to end-use locations.
Are units in stock or are they built against order?	It is presumed that they are made to order.
Do the units include software and database? Do the users have to subscribe for getting those features?	Software is provided with the hardware. Nokomis has a database of over 100 parts. Signature files come with the system if it is purchased in Automated Test configuration.
Do you have a product data sheet?	A datasheet, is provided on the Nokomis website.
Do you offer support service?	It is doubtful that the current system can be deployed without support from Nokomis. Nokomis offers services for additional signature file development.
Do you offer repair or upgrades?	This is not known.
What is the lead time to buy one?	This is not known.
What is the price of the unit?	This is not publicly available, although the nature of the hardware alone suggests that it is expected to cost well in excess of $100,000.
What are you selling to customers?	Hardware and software system, although software is most likely licensed rather than sold outright. Systems are available for procurement by the public. Nokomis has a sales team exclusively focused on commercial (non-defense) applications of the system.
Are the units built outside of the company?	Production facilities are not known.

[11] B. Pathak and G. Johnson, "Advanced Detection of Electronic Counterfeits (ADEC); DFARS Case 2012-D055, Detection and Avoidance of Counterfeit Electronic Parts," June 28, 2013, available online at https://www.acq.osd.mil/dpap/dars/publicmeeting/presentations/Nokomis_Presentation.pdf.

Participation in the blind study: Nokomis initially indicated an eagerness to participate in the blind study, when approached in December 2019. Subsequent attempts to obtain agreement to proceed with the blind study resulted in delays and obfuscation. Ultimately, Nokomis did not provide any test results for the blind study. A more complete description of the interaction with Nokomis regarding the blind study, and a statement by their CEO explaining why they did not participate, may be found in Section IVIV. B. of this report.

Nokomis's poor and uneven responsiveness to the opportunity for their technology and capabilities to be represented in the report through the blind study raises doubts about their confidence in the accuracy of their results. Independent discussions with subject matter experts (including Dr. Brian Cohen, cited in Section VIII, and personnel from ASSESS/JFAC) indicate a perception that the technology and the hardware system on which it is deployed continue to have drawbacks in terms of throughput and accuracy, and is not suitable for widespread deployment in its current state of development.

Based on the inputs to the NASA TRL Calculator, a TRL of 4 has been fully achieved by the Nokomis ADEC system, with a partial TRL of 6 (partially satisfied, or Yellow Level). It was found that the supplemental information listed above did not modify this assessment. Therefore, the final TRL was assessed to be 4.

3. Sandia PSA

Power spectrum analysis (PSA) measures the dynamic frequency-domain responses of ICs or electronic parts such as capacitors when subjected to a dynamic stimulus. Due to the non-linear aspects of the component's response and its inherent complexity, unique PSA signatures exist in the power spectrum associated with each IC. These signatures can be sensitive to very subtle changes, not detectable with conventional electrical testing. Hence, the PSA method may detect subtle differences in ICs and aid in the detection of counterfeits. PSA is a comparative technique that compares such signatures between components. "Unknown" PSA signatures are compared to the reference created earlier to detect differences. Counterfeit devices are likely to have distinct PSA signatures that allow differentiation from the "real" ICs. Sandia reports that PSA has been used to detect changes resulting from different manufacturers, different features (e.g., memory sizes), changes in processing, different foundries, and different functionalities.

Since Sandia is a federal-funded lab, it is not allowed to manufacture or sell the units. There are plans to commercialize PSA with outside companies; the outside companies can license PSA, make their branded PSA products, and sell PSA services.

a. **Basic information on the developers and technology:**

- **Location:** Albuquerque, New Mexico. Sandia National Laboratories consists of two laboratories: the main one is in Albuquerque, with the second one in Livermore, California.
- **Leadership:** Lab Director: Dr. James Peery;
- **The size and portability of the method or device**: The system can be made portable if a laptop computer is used. All the instruments can fit in a cart of size 2 ft×4 ft. Figure 4 shows a typical PSA system with a desktop computer.
- **Cost for the product**: A typical system costs about 50,000 US Dollars.
- **Resources and infrastructure required for testing**: A PSA system includes a spectrum analyzer, function generator, and oscilloscope. PSA system also includes an in-house Labview Data Acquisition program.
- **Preparations needed before testing can be performed**: The user needs a PSA board with the right socket for the parts. Information needed includes the pin layout of the part, including the pin locations of power and ground pins, and the part's normal operating voltage. Before PSA measurements, all the instruments (spectrum analyzer, function generator, and oscilloscope) need to warm up for at least 20 to 30 minutes.
- **Numbers of samples needed**: Sandia requires a few samples to develop test procedures (biasing conditions and spectral ranges) and identify features of interest that are specific to the device.
- **The skill level and training of personnel required to operate equipment, to analyze data, and to interpret results**: Individuals can be trained on the basics of PSA data acquisition and measurements within one or two hours. It requires several days of training to develop the test procedures, analyze data, and interpret results.

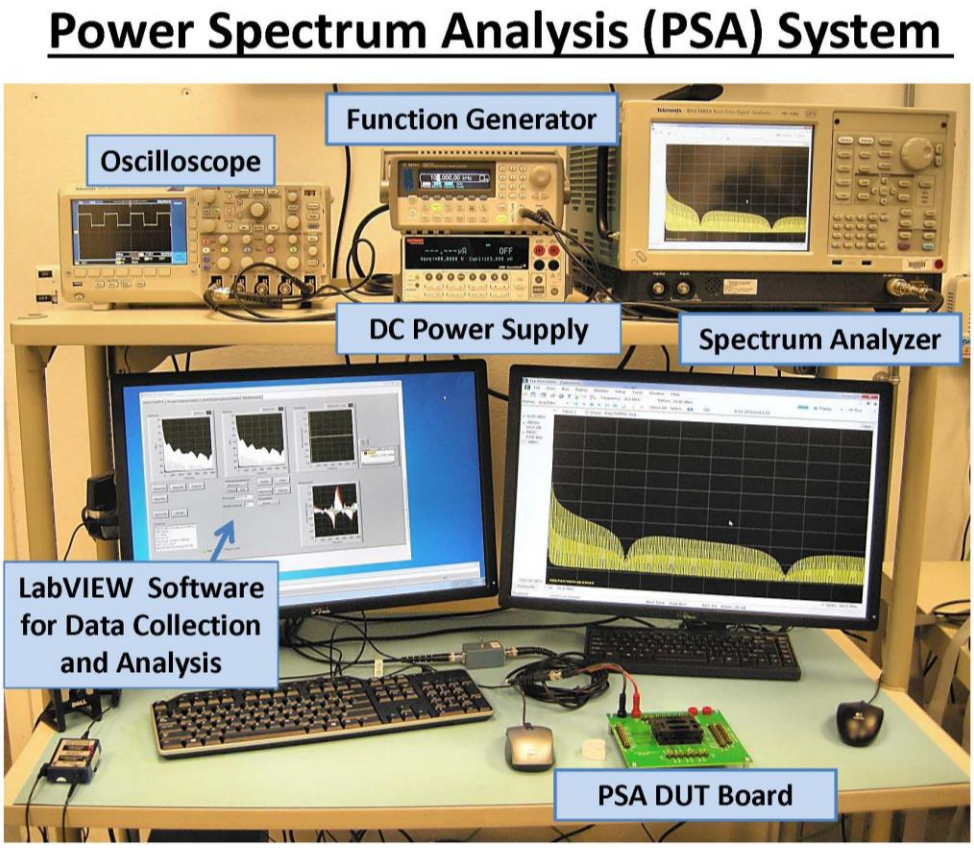


Figure 4: PSA System with Required Accessories

Steps in use of the PSA System:

1. A part is loaded into the system
2. The part is stimulated with an off-normal biasing, and a raw PSA spectrum (amplitude-versus-frequency plot) is recorded using a spectrum analyzer.
3. A normalized PSA spectrum is then generated before any data analysis. A normalized PSA spectrum is generated by dividing the raw PSA spectrum of a test sample by that of a reference.
4. Principal Component Analysis (PCA) is then used to analyze the data from a group of samples. PCA distribution is then generated to differentiate the samples from the group. PCA is then to determine the authenticity of the component and returns a verdict to the user.

In the stimulation step, a PSA system's function generator applies a repetitive AC voltage (usually a square-waveform voltage) to the device to produce a unique power spectrum. This stimulus is usually applied between the power and ground pins, with all other pins floating. A spectrum analyzer is connected to the device and function generator. The spectrum analyzer provides a real-time Fourier transform of the device's voltage signals, generating a PSA spectrum (amplitude versus frequency) used for classification.

The classification process depends on the availability of reference parts. If a reference part is available, principal component analysis is performed on both the reference and test signatures. The principal components with the three largest eigenvalues are plotted in three-dimensional space, and the system then performs a calculation to determine if the tested device is authentic using a user-selected threshold and the normal distribution. If a reference is unavailable, a large group of parts can be categorized based on their PSA signatures. In this case, each part or a representative, random sample of the parts must be logged in the PSA system. The responses from the parts are then graphed in three-dimensional space using the same method. Any further devices can be logged, and the system determines whether the part is similar to a part already logged or it belongs to a new category. A part that is put into a new category is reported as anomalous.

Table 9: Parts Evaluated by the Sandia System

Functionality	Package Type	Part Number	Tests Performed
Microcontroller	DIP	P89V51RD2FN (NXP) P89V51RC2FN (NXP) P89V51RB2FN (NXP) 89C51RC2-UM (ATMEL)	Discrimination between two manufacturers Detection of different memory size and/or different date codes from the same manufacturer
Operational Amplifier	SOIC	LF351 (ST Microelectronics, ON Semiconductor, TI)	Discrimination between three manufacturers
Temperature sensor (Analog)	SC70	LM20 (ST Microelectronics, TI, National Semiconductors)	Discrimination between manufacturers
Zener diode	SOD	MMSZ5239B1G (ON Semiconductor)	Detect the effects of aging (bake 500-3000 hours at 140℃)
FPGA	TQFP	XC4008E	General authenticity
Voltage Reference	SOIC	LM385 (National Semiconductor, TI, On Semiconductor)	Discrimination between manufacturers
Static RAM	SOJ	IDT71V016SA10Y	Differentiation of different date codes
Sandia-manufactured ASIC	BGA		Differentiation between different wafer lots and different packaging

b. **Patents:**

- P. Tangyunyong, E. Cole, Jr. and D. Stein, "Power Spectrum Analysis for Defect Screening in Integrated Circuit Devices," United States of America Patent US 9,188,622 B1, 17 November 2015.
- P. Tanyunyong, E. Cole, Jr., G. Loubriel and J. Beutler, "Scanning Method for Screening of Electronic Devices," United States of America Patent US 10,094,874 B1, 9 October 2018.
- P. Tanyunyong, J. Beutler, E. Cole, Jr., and G. Loubriel, "Defect Screening Method for Electronic Circuit and Circuit Components Using Power Spectrum Analysis," Patent US 10,145,894 B1, December 4, 2018.

c. **Presentations:**

- G. Loubriel and P. Tangyunyong, "Power Spectrum Analysis (PSA) for Counterfeit Electronics," in CALCE/SMTA Symposium for Counterfeit Parts and Materials, College Park, MD, 2017. P. Tangyunyong, E. Cole Jr, G. Loubriel, J. Beutler, D. Udoni, B. Paskaleva and T. Buchheit, "Power Spectrum Analysis (PSA)," in 43rd International Symposium for Testing and Failure Analysis, Pasadena, 2017.
- P. Tangyunyong, D. M. Udoni, and G. M. Loubriel, "Various Applications of Power Spectrum Analysis (PSA)," Proceedings of GOMACTech 2017, Reno, Nevada, March 2017.
- P. Tangyunyong, B. Paskaleva, D. M. Udoni, T. E. Buchheit, G. M. Loubriel, R. W. Stinnett, and E. I. Cole, Jr., "Aging Detection in Zener Diodes Using Power Spectrum Analysis (PSA)," Proceedings of GOMACTech 2016, Orlando, Florida , March 2016.
- P. Tangyunyong, E. I. Cole, Jr., G. M. Loubriel, and J. Beutler, "Counterfeit Detection Using Power Spectrum Analysis (PSA)," Proceedings of GOMACTech 2015, St. Louis, Missouri, March 2015.

d. **Articles:**

- P. Tangyunyong, E.I. Cole, G.M. Loubriel, J. Beutler, D.M. Udoni, B.S. Paskaleva, et al., "Power Spectrum Analysis (PSA)", Proc. From the 43rd International Symposium for Testing and Failure Analysis, pp. 73-78, 2017.
- E. Cole Jr., et al., "Transient Power Supply Voltage (V DDT) Analysis for Detecting IC Defects," in 2013 IEEE International Test Conference (ITC), Washington D.C., 1997 pp. 23. doi: 10.1109/TEST.1997.639590

Additional information regarding the status of the product is provided in Table 10. The information presented in the table is obtained by direct communication and from the publicly available literature.

Table 10: Additional Information About Sandia

Question	Answer
How many units are manufactured?	Less than 10
Are units in stock or are they built against order?	Since the product has not been commercialized, Sandia will provide an equipment list to customers. The customers usually assemble the system themselves; Sandia can also help with the assembly if needed.
Do the units include software and database? Do the users have to subscribe for getting those features?	The data acquisition program is provided to customers. Since the product has not been commercialized, the decisions about database and subscription are not yet made.
Do you have a product data sheet?	There seems to be no public datasheet; however, some general system information is provided via direct communication.
Do you offer a support service?	Since the product is not commercialized, these decisions are not yet made, and information is not available.
Do you offer repair or upgrades?	
What is the lead time to buy one?	
What are you selling to customers?	
What is the price of the unit?	Estimate: about USD 50,000.
Are the units built outside of the company?	For internal use at Sandia, the systems are assembled in house. For outside customers, Sandia provides an equipment list to the customers. The customers usually assemble the system themselves; Sandia can also help with the assembly if needed.

For this assessment, the process of generating and gathering the raw PSA spectrum (amplitude-versus-frequency plot) is considered as the Critical Technology Element (CTE). The TRA is performed for this CTE. Only hardware (and aspects of manufacturing) was considered for the assessment. It is found that the system has achieved TRL of 4 completely and has met some aspects of TRL 5.

At this point, the process of working with Sandia National Laboratory is and time-consuming. Unlike private organizations, they cannot start working unless a contract is in place, and payment is made for the services. The process could not be completed in more than seven weeks. As a result, despite the best efforts by CALCE and the technical contact at Sandia, no results are obtained at the time of this TRL assessment. If data is obtained before the closing time for the report finalization, those will be provided to DMEA. Sandia had been cooperative and provided and reviewed information for this assessment without delay or reservation.

4. PFP Cybersecurity

Power fingerprinting (PFP) is an approach that utilizes physical Side Channels to assess the integrity of an electronic device. Side Channels are those physical measurements that can be made from outside the specific component, but which contain information about the execution status of the target. For instance, features such as power consumption or electromagnetic emissions are Side Channels intrinsic to device operation. Side Channels, such as power consumption and electromagnetic emissions, depend on the circuit layout, semiconductor technology, and manufacturing process.

PFP is effective across the full execution stack, from hardware to firmware to software and is independent of platform and application. PFP is capable of detecting, with extreme accuracy, when unauthorized modifications, such as hardware Trojans or counterfeit parts, have compromised the integrity of an electronic system. PFP provides dynamic verification of hardware systems and a non-destructive process for tamper and intrusion detection at the supply chain.

PFP performs anomaly detection on the device's Side Channels to determine whether it has deviated from expected operation. A PFP monitoring setup uses a physical sensor to capture the fine grained Side Channel signals, which contain tiny patterns that emerge during operation that are unique to the hardware and software executing within the device. Also, PFP can be performed much faster compared to other inspection approaches, since PFP can observe and perform its analysis in parallel with routine functional testing. PFP has been shown effective in a variety of chips, devices and platforms to assess the execution integrity of hardware and firmware.

a. Basic information on the developers and technology:

- **Location:** Vienna, VA 22182
- **Leadership:** Carlos Aguayo Gonzalez, CEO, Stephen Chen, CTO
- **The size and portability of the method or device**: NA
- **Cost for the product**: scalable – 100K to higher
- **Resources and infrastructure required for testing**: appropriate electrical tools including benchtop test equipment, data acquisition computer and internet connection
- **Preparations needed before testing can be performed**: development of fixture and test board
- **Numbers of samples needed**: the system can work with few samples
- **The skill level and training of personnel required to operate equipment, to analyze data, and to interpret results**: Individuals can be trained on data acquisition and measurements within a few days. Data analysis is automated.

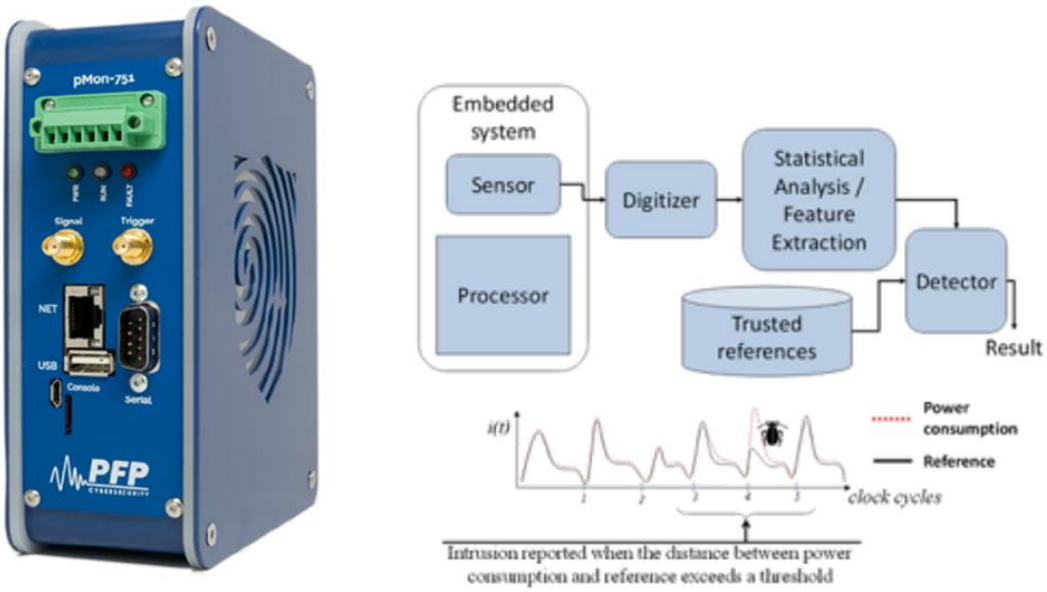


Figure 5: Schematic of the PFP System

Steps in use of the PFP System:

1. A part is loaded into the system
2. The PFP system monitors the dynamic power consumption of the suspect device while running a known software module
3. The current drain is measured throughout the execution of the code
4. This process is repeated many times to establish a "fingerprint"
5. After establishing the fingerprint, the same device is continuously monitored, reporting any anomalous activity by way of deviations in the system's power consumption

Table 11: Parts Evaluated by the PFP System (from Company Literature)

Functionality	Package Type	Part Number	Tests Performed
Flash memory		Intel TB28F400B5JT80	Counterfeit detection
FPGA		Xilinx	Classification by aging
FPGA		Xilinx	Simulated "tamper" detection
FPGA		Xilinx XC3S500E	Consistency validation
Circuit boards			Detection of changes in the firmware
EEPROM	28 pin SOIC	AT28C256-15SU AT28HC256-90SU	Differentiation between grades of parts

b. **Patents:**

- C. Aguayo Gonzalez, "Using Power Fingerprinting to Monitor the Integrity and Enhance Security of Computer Based Systems," United States Patent 9,262,632 B2, Feb. 16, 2016

c. **Articles:**

- C. Aguayo Gonzalez, "Power Fingerprinting for Integrity Assessment of Embedded Systems," PhD Dissertation, Virginia Polytechnic Institute, Blacksburg VA, 2011.
- C. Aguayo Gonzalez, "Power Fingerprinting in SDR and CR Integrity Assessment," in Proceedings of MILCOM 2009: 2009 IEEE Military Communications Conference, October 18-21, 2009, Boston, MA [Online]. Available: https://ieeexplore.ieee.org/document/5379826

Additional information regarding the status of the product is provided in Table 12. The information presented in the table is obtained by direct communication and from the publicly available literature.

Table 12: Additional Information About PFP Cybersecurity

Question	Answer
How many units are manufactured?	NA
Are units in stock or are they built against order?	NA
Do the units include software and database? Do the users have to subscribe for getting those features?	The software is included with the system and can be implemented for cloud or in-premise access.
Do you have a product data sheet?	There is a product datasheet, and some general system information is provided via direct communication and through the web site.
Do you offer support service?	Yes
Do you offer repair or upgrades?	Yes
What is the lead time to buy one?	Same as the time to assess the requirement of the customer
What are you selling to customers?	Integrated implementation (if needed sockets and fixtures)
What is the price of the unit?	It depends on the complexity of implementation.
Are the units built outside of the company?	NA

For this assessment, the PFP Analytics Software is the Critical Technology Element (CTE) and the TRA is performed for this CTE. Only software was considered for the assessment. The system has achieved TRL of 5 and has met some aspects above that.

At the time of this assessment, only one part result is available, and the classification feature between the two sets of parts is not well defined, and it is open to interpretation. We determine that the accuracy is low and is below 70%. The organization is small and had difficulty providing necessary logistics information but had been forthcoming with information about the technology.

5. Summary of TRL Analysis of Side Channel Technologies

Table 13: TRL Summary (Side-Channel)

Company	Critical Technology Element	Focus of Assessment	TRL Complete (Partial)
Battelle	Barricade hardware system used to test device and collect data as well as the software algorithm which performs classification	Hardware Software	4 – (up to 8) 5 – (up to 8)
Nokomis	ADEC Hardware for electromagnetic signal capture	Hardware	4 – (up to 6)
Sandia	The process of generating and gathering the raw power spectrum (amplitude-versus-frequency plot)	Hardware	4 – (up to 5)
PFP	PFP analytics software	Software	4 – (up to 7)

B. Task 1b: Evaluation of Effectiveness of Existing Systems via Blind Study with Known Clones (Side-Channel, Image Analysis, and Conventional Testing)

CALCE planned and led a blind study to assess the effectiveness of each of the counterfeit detection systems with respect to the identification of suspect counterfeit parts from among a mixed lot of authentic and counterfeit parts, or in some cases, to distinguish these two groups from each other without specifically indicating which group was suspect counterfeit. CALCE enlisted the support of SMT Corporation as the Subject Matter Expert (SME) regarding advanced counterfeit components and clones, to provide the parts required for the study, and to provide reference test reports that serve as the basis for evaluation of the counterfeit detection systems that were the subject of the study. At the commencement of the study, SMT already had all the counterfeit parts that were needed for the study in their possession. They procured corresponding parts with identical part numbers from well-known and respected distributors. Using a combination of AS6171-based testing and part information analysis, SMT generated convincing evidence that the recently procured parts were authentic. SMT produced a complete test report, following AS6171, for both the parts in their inventory and the recently procured parts, for all 11 part numbers. These test reports are provided in Appendix 3.

The parts that SMT shipped to each participating organization were packaged individually in boxes labeled only with an alphanumeric serial number that was assigned to each part by SMT. While testing was being performed, only SMT was aware of which parts were counterfeit and which were authentic. This

blinding applied to all study partner organizations, including CALCE. Only after testing at CALCE had been completed and documented was CALCE unblinded for the purpose of evaluating the results.

1. Part Selection for the Blind Study

SMT Corporation had shared with the project team two master lists of counterfeit parts from their inventory, along with some additional information identifying the parts. One list was for "cloned" parts and the other list was for traditional (i.e., conventional, non-clone) counterfeit parts. CALCE performed a down-select from the list based on the following initial criteria:

1. For the cloned parts, the selection was based on number of parts available in the stock of SMT Corporation and only the parts with more than fifty in inventory were considered for down selection. This list included 34 parts.
2. For the traditional counterfeit parts, the criterion was to select more complex (in functionality and in package type) parts. One other additional factor was to include Xilinx FPGAs from the Spartan family. This list included 15 parts.

The following criteria were used in the selection:

1. Diversity of functionality
2. Diversity of package type
3. Availability of "known good" parts
4. Availability of test reports

Eleven part numbers were selected for the study, having a variety of packaging styles, functions, and OCMs. The eleven part numbers included eight for which clones were available and three for which conventional counterfeits were available in SMT's inventory. SMT procured additional parts of each part number from reliable sources that were presumed to be authentic, and subsequently evaluated these parts through unblinded testing in order to verify that they were not suspect counterfeit. The parts used in the study and related information are provided in Appendix 2. This Appendix contains a summary of available part information, the first page of relevant datasheets, materials declaration forms, and GIDEP and ERAI reports (primarily reporting counterfeit parts).

The first eight parts in the list are cloned counterfeits and the next three are conventional counterfeits.

Table 14. Parts Used for Blind Study;

Note: Date Codes were redacted in order to preserve the opportunity to conduct further studies with these parts

Part Number	Manufacturer	Package Type	Date Code: Authentic	Date Code: Counterfeit
Clones – advanced counterfeits				
LM324N	TI	DIP-14	■■■■	(■■■■) not clearly marked
SG3525AN	ST MICRO	DIP-16	■■■■	■■■■
OP07CP	TI	DIP-8	■■■■	■■■■
CD4093BM	TI	SOIC-14	■■■■	■■■■
MAX232ESE+	MAXIM	SOIC-16	■■■■	■■■■
EPCS4SI8N	ALTERA	SOIC-8	■■■■	■■■■
MC34063	ON SEMI	SOIC-8	■■■■	■■■■
LM317T	ST MICRO	TO-220	■■■■	■■■■
Traditional – basic counterfeits				
IDT71215S10PF	IDT	TQFP	■■■■	■■■■
XC3S200AN-4FTG256C	XILINX	FTBGA	■■■■	■■■■
XC3030A-7PC84C	XILINX	LCC	■■■■	■■■■

2. Summary of participation in the blind study

Three categories of counterfeit detection technology were evaluated in the blind study: conventional testing (CT), following methods described in standards such as SAE AS6171; Side Channel (SC); and Image Analysis-based imaging (IA). A list of the study partner organizations and a summary of their participation in the blind study is provided in Table 15.

Table 15. Summary of Company Participation in the Blind Study

Company	Parts Tested	Summary
SMT Corp. (CT)	Tested all 11 part numbers (counterfeit and authentic)	Test reports were received on all 11 part numbers. (See Appendix 3). These reports serve as the reference for evaluating the counterfeit detection methods investigated in the blind study. SMT also provided all the parts for the blind study, and performed the shipping and tracking of parts to all partner companies.

Company	Parts Tested	Summary
Integra (CT)	Five part numbers (20 parts each) SG3525AN EPCS4SI8N LM317T IDT71215S10PF XC3S200AN-4FTG256C	Test reports were received on all 5 part numbers. (See Appendix 5)
Micross (CT)	Agreed to test 5 part numbers (20 parts each) SG3525AN EPCS4SI8N LM317T IDT71215S10PF XC3S200AN-4FTG256C	Test report was received on part SG3525AN. (See Appendix 6)
CALCE (CT)	Five part numbers (20 parts each) SG3525AN EPCS4SI8N LM317T IDT71215S10PF XC3S200AN-4FTG256C	Test reports were received for all 5 part numbers. (See Appendix 7)
Alitheon (IA)	Registered all 11 part numbers (10 parts each) Authenticated six part numbers (20 parts each) LM317T SG3525AN LM324N CD4093BM MAX232ESE+ EPCS4SI8N	Test reports were received for 6 part numbers. (See Appendix 14)

Company	Parts Tested	Summary
Covisus (IA)	Registered six part numbers (10 parts each) SG3525AN EPCS4SI8N CD4093BM LM317T XC3S200AN-4FTG256C XC3030A-7PC84C	Registration test reports were received for all 6 part numbers. (See Appendix 15)
Creative Electron (IA)	Registered all 11 part numbers (10 parts each) Authenticated six part numbers (20 parts each) LM317T SG3525AN LM324N CD4093BM MAX232ESE+ EPCS4SI8N	Test reports were received for 6 part numbers. (See Appendix 16)
Battelle (SC)	Tested eight clones (20 parts each) LM324N SG3525AN OP07CP CD4093BM MAX232ESE+ EPCS4SI8N MC34063 LM317T	Test reports were received for all 8 part numbers. (See Appendix 9)
Nokomis (SC)	Agreed to test 6 part numbers (20 parts each) OP07CP CD4093BM MAX232ESE+ EPCS4SI8N IDT71215S10PF XC3030A-7PC84C	Failed to deliver any reports. (See below and Appendix 10)

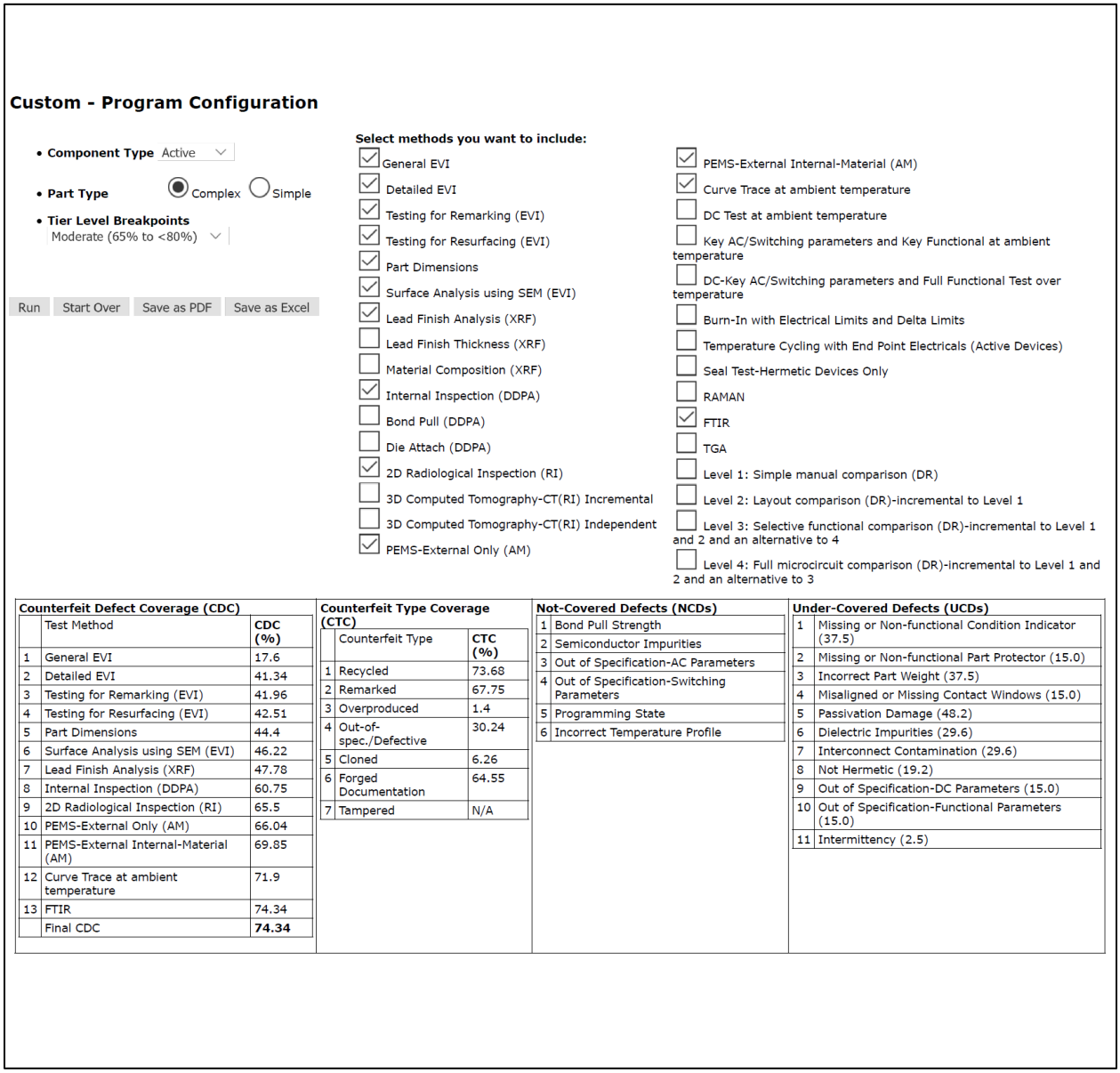
Company	Parts Tested	Summary
Sandia (SC)	Agreed to test 6 part numbers (20 parts each) LM324N SG3525AN OP07CP EPCS4SI8N MC34063 XC3S200AN-4FTG256C	Test report was received for part LM324N, SG3525AN, OP07CP, EPCS4SI8N, MC34063, XC3S200AN-4FTG256C. (See Appendix 11 and Appendix 11A)
PFP (SC)	Agreed to test 6 part numbers (20 parts each) SG2525 LM317 CD4093BM EPCS4SI8N XC3S200AN-4FTG256C XC3030A-7PC84C	Test reports were received for parts LM317, CD4093BM, EPCS4SI8N, SG2525 (See Appendix 12 and Appendix 12A)

3. Conventional Testing

Three laboratories performed testing for the blind study using conventional test methods described in AS6171. The conventional testing portion of the blind study was designed to include five of the eleven part numbers listed above. This testing was governed by a statement of work which is found in Appendix 4 and was provided to each test lab in advance of their receipt of parts for testing. As testing progressed, some modifications to the original plan were found to be necessary as a result of the need for CALCE to receive test reports in time to meet the deadline for submission of the final report. The parts selected for use for conventional testing were as follows:

Part Number	Manufacturer
Clones	
SG3525AN	ST MICRO
EPCS4SI8N	ALTERA
LM317T	ST MICRO
Traditional	
IDT71215S10PF	IDT
XC3S200AN-4FTG256C	XILINX

An analysis was performed, using the SAE CDC web-based tool[12], of the Counterfeit Defect Coverage (CDC) and Counterfeit Type Coverage (CTC) expected for the sequence of tests performed for the Blind Study using conventional testing. The results are provided in Figure 6.



Custom - Program Configuration

- **Component Type** Active
- **Part Type** Complex / Simple
- **Tier Level Breakpoints** Moderate (65% to <80%)

Run | Start Over | Save as PDF | Save as Excel

Select methods you want to include:

- [x] General EVI
- [x] Detailed EVI
- [x] Testing for Remarking (EVI)
- [x] Testing for Resurfacing (EVI)
- [x] Part Dimensions
- [x] Surface Analysis using SEM (EVI)
- [x] Lead Finish Analysis (XRF)
- [ ] Lead Finish Thickness (XRF)
- [ ] Material Composition (XRF)
- [x] Internal Inspection (DDPA)
- [ ] Bond Pull (DDPA)
- [ ] Die Attach (DDPA)
- [x] 2D Radiological Inspection (RI)
- [ ] 3D Computed Tomography-CT(RI) Incremental
- [ ] 3D Computed Tomography-CT(RI) Independent
- [x] PEMS-External Only (AM)
- [x] PEMS-External Internal-Material (AM)
- [x] Curve Trace at ambient temperature
- [ ] DC Test at ambient temperature
- [ ] Key AC/Switching parameters and Key Functional at ambient temperature
- [ ] DC-Key AC/Switching parameters and Full Functional Test over temperature
- [ ] Burn-In with Electrical Limits and Delta Limits
- [ ] Temperature Cycling with End Point Electricals (Active Devices)
- [ ] Seal Test-Hermetic Devices Only
- [ ] RAMAN
- [x] FTIR
- [ ] TGA
- [ ] Level 1: Simple manual comparison (DR)
- [ ] Level 2: Layout comparison (DR)-incremental to Level 1
- [ ] Level 3: Selective functional comparison (DR)-incremental to Level 1 and 2 and an alternative to 4
- [ ] Level 4: Full microcircuit comparison (DR)-incremental to Level 1 and 2 and an alternative to 3

Counterfeit Defect Coverage (CDC)

	Test Method	CDC (%)
1	General EVI	17.6
2	Detailed EVI	41.34
3	Testing for Remarking (EVI)	41.96
4	Testing for Resurfacing (EVI)	42.51
5	Part Dimensions	44.4
6	Surface Analysis using SEM (EVI)	46.22
7	Lead Finish Analysis (XRF)	47.78
8	Internal Inspection (DDPA)	60.75
9	2D Radiological Inspection (RI)	65.5
10	PEMS-External Only (AM)	66.04
11	PEMS-External Internal-Material (AM)	69.85
12	Curve Trace at ambient temperature	71.9
13	FTIR	74.34
	Final CDC	**74.34**

Counterfeit Type Coverage (CTC)

	Counterfeit Type	CTC (%)
1	Recycled	73.68
2	Remarked	67.75
3	Overproduced	1.4
4	Out-of-spec./Defective	30.24
5	Cloned	6.26
6	Forged Documentation	64.55
7	Tampered	N/A

Not-Covered Defects (NCDs)

1	Bond Pull Strength
2	Semiconductor Impurities
3	Out of Specification-AC Parameters
4	Out of Specification-Switching Parameters
5	Programming State
6	Incorrect Temperature Profile

Under-Covered Defects (UCDs)

1	Missing or Non-functional Condition Indicator (37.5)
2	Missing or Non-functional Part Protector (15.0)
3	Incorrect Part Weight (37.5)
4	Misaligned or Missing Contact Windows (15.0)
5	Passivation Damage (48.2)
6	Dielectric Impurities (29.6)
7	Interconnect Contamination (29.6)
8	Not Hermetic (19.2)
9	Out of Specification-DC Parameters (15.0)
10	Out of Specification-Functional Parameters (15.0)
11	Intermittency (2.5)

Figure 6. Analysis of Conventional Test Sequence for Blind Study using SAE CDC Tool.

A summary and analysis of the results received for conventional testing are as follows:

[12] http://cdctool.sae.org/

a. **Integra Technologies:**

The Integra test reports are in Appendix 5. Integra also documented all of the counterfeit defects (based on SAE AS6171/1) that were observed for each test method on a part by part basis, for all five part numbers. Sample defect spreadsheets for two part numbers have been included in Appendix 5. One of those defect spreadsheets is for part number EPCS4SI8N, which is a clone. The other spreadsheet is for part number IDT71215S10PF, which is a conventional counterfeit part.

Integra successfully identified inconsistencies between counterfeit and authentic parts for all five part numbers. On this basis alone, each of these groups of 20 parts would be considered a mixed lot rather than a homogeneous lot, thus correctly raising a red flag concerning their use.

In the absence of an exemplar, conventional test labs were not obligated to identify the specific parts that were suspect counterfeit, although they were encouraged to attempt that identification. The criteria for this type of identification include a combination of observable defects and comparison to available part information. Integra correctly identified the suspect counterfeit parts for part numbers IDT71215S10PF and LM317T. They did not correctly identify the suspect counterfeit parts for part numbers SG3525AN and XC3S200AN-4FTG256C. For the EPCS4SI8N, they did not attempt to identify the counterfeit parts. For each part number, however, their identification of inconsistencies within each group correctly provided the necessary warning against the use of those parts without further attempts to authenticate them.

b. **Micross:**

The Micross test report on part number SG3525AN is in Appendix 6. Similarly to Integra, Micross successfully identified inconsistencies between counterfeit and authentic parts and some defects associated with the suspect parts. They did not attempt to identify which specific parts were suspect counterfeit.

c. **CALCE:**

CALCE's test reports are in Appendix 7. CALCE successfully identified inconsistencies between counterfeit and authentic parts and defects associated with the suspect parts for all five part numbers. Despite the absence of an exemplar for any of the part numbers, CALCE attempted an identification of which specific parts within each group were suspect counterfeit. The criteria for this type of identification include a combination of observable defects and comparison to available part information. CALCE successfully identified the correct suspect counterfeit parts within each group for all five part numbers.

d. **Observations and conclusions regarding the conventional testing portion of the blind study:**

The original test sequence for the conventional testing provides just under 75% Counterfeit Defect Coverage, based on the analysis performed using the SAE CDC Tool,[13] shown in Figure 6. This is equivalent to a moderate risk level of testing. The same analysis indicates that the Counterfeit Type Coverage for clones is expected to be only about 6%, even though the results of the study show that all labs were able to detect defects and inconsistencies associated with cloned counterfeit parts. This is evidence that defect coverage of cloned devices is higher than estimated in AS6171 and predicted by the CDC Tool. The reason is that most material and appearance-related defects are also present in the cloned devices. The counterfeit defect coverage (CDC) contained within AS6171 was based on achieving consensus among subject matter experts. These experts took a conservative approach to the estimation of CDC values, and they assumed that a clone would be manufactured to be barely distinguishable from an authentic device. Nevertheless, this study has revealed that the coverage for this counterfeit type should be re-examined.

The documentation of specific counterfeit defects provides a valuable source of information on the effectiveness of each test method, consistent with the counterfeit defect coverage analysis described in AS6171/1. It further sheds light on the coverage of counterfeit part types, since both conventional and clone counterfeits were included in this study. Prior to any revision of the counterfeit defect and counterfeit type coverages in the standards, a quantitative analysis of the data in the defect spreadsheets should be performed. The extraction of quantitative information from these spreadsheets requires extensive analysis, which should be the focus of a follow-up study based on funding availability.

This blind study provided objective, uncensored data on the effectiveness of each test method: all test methods were completed, regardless of whether a part was determined by another test method to be suspect counterfeit. These results could also indicate whether a particular sequence of tests is likely to perform more efficiently than commonly employed test sequences. For example, it is possible that performing X-ray imaging prior to external visual inspection could be more time- and cost-effective across all counterfeit types. Standards bodies should therefore examine the order of tests and make modifications to the current flow.

It was observed that the conventional testing process following AS6171 required a long time, even for professional laboratories. The two professional labs took more than four months to provide their test reports. One reason for this is that many laboratories do not have all the necessary analytical tools under

[13] http://cdctool.sae.org/

one roof for test sequences covering greater than low risk levels (per AS6171). This requires them to obtain quotes and ship parts to outside labs or other facilities for getting some of the analysis performed.

As was true in this study, in which "lots" were mixed, some physical defects may be present only on a subset of the parts in a lot. This indicates the importance of adequate sampling to ensure detection of counterfeit defects within such a mixed lot, especially for large lots. This supports the need for a sampling plan, such as that in AS6171, to go hand in hand with the selection of tests that are intended to satisfy the DFARS requirement for risk-based testing. It is useful to determine the expected part marking and material composition for each part number and date/lot code and make that available to each inspector before the beginning of the inspection. CALCE also observed that it was beneficial to review their own results of testing as they become available, rather than comparing all test results upon completion of all testing. This study also validated the need for multiple test methods that work together to provide evidence of defects and confidence in a determination that a part is or is not suspect counterfeit. For example, CALCE found that FTIR proved to be valuable for detecting conventional counterfeits, even though it is not one of the more commonly employed test methods.

Table 26 and Table 27 in the conclusions section include a summary of the results of conventional testing along with those of Side Channel and Image Analysis methods. Table 26 shows the detailed summary of results including both detection and clustering accuracy for clones and conventional counterfeits separately and combined and Table 27 shows the same with both clones and combined counterfeit parts combined.

4. Side Channel Testing

Four organizations, Battelle, Nokomis, Sandia National Laboratories, and PFP Cybersecurity, were asked to perform testing for the Blind Study using Side Channel test methods. The Side Channel testing portion of the Blind Study was designed to include all eleven part numbers listed above. This testing was governed by a statement of work which is found in Appendix 8 and was provided to each test lab in advance of their receipt of parts for testing. As testing progressed, some modifications to the original plan were found to be necessary as a result of the need for CALCE to receive test reports in time to meet the deadline for submission of the final report.

Three of the four organizations listed above (all except Nokomis) performed testing using Side Channel test methods on a subset of the eleven parts listed above. This testing was governed by a statement of work which is found in Appendix 8.

Results of the Blind Study from the organizations included in the Side Channel testing portion of the study are summarized below.

a. **Battelle:**

CALCE received Battelle's report on analysis of the eight clones listed above. The Battelle test reports are in Appendix 9. Accuracy and confusion matrices have been calculated for each of the eight parts analyzed by Battelle and are presented below.

Battelle: CD4093BM			
SN	Authentic (A) or Counterfeit (C)	**SN**	Authentic (A) or Counterfeit (C)
AC-0185	C	CC-1966	A
AQ-0570	C	DB-1572	A
BS-0877	C	DC-1285	A
CY-0347	C	JQ-1714	A
DC-0363	C	LK-1818	A
DC-0765	C	NA-1532	A
EN-0437	C	OC-1717	A
MS-0325	C	OW-2185	A
PG-0633	C	UW-1549	A
XU-0327	C	XY-1512	A

10	0		1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10		0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

Battelle: EPCS4SI8N			
SN	Authentic (A) or Counterfeit (C)	**SN**	Authentic (A) or Counterfeit (C)
CT-0399	C	DQ-1527	A
EK-1011	C	GR-1332	A
FS-0931	C	IV-1152	A
HK-0634	C	JB-1154	A
MJ-0171	C	JG-2100	A
QM-0432	C	NT-1571	A
RK-0357	C	OF-2246	A
RU-0189	C	QM-1660	A
SJ-0926	C	SD-1117	A
SQ-0050	C	VS-2283	A
WB-0459	C		
WS-0003	C		

12	0		1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10		0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

Battelle: LM317T			
SN	Authentic (A) or Counterfeit (C)	**SN**	Authentic (A) or Counterfeit (C)
DC-1046	C	BN-1203	A
DK-0907	C	GA-2260	A
FD-0039	C	IP-1935	A
HA-0532	C	IZ-1360	A
PV-0203	C	JZ-1083	A
RQ-0248	C	LT-1724	A
TX-0167	C	MM-1248	A
UN-0435	C	MR-1804	A
YZ-0616	C	QX-1690	A
ZL-0455	C	WT-1238	A

10	0		1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10		0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

Battelle: LM324N			
SN	Authentic (A) or Counterfeit (C)	**SN**	Authentic (A) or Counterfeit (C)
AN-1027	A	AA-2074	A
NA-0362	A	DQ-2227	A
NU-0065	A	EG-1150	A
PM-0283	A	IZ-1906	A
QD-0356	A	LM-2183	A
TG-0055	A	QF-2241	A
UI-0294	A	SD-2177	A
XL-0454	A	WY-2005	A
ZJ-0353	A	WY-2220	A
ZK-0974	A	YL-1654	A

0	0		0.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
10	10		1.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 0.50

Battelle: MAX232ESE+			
SN	Authentic (A) or Counterfeit (C)	**SN**	Authentic (A) or Counterfeit (C)
FA-0386	C	EM-1773	A
GW-0306	C	KT-1517	A
NZ-0511	C	LL-1811	A
OE-1072	C	LY-1447	A
PI-0125	C	ML-2293	A
PQ-0251	C	RG-2300	A
RA-0982	C	RQ-1590	A
TT-0287	C	UU-1362	A
UM-0894	C	YB-2073	A
WP-1061	C	ZH-1960	A

10	0		1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10		0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

Battelle: MC34063			
SN	Authentic (A) or Counterfeit (C)	**SN**	Authentic (A) or Counterfeit (C)
AJ-0571	C	CG-1825	A
BJ-0403	C	HC-1108	A
FG-0008	C	KV-1397	A
GU-0695	C	NM-1394	A
HV-0091	C	OG-2119	A
IW-0180	C	QS-1580	A
KE-0383	C	RY-2167	A
NP-0115	C	WZ-1122	A
UO-0182	C	XO-1755	A
WW-0998	C	ZJ-1329	A

10	0		1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10		0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

Battelle: OP07CP			
SN	Authentic (A) or Counterfeit (C)	**SN**	Authentic (A) or Counterfeit (C)
GD-0174	C	AH-1540	A
GF-0442	C	EJ-2248	A
IE-0482	C	GF-1609	A
LM-0244	C	HZ-1619	A
MU-0889	C	KB-2095	A
OH-0162	C	RM-1885	A
OP-0647	C	UW-1987	A
RB-0130	C	WX-1552	A
TK-0417	C	ZP-1218	A
ZK-0214	C	ZQ-2024	A

10	0		1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10		0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

Battelle: SG3525A			
SN	Authentic (A) or Counterfeit (C)	**SN**	Authentic (A) or Counterfeit (C)
BQ-0193	C	BW-1431	A
EC-0737	C	DL-1165	A
IG-0701	C	HJ-1858	A
KW-0212	C	HY-2092	A
LZ-0643	C	JU-1308	A
PF-0047	C	LA-145	A
VL-0870	C	ML-1181	A
VP-0097	C	QC-2153	A
WK-0857	C	VR-2166	A
XU-0583	C	VS-1652	A

10	0		1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10		0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

i. Summary of Battelle's performance in the Blind Study.

Battelle's accuracy was 100% for 7 of the 8 parts they tested. For 1 of the parts, the LM324N, they were not able to distinguish the counterfeit (clone) parts from the authentic parts, producing an accuracy of 50%. It is noteworthy that Sandia PSA was able to correctly cluster (unsupervised learning-based classification) the LM324N parts with 100% accuracy.

They are unique among the side-channel participants in stating which parts are suspect counterfeit and which are authentic. Their ability to identify suspect counterfeit and authentic parts was due to the fact that they were in possession of reference parts that they believed to be authentic. Battelle deviated from the statement of work for the blind study by procuring reference samples from two different suppliers (Digikey and Mouser; not necessarily authorized distributors) prior to testing. To the knowledge of CALCE, Battelle did not perform any further testing to verify that the reference parts were not themselves suspect counterfeit. This exposed them to a risk that their reference parts would not serve as training samples as authentic devices. Furthermore, there was no guarantee that the date codes on the reference parts

would make those parts representative of authentic parts in the Blind Study, particularly if Process Change Notices impacting electrical functionality had been issued by the OCM between the date codes of the purchased reference parts and those in the Blind Study.

In terms of their participation in the Blind Study, Battelle provided more results than any of the Side Channel participant in the Blind Study. They initially quoted nearly $5,000 per part number to perform the testing, analysis and reporting. Upon intervention by DMEA, they reduced the total cost to $10,000 for an abbreviated level of reporting and data sharing on all 11 part numbers. Ultimately, they elected to provide results on 8 parts. It may not be pure coincidence that the 8 parts they chose to test were all clones, and did not include any of the 3 conventional counterfeit parts, in view of their prior collaboration with SMT Corp. on clone detection with the Barricade system, and their possible prior experience with some of the same parts. The selection of those parts may also have simply reflected the availability of fixturing for those package types. However, for the purposes of this Blind Study, SMT and Battelle maintained an embargo on mutual communications throughout the study CALCE requested direct contact between the two organizations.

Battelle prefers to use reference parts for supervised learning-based classification, as opposed to unsupervised learning that involves clustering of parts into similar groups. The classification process is aided by the acquisition of test results using multiple test vectors for each part, which allows the use of bagging algorithms.

Battelle also participated in the "Known Good Virtual Golden Sample" demonstration (see Section VI.VI. A. 1.) and provided background information issues that could affect the use of the Barricade system for authentication when there is a span of several years between registration of golden samples and testing of unknown samples. Battelle was forthcoming about the capabilities and limitations of their technology for this application and their efforts to overcome the challenges. See the above-referenced section for further details.

b. **Nokomis:**

Nokomis elected not to participate in the blind study.

Nokomis initially indicated an eagerness to participate in the Blind Study, when approached in December 2019. An email from Dr. Andrew Portune from Dec. 9, 2019, in which he states "We look forwards to working with you and your team as part of MVP," is found in Appendix 10. After some initial exchanges of communication with Dr. Portune, many months passed during which CALCE was not able to communicate with him. It was later learned that he was no longer employed by the company. Subsequent attempts to obtain agreement to proceed with the Blind Study resulted in further delays and obstacles,

including their expectation of significant financial support (about $50,000) from CALCE in order for them to participate. In 2020 Nokomis was being contracted by DMEA to provide and further develop the ADEC system, and it was granted a contract extension by DMEA in order to facilitate their participation in the Blind Study. In October 2020, direct communication between Nokomis and DMEA regarding the Blind Study resulted in an affirmation to CALCE that they wished to participate. In early November 2020 Nokomis confirmed to CALCE the list of part numbers that they planned to test, based on their stated ability to complete testing before the end of that month. Nevertheless, more time passed during which Nokomis specifically instructed CALCE not to ship parts to them for testing. Multiple further efforts by CALCE to contact management at Nokomis in November 2020 were not successful. As the deadline for submission of this report approached, and absent any communications or requests for parts by Nokomis, CALCE instructed SMT Corp. to send parts to Nokomis anyway so that parts would be available to them as soon as they were able to begin testing. On November 30 (the date that CALCE's final report to DMEA was due), CALCE was contacted by Dr. Matt Moynihan of Nokomis. CALCE was informed that Dr. Moynihan had been out of the office for the two prior weeks on leave. He indicated that Nokomis would indeed like to participate in the study, despite their knowledge that CALCE's report to DMEA was due that same day and that their results would likely not be included in the final project report. Ultimately, Nokomis did not provide any test results to CALCE prior to the submission of this report.

An email exchange between CALCE and Nokomis, containing a statement from their CEO, Dr. Walter Keller explaining why they were unable to provide test results in time for inclusion in this report, is found in Appendix 10. The statement from Dr. Keller reads as follows: "Your comments are accurate, we were very excited about the study. Unfortunately, it was just not possible considering the unique challenges the COVID environment is presenting. We are just as disappointed as you are, but it was beyond our control. We'd still like to test the parts even if they will not be in the study after things settle in the new year."

Nokomis did indicate that they had procured reference parts for the part numbers that they eventually plan to test. This would allow them, like Battelle, to potentially classify the test parts as suspect counterfeit or authentic parts, but it also introduces the same risks as those mentioned above for Battelle.

c. Sandia National Laboratories:

CALCE received Sandia's report on analysis of the six part numbers that they had agreed to test, listed above in Table 5. Accuracy and confusion matrices have been calculated and are presented below. Sandia's report is found in Appendix 11.

Sandia: LM324N						
Sample	**SN**	**Group**		**Sample**	**SN**	**Group**
2	CS-0242	2		1	CK-2150	1
3	ED-0743	2		7	JV-2014	1
4	GU-0350	2		8	JW-1216	1
5	GX-0433	2		9	KZ-1135	1
6	JM-0240	2		13	QT-1163	1
10	OV-0948	2		14	RB-1125	1
11	PD-0717	2		15	SD-1168	1
12	PY-0381	2		16	SJ-1962	1
17	UA-0828	2		18	WM-1637	1
19	XC-0218	2		20	XD-1797	1

10	0	1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10	0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

Sandia: EPCS4SI8N						
Sample	**SN**	**Group**		**Sample**	**SN**	**Group**
2	ER-0173	2		1	CR-1984	1
4	DF-0278	2		3	AJ-1917	1
5	DG-0151	2		6	EL-1523	1
9	FU-0574	2		7	EO-1280	1
10	IE-0380	2		8	FM-2037	1
11	IT-0599	2		12	NB-1734	1
15	RQ-0061	2		13	OK-1934	1
18	XF-0404	2		14	RM-1840	1
19	YG-0801	2		16	RZ-1354	1
20	ZO-1028	2		17	TA-1948	1

10	0	1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10	0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

Sandia: MC34063						
Sample	**SN**	**Group**		**Sample**	**SN**	**Group**
2	OR-0640	2		1	AF-1318	1
6	KH-0504	2		3	AG-1963	1
7	LX-0965	2		4	CB-1936	1
9	NO-0095	2		5	FJ-2076	1
10	OC-0366	2		8	LX-2320	1
12	PY-0874	2		11	PR-1727	1
17	VK-0176	2		13	QT-2289	1
18	WJ-0563	2		14	QW-1577	1
19	YC-0169	2		15	TT-1469	1
20	ZC-0170	2		16	VF-1736	1

10	0	1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10	0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

Sandia: OP07CP						
Sample	**SN**	**Group**		**Sample**	**SN**	**Group**
2	UM-0255	2		1	XK-1317	1
4	BZ-0961	2		3	AD-2274	1
7	DQ-0748	2		5	CE-1127	1
8	HK-0223	2		6	CG-2275	1
11	JZ-0196	2		9	HL-1964	1
12	KI-0893	2		10	IH-1305	1
13	KT-0246	2		14	MM-2173	1
16	NT-0747	2		15	NI-1385	1
17	QQ-1003	2		18	ST-1543	1
20	XA-0810	2		19	VG-1100	1

10	0	1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10	0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

Sandia: SG3525						
Sample	**SN**	**Group**		**Sample**	**SN**	**Group**
1	AJ-0986	1		2	VL-1756	2
3	FA-0020	1		4	FP-2048	2
5	IN-0904	1		7	JM-1519	2
6	IR-0443	1		8	MH-1927	2
10	OM-0624	1		9	NW-2155	2
12	QY-0200	1		11	PC-1769	2
14	UR-0100	1		13	RN-1883	2
16	VZ-0153	1		15	UZ-2161	2
17	WX-0977	1		18	XI-1454	2
19	XP-0011	1		20	YM-1113	2

10	0	1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10	0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

Sandia: XC3S200AN						
Sample	**SN**	**Group**		**Sample**	**SN**	**Group**
2	TL-0355	2		1	ON-1395	1
5	EC-0243	2		3	CN-1242	1
8	GO-0006	2		4	EA-1919	1
9	GP-0470	2		6	EU-2051	1
10	JD-0674	2		7	FB-2324	1
12	JO-0838	2		11	JD-1744	1
13	LX-0056	2		14	OE-1347	1
17	RP-0729	2		15	PU-1448	1
19	SY-0232	2		16	RI-1586	1
20	TP-0588	2		18	SO-1809	1

10	0		1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10		0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

Sandia's accuracy was 100% for clustering of the parts. It is noteworthy that for LM324N, Sandia has achieved 100% accuracy whereas Battelle was not able to distinguish the counterfeit (clone) parts from the authentic parts.

The effort to secure Sandia's participation in the Blind Study was impeded by administrative and bureaucratic hurdles between a federally funded (DOE) national laboratory and a state university (UMD). The two biggest such hurdles were the execution of a non-disclosure agreement (NDA) and execution of a Strategic Partnership Projects (SPP) Funds-In Agreement. Even after the NDA was signed in October 2020, Sandia was unable to accept a simple purchase order for the purposes of performing testing. The SPP agreement required pre-payment and generation of a charge account before any activity by the research engineer involved in the project was allowed to take place. As a result of these administrative hurdles, the charge account was ultimately created on December 7, 2020. Sandia provided us with test results on one part number on that same day.

Sandia has also provided a video conference-based demonstration of the testing procedure and shared video clips of the process of data collection. Sandia's research engineer, Dr. Paiboon Tangyunyong, had been helpful during the preparation for the Blind Study through provision of information about the technology, fixtures, and test processes.

d. **PFP Cybersecurity:**

CALCE received PFP's report on analysis of four of the six part numbers that they had agreed to test, listed above in Table 5. Accuracy and confusion matrices have been calculated and are presented below. PFP's report is in Appendix 12.

PFP: EPCS4SI8N								
State	**SN**	**P Value**	**KS**		**State**	**SN**	**P Value**	**KS**
2	CK-0707	0.0081617	1		1	AG-1162	0.77095	0
4	FQ-0004	0.00018331	1		3	DF-1192	3.629E-08	1
5	IK-0856	1.53E-06	1		6	IZ-1678	0.77095	0
7	JH-1017	0.059142	0		8	JU-1905	0.00018331	1
10	MH-0445	2.49E-07	1		9	KW-1916	0.27527	0
13	ON-0512	3.63E-08	1		11	OD-1092	8.42E-06	1
14	PI-0341	8.42E-06	1		12	OI-2245	0.059142	0
15	QA-0143	3.63E-08	1		17	RP-1206	1.53E-06	1
16	QX-0687	0.77095	0		18	RW-1559	9.31E-05	1
20	**ZP-0421**	**Comparison**	-		19	TJ-2121	0.0081617	1

7	6	0.78	0.60	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
2	4	0.22	0.40	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 0.58

PFP: EPCS4SI8N Against AG-1162						
State	**SN**	**KS**		**State**	**SN**	**KS**
2	CK-0707	1		1	**AG-1162**	0
4	FQ-0004	1		3	DF-1192	1
5	IK-0856	1		6	IZ-1678	1
7	JH-1017	1		8	JU-1905	1
10	MH-0445	1		9	KW-1916	1
13	ON-0512	1		11	OD-1092	1
14	PI-0341	1		12	OI-2245	1
15	QA-0143	1		17	RP-1206	1
16	QX-0687	1		18	RW-1559	1
20	ZP-0421	1		19	TJ-2121	1

10	9	1.00	0.90	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	1	0.00	0.10	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 0.55

PFP: EPCS4SI8N Against CK-0707						
State	**SN**	**KS**		**State**	**SN**	**KS**
2	**CK-0707**	0		1	AG-1162	1
4	FQ-0004	1		3	DF-1192	1
5	IK-0856	1		6	IZ-1678	1
7	JH-1017	1		8	JU-1905	1
10	MH-0445	1		9	KW-1916	1
13	ON-0512	1		11	OD-1092	1
14	PI-0341	1		12	OI-2245	1
15	QA-0143	1		17	RP-1206	1
16	QX-0687	1		18	RW-1559	1
20	ZP-0421	1		19	TJ-2121	1

1	0	0.10	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
9	10	0.90	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 0.55

PFP: EPCS4SI8N				
Matches: CK-0707	**Correct (Y/N)**		**Matches: AG-1162**	**Correct (Y/N)**
CK-0707	Y		**AG-1162**	Y
FQ-0004	Y		DF-1192	Y
IK-0856	Y		IZ-1678	Y
JH-1017	Y		JU-1905	Y
MH-0445	Y		KW-1916	Y
ON-0512	Y		OD-1092	Y
PI-0341	Y		OI-2245	Y
QA-0143	Y		RP-1206	Y
QX-0687	Y		RW-1559	Y
ZP-0421	Y		TJ-2121	Y

10	0		1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10		0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

PFP: LM317T Against ZK-2340						
State	**SN**	**KS**		**State**	**SN**	**KS**
1	JJ-0220	1		10	IU-2199	0
2	QZ-0935	1		11	RZ-1183	0
3	QK-0484	1		12	SQ-1340	0
4	YI-1015	1		13	NP-1363	0
5	YA-0268	1		15	RJ-1102	0
6	SH-0867	1		16	YS-1993	0
7	LZ-0825	1		17	LA-1257	0
8	WP-0268	1		18	JY-1561	0
9	QN-0198	1		19	BG-1182	0
14	VT-0659	1		20	**ZK-2340**	0

10	0	1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10	0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

PFP: LM317T Against JJ-0220						
State	**SN**	**KS**		**State**	**SN**	**KS**
1	**JJ-0220**	0		10	IU-2199	1
2	QZ-0935	0		11	RZ-1183	1
3	QK-0484	0		12	SQ-1340	1
4	YI-1015	0		13	NP-1363	1
5	YA-0268	0		15	RJ-1102	1
6	SH-0867	0		16	YS-1993	1
7	LZ-0825	0		17	LA-1257	1
8	WP-0268	0		18	JY-1561	1
9	QN-0198	0		19	BG-1182	1
14	VT-0659	1		20	ZK-2340	1

9	0	0.90	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
1	10	0.10	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 0.95

PFP: LM317T				
Matches: ZK-2340	**Correct (Y/N)**		**Matches: JJ-0220**	**Correct (Y/N)**
IU-2199	Y		JJ-0220	Y
RZ-1183	Y		QZ-0935	Y
SQ-1340	Y		QK-0484	Y
NP-1363	Y		YI-1015	Y
RJ-1102	Y		YA-0268	Y
YS-1993	Y		SH-0867	Y
LA-1257	Y		LZ-0825	Y
JY-1561	Y		WP-0268	Y
BG-1182	Y		QN-0198	Y
ZK-2340	Y		VT-0659	Y*

10	0		1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10		0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

PFP: CD4093 Against OW-0621						
State	**SN**	**KS**		**State**	**SN**	**KS**
6	DV-0361	0		1	CR-1442	1
8	QH-0888	0		2	NX-1596	1
10	QC-0499	0		3	DI-1534	1
11	XU-0502	0		4	PU-2253	1
14	TN-0279	0		5	TU-1707	1
15	OH-0626	0		7	RZ-1557	1
16	AD-0177	0		9	NC-1526	1
17	FR-0749	0		12	EU-1763	1
18	XF-0393	0		13	DP-1368	1
20	**OW-0261**	0		19	ZF-1558	1

10	0	1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10	0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

PFP: CD4093 Against CR-1442						
State	**SN**	**KS**		**State**	**SN**	**KS**
6	DV-0361	1		1	**CR-1442**	0
8	QH-0888	1		2	NX-1596	0
10	QC-0499	1		3	DI-1534	0
11	XU-0502	1		4	PU-2253	0
14	TN-0279	1		5	TU-1707	0
15	OH-0626	1		7	RZ-1557	0
16	AD-0177	1		9	NC-1526	1
17	FR-0749	1		12	EU-1763	0
18	XF-0393	1		13	DP-1368	0
20	OW-0261	1		19	ZF-1558	0

10	1	1.00	0.10	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	9	0.00	0.90	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 0.95

PFP: CD4093				
Matches: CR-1442	**Correct (Y/N)**		**Matches: OW-0621**	**Correct (Y/N)**
CR-1442	Y		DV-0361	Y
NX-1596	Y		QH-0888	Y
DI-1534	Y		QC-0499	Y
PU-2253	Y		XU-0502	Y
TU-1707	Y		TN-0279	Y
RZ-1557	Y		OH-0626	Y
EU-1763	Y		AD-0177	Y
DP-1368	Y		FR-0749	Y
ZF-1558	Y		XF-0393	Y
NC-1526	**Not Grouped**		**OW-0261**	Y

10	**1**		1.00	0.10	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	9		0.00	0.90	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 0.95

PFP: SG3525AN: Against EC-0686						
State	**SN**	**KS**		**State**	**SN**	**KS**
2	JD-0257	0		1	PF-1427	1
8	OO-0751	0		3	XI-1945	1
9	PS-1054	0		4	DA-1899	1
13	BA-0698	0		5	LR-1267	1
14	HX-0824	0		6	MW-2011	1
15	LW-1021	0		7	CG-1275	1
17	YD-0850	0		10	GZ-1566	1
18	SN-0561	0		11	MD-1897	1
19	NK-0714	0		12	LN-1776	1
20	**EC-0686**	0		16	EH-1878	1

10	0	1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10	0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

PFP: SG3525AN: Against PF-1427						
State	**SN**	**KS**		**State**	**SN**	**KS**
2	JD-0257	1		1	**PF-1427**	0
8	OO-0751	1		3	XI-1945	0
9	PS-1054	1		4	DA-1899	0
13	BA-0698	1		5	LR-1267	0
14	HX-0824	1		6	MW-2011	0
15	LW-1021	1		7	CG-1275	0
17	YD-0850	1		10	GZ-1566	0
18	SN-0561	1		11	MD-1897	0
19	NK-0714	1		12	LN-1776	0
20	EC-0686	1		16	EH-1878	0

10	0	1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10	0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

PFP: SG3525AN				
Matches: EC-0686	**Correct (Y/N)**		**Matches: PF-1427**	**Correct (Y/N)**
JD-0257	Y		**PF-1427**	Y
OO-0751	Y		XI-1945	Y
PS-1054	Y		DA-1899	Y
BA-0698	Y		LR-1267	Y
HX-0824	Y		MW-2011	Y
LW-1021	Y		CG-1275	Y
YD-0850	Y		GZ-1566	Y
SN-0561	Y		MD-1897	Y
NK-0714	Y		LN-1776	Y
EC-0686	Y		EH-1878	Y

10	0		1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	10		0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

PFP Cybersecurity tested four of the six parts that they had agreed to test for the blind study by December 7. The results are mixed. The first test result, covering only the Altera EPCS4SI8N, had poor performance. A repeat test on that same part number, and the tests on the other two part numbers, showed almost perfect separation between the authentic and counterfeit parts. PFP plans to test the remaining three parts within the month of December, but that is contingent on the receipt and calibration of the fixtures needed to acquire data.

Communication with PFP started in early 2020, but there was a significant gap in communications in the early part of the COVID shutdown. Since September 2020, there had been consistent communications between CALCE and PFP concerning the parts list, the statement of work, and some sample parts that were shared in early October. The mutual expectation was that PFP would provide CALCE with a quotation for the cost of the testing, and a list of the part numbers that they would be able to test. However, CALCE was never presented with a quotation, and they ultimately performed the testing at no charge. In the middle of November, PFP gave CALCE a list of part numbers that they could test. They received the parts from SMT on Nov. 17 and results on the first part number was received by CALCE on Nov 30. A repeat test on that

first part number, and test results for two additional part numbers, were received between Dec. 4 and Dec. 7. CALCE held a meeting with PFP on Dec. 8 to discuss the testing and clarify the data analysis and reporting.

The PFP team was forthcoming regarding the difficulties that they faced in testing. While PFP seeks to become primarily a software provider that can analyze data collected using commercial test and measurement tools, the data collection is clearly dependent on the test boards and fixtures. The quality of the collected data and "noise" in the data impacted the classification process. This was the reason provided to CALCE for the poor results in the initial testing of the Altera EPCS4SI8N.

Part classification was unsupervised but required repeated manual intervention and visual data analysis to reach a conclusion. After acquisition of data on all 20 parts of a particular part number, they randomly selected one part to which all other parts in the group were compared. After parts that matched the selected part were identified, one random part from the remaining set was selected for a subsequent matching process. All parts were compared with this second part, and matching parts were placed into a second cluster. Matching was initially performed using a hypothesis test applied to a Bounded Bayesian classifier, although the threshold used for separation of clusters had to be customized for each round of comparisons. In some cases where separation was difficult on this basis, clustering of parts was accomplished through manual inspection of histograms constructing using variation on means.

e. Observations and conclusions regarding the Side Channel portion of the blind study:

It is advantageous that Side Channel testing does not require the measurement of a full complement of datasheet electrical parameters, thus reducing the test time per part, the complexity of the test setup, and the cost of the equipment. To avoid the possibility of damage to a part due to testing, the datasheet must be consulted to remain within the manufacturer's recommended stress levels.

With some technologies, such as the Battelle Barricade, customized test systems are required, whereas in other cases commercial test equipment makes up the majority or entirety of the hardware requirement. There are benefits and disadvantages for both approaches. For example, when commercial tools are used, there is a greater flexibility and possibly lower overall cost, but also a greater chance that over a period of several decades, obsolescence will cause changes to the available test configurations and settings that might make comparison to collected data challenging. In addition, the software suite must be integrated with whatever hardware is selected for use. On the other hand, the use of custom equipment requires the company providing that equipment to remain viable and provide support for the duration of its use. The equipment must also retain backward compatibility in some form to configurations that were used

to collect baseline data, although this may be facilitated by having a single organization responsible for that process. At this point, the two companies that are producing custom test equipment for Side Channel testing, namely Battelle and Nokomis, do not have sufficient production volumes to ensure tight process control and avoid significant unit-to-unit variability. Sandia's test system is made up of a combination of commercial and custom hardware, and is not currently mass produced.

Since all testing was performed during the coronavirus pandemic, there was no opportunity for CALCE personnel to travel to the locations were testing was being performed, in order to witness the process and make an assessment of the set-up process and timing associated with testing. CALCE's experience of working with the Side Channel organizations to plan and conduct testing indicated that none of the organizations could offer to test all 11 part numbers in a reasonable time and at reasonable cost. In all cases, testing of part numbers for which the organizations did not already have fixtures would have added one or two months to the preparation time for testing. As a result, most organizations were willing to test only a subset of the part numbers, typically 6 (8 in the case of Battelle).

One of the observations from the Blind Study was that the same part number could produce very different accuracy results with different systems. For example, the LM324N part number produced inconclusive results with the Battelle Barricade system, but good accuracy of clustering with the Sandia PSA, both of which are power-based systems. It would be very useful to identify many such variations, and determine the root cause of such differences. On the one hand, this would allow improvements to the accuracy of the system with the poorer performance and on the other hand it can be helpful to identify which part types are not as suitable for evaluation with certain systems. However, this type of root cause analysis will require application of conventional standards-based test methods to provide insight into the physical characteristics of the devices that lead to such differences. At the current level of development of these techniques, the results produced by Side Channel methods are essentially black box outputs. They do not reveal specific physical defects associated with counterfeit parts in the way that conventional, standards-based tests are capable of. Consequently, the acceptance of a finding of counterfeit for a lot in an actual purchasing transaction may not be accepted by all parties, and yet cannot be easily justified without recourse to conventional testing. Even after these tools have attained a high level of technology readiness and reliability, it will continue to require a leap of faith to accept findings that are based purely on application of mathematical algorithms to data.

All four Side Channel techniques can potentially be used without a set of reference samples (i.e., exemplars or golden parts). In this mode, the results are obtained by unsupervised learning to cluster parts according to mutual similarities. This can provide an indication of uniformity within a lot, but not necessarily an identification of counterfeit parts. In many practical circumstances, when reference parts are

not available, the results may have reduced accuracy (as communicated to CALCE by Battelle) and could be misleading or inconclusive in the case of lots that are made up entirely of counterfeits. The solution to this problem that has been employed by these organizations is to build up a database of data from known authentic parts of various types and vintage. This is a costly and time-consuming process. Storage, age, and process changes can all affect the test results and may lead to false positives. Databases must therefore include results on parts that cover the range of variations that may be encountered, and the software must account for the variations that may be caused by differences other than counterfeiting.

As discussed above, the usefulness of Side Channel methods is dependent on the database of test results that is available for comparison when needed. This database must be maintained and secured over a span of many years, quite possibly decades. Thus the integrity and confidentiality of the data must be ensured for the duration of applicability of the Side Channel system to authentication of parts. Cybersecurity issues concerning the database must be managed and protected, especially for defense and related applications characterized by long life and high criticality. Other aspects of database management will also have to be considered in the business model, including database ownership, read- and write-accessibility, and servers on which the data are hosted. A related set of issues concerns the longevity of the organizations controlling the technology and database. Of the organizations that CALCE evaluated, two (PFP and Nokomis) are relatively small technology companies with uncertain long-term futures. The other two, Sandia and Battelle, are large organizations, but this niche technology is not a major focus for their business and they may wish to find licensees or buyers to manage and roll out the technology and build a market. If DoD commits to the use of one of more Side Channel technologies for securing their supply chain, it must first evaluate the risks and potential financial and supply chain liabilities that may come from failure of the technology provider to continue supporting the technology. In addition to the management of the supply chain for components, DoD is now, and will increasingly, need to ensure the security of the supply chain for assemblies. Prior to the selection of a technology for part authentication, DoD should evaluate whether the technology is suitable for similar tasks at an assembly level. Among the four organizations that CALCE evaluated for the Blind Study, PFP is the one company that has made testing of assemblies a focus of their business plan.

Table 26 and Table 27 in the conclusions section include a summary of the results of Side Channel testing along with those of conventional and Image Analysis methods. Table 26 shows the detailed summary of results including both detection and clustering accuracy for clones and conventional counterfeits separately and combined and Table 27 shows the same with both clones and combined counterfeit parts combined.

5. Image Analysis Testing

Three organizations, Alitheon, Creative Electron, and Covisus, performed testing using Image Analysis test methods on a subset of the eleven parts listed above. This testing was governed by a statement of work which is found in Appendix 13. The original plan called for a single set of parts to be used for testing by all three Image Analysis companies. For each part number, 10 parts consisting of 5 counterfeit and 5 authentic would be used for registration. The parts would be shipped by SMT to one company for registration; they would be returned to SMT and then shipped to the next company for registration; and they would be shipped back to SMT and then shipped to the third company for registration. After receipt of parts from the third and final Image Analysis company, SMT would assign new serial numbers to the registration parts and expand each group using 5 additional counterfeit and 5 authentic parts that had not been registered. For each of these groups of 20 parts, some parts would undergo stress aging, consisting of scuffing and scratching of the surface. Stress aging was performed on 2 counterfeit and 2 authentic parts from each registered group, and on 2 counterfeit and 2 authentic parts from the non-registered group. This was done to alter the visual features of the parts in order to simulate the kind of changes that could occur during usage and handling, in order to challenge the Image Analysis systems. The severity of this surface damage was mild. The parts would then be shipped again in sequence to each company for the authentication phase of the study, in which parts would be compared to the data collected during registration in order to determine which of the 20 parts from each part number had been previously registered and which had not, and, if possible, to cluster the parts according to mutual similarities and differences.

The original plan had to be modified due to the amount of time that was used by the companies during the registration phase. By the time parts had completed registration by Creative Electron and Alitheon, it became evident that there would not be enough time to complete the entire study if Covisus was included in the sequence. Thus, a decision was made to use a different set of parts for Covisus and create a second, parallel plan for them. Based on the number of parts available in inventory for this purpose, only 6 of the 11 part numbers were able to be tested by Covisus. This approach allowed Creative Electron and Alitheon to complete both the registration and authentication phases of the study, and data to be received from Covisus on the registration phase of the study. Data from Covisus on the authentication phase was not available at the time of submission of this report, but will be made available to DMEA once that phase of the study has been completed.

The results of the Blind Study from the three organizations that performed Image Analysis testing are summarized below.

a. **Alitheon:**

Alitheon conducted registration on all eleven part numbers (ten parts each) and completed authentication for six part numbers with near perfect results. Alitheon's test report is in Appendix 14.

Alitheon: LM317T					
Original SN	**New SN**	**Correct (Y/N)**	**Unregistered**	**Correct (Y/N)**	**Note**
IQ-0258	MO-0090	Y	LS-0608	Y	Aged
GY-0547	AJ-1001	Y	NX-0059	Y	Aged
OP-1004	FC-0912	Y	DL-0213	Y	
VZ-0418	LI-0093	Y	KS-0884	Y	
EP-0900	QW-0953	Y	ZV-0739	Y	
DR-1239	TW-1419	Y	DE-1504	Y	Aged
ID-1440	JL-2206	Y	SX-1799	Y	Aged
NQ-2221	ML-1921	Y	UL-1446	Y	
LK-2171	FC-1400	Y	QC-1346	Y	
BP-1957	JA-1821	Y	DP-2264	Y	

10	0	1.00	0.00	TP: Unregistered part correctly identified as unregistered	FP: Registered part identified as unregistered -or- registered part identified as incorrect register part label
0	10	0.00	1.00	FN: Unregistered part identified as registered	TN: Registered part correctly identified as registered

Accuracy = 1.00

Alitheon: CD4093BM					
Original SN	**New SN**	**Correct (Y/N)**	**Unregistered**	**Correct (Y/N)**	**Note**
HG-0861	JN-0103	Y	ZD-0262	Y	Aged
AI-0299	ZO-0444	Y	PN-0290	Y	Aged
BV-0094	PQ-0179	Y	TQ-0449	Y	
CQ-0340	WC-0641	Y	VQ-0228	Y	
AL-0496	ZM-0211	Y	NG-0592	Y	
ZG-2309	DD-1832	Y	EQ-2108	Y	Aged
XG-2368	TW-1569	Y	PS-2310	Y	Aged
RD-1235	ZM-2219	Y	WQ-1159	Y	
QU-1188	ME-1759	Y	HO-2122	Y	
HZ-2198	QF-1710	Y	GQ-1392	Y	

10	0		1.00	0.00	TP: Unregistered part correctly identified as unregistered	FP: Registered part identified as unregistered -or- registered part identified as incorrect register part label
0	10		0.00	1.00	FN: Unregistered part identified as registered	TN: Registered part correctly identified as registered

Accuracy = 1.00

Alitheon: EPCS4SI8N					
Original SN	**New SN**	**Correct (Y/N)**	**Unregistered**	**Correct (Y/N)**	**Note**
XR-0820	LG-0108	Y	OH-0054	Y	Aged
MY-1006	JR-0509	Y	NV-0346	Y	Aged
AL-0914	JG-0507	Y	RM-0263	Y	
PL-0584	HV-0254	Y	JC-0887	Y	
JH-0286	ZH-0691	Y	XN-0426	Y	
VN-1515	GV-2363	Y	JY-1132	Y	Aged
RL-1408	BH-1805	Y	WQ-1229	Y	Aged
DA-1141	GK-1489	Y	EA-1998	Y	
JD-1913	SP-1341	Y	JX-1705	Y	
RI-2049	XB-2039	Y	EQ-2067	Y	

10	0		1.00	0.00	TP: Unregistered part correctly identified as unregistered	FP: Registered part identified as unregistered -or- registered part identified as incorrect register part label
0	10		0.00	1.00	FN: Unregistered part identified as registered	TN: Registered part correctly identified as registered

Accuracy = 1.00

Alitheon: LM324					
Original SN	**New SN**	**Correct (Y/N)**	**Unregistered**	**Correct (Y/N)**	**Note**
VV-0027	TE-0329	Y	ZA-0946	Y	Aged
MP-0822	DK-0902	Y	CQ-0766	Y	Aged
JV-1042	FL-0837	Y	XE-0544	Y	
DW-0876	JO-0891	Y	BD-0631	Y	
JI-0277	GI-0320	Y	OF-0060	Y	
MM-2182	FN-2017	Y	JD-1513	Y	Aged
CA-1985	NM-1247	Y	CG-1766	Y	Aged
MN-1656	ZW-1779	Y	OQ-1694	Y	
NH-1411	TS-1219	Y	TD-1803	Y	
GX-1124	IJ-1375	Y	BS-1553	Y	

10	0		1.00	0.00	TP: Unregistered part correctly identified as unregistered	FP: Registered part identified as unregistered -or- registered part identified as incorrect register part label
0	10		0.00	1.00	FN: Unregistered part identified as registered	TN: Registered part correctly identified as registered

Accuracy = 1.00

Alitheon: MAX232ESE					
Original SN	**New SN**	**Correct (Y/N)**	**Unregistered**	**Correct (Y/N)**	**Note**
KT-2162	NR-0710	Y	KQ-0087	Y	Aged
PD-2257	XE-0157	Y	SY-0249	Y	Aged
AN-0188	FB-0704	Y	CD-0427	Y	
ZX-0297	QV-0786	Y	ST-0183	Y	
YO-0422	ZZ-0642	Y	EO-0966	Y	
YJ-0132	AD-1812	Y	OU-1348	Y	Aged
YE-0373	BM-1387	Y	AZ-1176	Y	Aged
ZU-1198	SE-1568	Y	CZ-1236	Y	
IE-1472	VG-2224	Y	MN-2360	Y	
ST-1735	KA-1251	Y	CL-1980	Y	

10	0		1.00	0.00	TP: Unregistered part correctly identified as unregistered	FP: Registered part identified as unregistered -or- registered part identified as incorrect register part label
0	10		0.00	1.00	FN: Unregistered part identified as registered	TN: Registered part correctly identified as registered

Accuracy = 1.00

Alitheon: SG3525AN					
Original SN	**New SN**	**Correct (Y/N)**	**Unregistered**	**Correct (Y/N)**	**Note**
VK-0451	JK-0735	Y	SO-1033	Y	Aged
PL-0307	VC-0002	No Match	NE-0280	Y	Aged
ZM-0594	VT-0485	Y	TL-0951	Y	
DL-0683	EV-0265	Y	ZD-1031	Y	
SB-0460	MI-0256	Y	PX-0600	Y	
BT-2338	FJ-1177	Y	EB-2353	Y	Aged
RS-1582	RM-1898	Y	VL-2318	Y	Aged
CW-2136	RM-1563	Y	RL-1120	Y	
JS-2164	AP-1276	Y	FH-1709	Y	
UB-2343	FE-1866	Y	KJ-1764	Y	
			VC-0002	N	

10	1		1.00	0.10	TP: Unregistered part correctly identified as unregistered	FP: Registered part identified as unregistered -or- registered part identified as incorrect register part label
0	9		0.00	0.90	FN: Unregistered part identified as registered	TN: Registered part correctly identified as registered

Accuracy = 0.95

Alitheon's indicated which of the parts in the authentication group matched with the previously registered parts. They identified the specific serial number to which the matching parts corresponded. They also listed the serial numbers of those parts that they did not match to previously registered parts. They correctly identified 119 out of the 120 parts that were authenticated. However, since the level of surface alteration on the stress aged parts was not severe, further testing with a greater level of damage would be needed to determine the boundaries of the capabilities of the system. Alitheon claims that even with less than 10% of the original surface intact they would be able to authenticate a part.

Alitheon did not attempt to cluster parts within each group based on mutual similarities and differences, so there was no identification of which parts belong to groups that could have been used to separate the counterfeit from the authentic parts. They indicated that a different approach would have been needed in order to accomplish this type of analysis.

Alitheon had been cooperative and forthcoming from the beginning and forceful in making a case for their technology and its benefits. Although they were interested in establishing an agreement between SMT, CALCE and them, they did not refuse to begin the work when those agreements could not be completed. Based on discussions between CALCE and Alitheon's team members, and their involvement in the process of establishing the terms governing data sharing and rights to data, it is clear that they have thought through the process of their future development. Despite the fact that they did not have resources to perform testing on our schedule, when parts were shipped to them they actually performed the tests very quickly (within about a day) and were very responsive with respect to communication of status and the logistics of shipping and receiving parts. They were also clear in communicating when they were not in a position to perform any more tests due to competing commitments, and were very prompt in returning parts that they were not able to tests.

b. **Covisus:**

CALCE received Covisus's initial (registration) report on the six part numbers that they were sent. Covisus's test report is in Appendix 15.

Covisus: CD4093BM ECHO						
Item	**SN**	**Group**		**Item**	**SN**	**Group**
4	GY-0452	2		1	DA-2290	1
5	IZ-0269	2		2	FV-1815	1
7	WZ-0993	2		3	GI-1547	1
8	XL-0135	2		6	WO-1455	1
9	XW-0515	2		10	YE-2348	1

5	0	1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	5	0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

Covisus: CD4093BM KILO						
Item	**SN**	**Group**		**Item**	**SN**	**Group**
4	GY-0452	1		1	DA-2290	1
5	IZ-0269	1		2	FV-1815	1
7	WZ-0993	2		3	GI-1547	1
8	XL-0135	1		6	WO-1455	1
9	XW-0515	1		10	YE-2348	1

1	0	0.20	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
4	5	0.80	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 0.60

Covisus: EPCS4SI8N ECHO						
Item	**SN**	**Group**		**Item**	**SN**	**Group**
1	BS-0231	2		2	BZ-1893	1
6	GM-0793	1		3	CF-1611	1
7	HH-0675	1		4	DV-1827	1
8	HO-0365	1		5	EZ-1186	1
10	QA-0910	1		9	OX-1085	1

1	0	0.20	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
4	5	0.80	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 0.60

Covisus: EPCS4SI8N KILO						
Item	**SN**	**Group**		**Item**	**SN**	**Group**
1	BS-0231	2		2	BZ-1893	1
6	GM-0793	2		3	CF-1611	1
7	HH-0675	2		4	DV-1827	1
8	HO-0365	2		5	EZ-1186	1
10	QA-0910	2		9	OX-1085	1

5	0	1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	5	0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

Covisus: LM317 ECHO						
Item	**SN**	**Group**		**Item**	**SN**	**Group**
1	CI-0785	1		2	DF-1498	2
3	EA-0759	1		5	HH-1682	2
4	ER-0920	1		7	LW-2124	2
6	LO-0796	1		9	SV-1786	2
8	PW-0275	1		10	UJ-1091	2

5	0	1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	5	0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

Covisus: LM317 KILO						
Item	**SN**	**Group**		**Item**	**SN**	**Group**
1	CI-0785	2		2	DF-1498	1
3	EA-0759	2		5	HH-1682	1
4	ER-0920	2		7	LW-2124	1
6	LO-0796	2		9	SV-1786	1
8	PW-0275	2		10	UJ-1091	1

5	0	1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	5	0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

Covisus: SG3525AN ECHO						
Item	**SN**	**Group**		**Item**	**SN**	**Group**
1	BB-0630	1		2	BU-1365	2
4	CL-0843	1		3	CA-2126	2
6	GJ-0750	1		5	FW-2172	2
8	KD-0620	1		7	HX-2184	2
9	SV-0760	1		10	WJ-2034	2

5	0	1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	5	0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

Covisus: SG3525AN KILO						
Item	**SN**	**Group**		**Item**	**SN**	**Group**
1	BB-0630	2		2	BU-1365	2
4	CL-0843	2		3	CA-2126	2
6	GJ-0750	2		5	FW-2172	1
8	KD-0620	2		7	HX-2184	1
9	SV-0760	2		10	WJ-2034	2

5	3	1.00	0.60	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	2	0.00	0.40	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 0.70

Covisus: XC3S200AN-4FTG256C ECHO						
Item	**SN**	**Group**		**Item**	**SN**	**Group**
2	BW-0321	1		1	AZ-1320	2
4	QX-0958	1		3	NB-1887	2
6	VD-0456	1		5	UB-2078	2
8	WZ-0988	1		7	VO-1847	2
10	ZR-0385	1		9	XY-1881	2

5	0	1.00	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
0	5	0.00	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 1.00

Covisus: XC3S200AN-4FTG256C KILO						
Item	**SN**	**Group**		**Item**	**SN**	**Group**
2	BW-0321	1		1	AZ-1320	2
4	QX-0958	1		3	NB-1887	2
6	VD-0456	1		5	UB-2078	2
8	WZ-0988	1		7	VO-1847	2
10	ZR-0385	2		9	XY-1881	2

4	0	0.80	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
1	5	0.20	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 0.90

Covisus: XC3030A-7PC84C ECHO						
Item	**SN**	**Group**		**Item**	**SN**	**Group**
2	CD-0501	2		1	BY-2299	2
6	JV-0817	1		3	DW-1886	2
7	NK-0787	2		4	FV-1761	2
9	QR-0070	2		5	IU-1706	2
10	ZI-0930	2		8	QH-2019	2

1	0	0.20	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
4	5	0.80	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 0.60

Covisus: XC3030A-7PC84C KILO						
Item	**SN**	**Group**		**Item**	**SN**	**Group**
2	CD-0501	1		1	BY-2299	1
6	JV-0817	1		3	DW-1886	1
7	NK-0787	1		4	FV-1761	1
9	QR-0070	1		5	IU-1706	1
10	ZI-0930	2		8	QH-2019	1

1	0	0.20	0.00	TP: Correctly identified in the counterfeit group	FP: Identified authentic as counterfeit
4	5	0.80	1.00	FN: Identified counterfeit as authentic	TN: Correctly identified in authentic group

Accuracy = 0.60

i. Summary of Covisus's performance in the Blind Study.

Covisus performed unsupervised learning to cluster the parts from each group of 10 parts. The top and bottom surfaces of parts were imaged using their vTag scanner. The images were analyzed using the DTEK software. The images contained surface texture information that is characteristic of the surface. On the basis of similarities between the vTags obtained from the surfaces of parts within each group, Covisus identified which cluster each part belonged to. Two methods of comparison (ECHO and KILO, described in Figure 7. DTEK Features available for analysis in Covisus vTag. Figure 7) were used for classification of parts into groups. The accuracy of their clustering varied from part number to part number and between the two methods of classification. For most of the 6 part numbers, at least one of the two classification methods produced an accuracy of 100%, but in many of those cases, the second method produced lower accuracy. In summary, the ECHO method correctly classified 52 of the 60 parts that were tested. The KILO method correctly classified 48 of the 60 parts. In many cases, the parts erroneously classified by ECHO were different from the parts misidentified by KILO. If this were an actual counterfeit detection test, this would create a dilemma on how to interpret the result regarding which criterion to trust.

Communications between CALCE and Covisus were satisfactory and their responsiveness was to requests for information and testing or shipping of parts were good. Covisus's incomplete test results were a result of the delay caused by Creative Electron during the registration phase of the Study, and not due to a lack of cooperation by Covisus.

Test Name	Test Description	Surface Values Considered	Notes
DELTA	Compares the test lot sample versus a user-supplied reference sample. The consistency index provides the relative similarity of the surface regions selected.	Test tops versus reference tops	When a user-supplied reference sample is not available, this test will not populate into the report.
TANGO	Compares the top and bottom characteristics of the test lot samples. The consistency index provides a percentage value describing the relative similarity of the surface regions selected.	Test tops versus test bottoms	If the component has visually obvious differences between the top and bottom, this test may yield erroneous results. If "top/bottom different" is chosen as "yes" on the lot scan info screen, the TANGO test will not be preformed.
ECHO	Examines variations within the top surface characteristics of the test lot sample in order to identify lot mixing or "peppering". The test will "flag" any components considered statistical outliers.	Test sample top side specified by user.	The criteria for clustering the samples is based on "typical" surface variations.
KILO	Examines variations within the bottom surface characteristics of the test lot sample in order to identify lot mixing or "peppering". The test will "flag" any components considered statistical outliers.	Test sample bottom side specified by user.	The criteria for clustering the samples is based on "typical" surface variations.

Figure 7. DTEK Features available for analysis in Covisus vTag.

c. Creative Electron:

Creative Electron conducted registration on all eleven part numbers (ten parts each) and completed authentication for six part numbers with mixed results. The Creative Electron test report on the authentication of six of the part numbers is in Appendix 16.

In the following tables, serial numbers that were incorrectly matched are listed in bold font if an unregistered part was identified as a registered part.

Creative Electron: LM317T					
Original SN	**New SN**	**Correct (Y/N)**	**Unregistered**	**Correct (Y/N)**	**Note**
IQ-0258	MO-0090	Y	LS-0608	Y	Aged
GY-0547	AJ-1001	Y	NX-0059	Y	Aged
OP-1004	FC-0912	Y	DL-0213	Y	
VZ-0418	LI-0093	Y	KS-0884	Y	
EP-0900	QW-0953	Y	ZV-0739	Y	
DR-1239	TW-1419	Y	DE-1504	Y	Aged
ID-1440	JL-2206	Y	SX-1799	Y	Aged
NQ-2221	ML-1921	Y	UL-1446	Y	
LK-2171	FC-1400	Y	QC-1346	Y	
BP-1957	JA-1821	Y	DP-2264	Y	

10	0		1.00	0.00	TP: Unregistered part correctly identified as unregistered	FP: Registered part identified as unregistered -or- registered part identified as incorrect register part label
0	10		0.00	1.00	FN: Unregistered part identified as registered	TN: Registered part correctly identified as registered

Accuracy = 1.00

Creative Electron: CD4093BM					
Original SN	**New SN**	**Correct (Y/N)**	**Unregistered**	**Correct (Y/N)**	**Note**
HG-0861	JN-0103	Y	ZD-0262	Y	Aged
AI-0299	ZO-0444	Y	PN-0290	Y	Aged
BV-0094	PQ-0179	Y	TQ-0449	Y	
CQ-0340	WC-0641	Y	VQ-0228	Y	
AL-0496	ZM-0211	Y	NG-0592	Y	
ZG-2309	DD-1832	Y	EQ-2108	N	Aged
XG-2368	TW-1569	Y	PS-2310	N	Aged
RD-1235	ZM-2219	**EQ-2108**	WQ-1159	Y	
QU-1188	ME-1759	Y	HO-2122	Y	
HZ-2198	QF-1710	**PS-2310**	GQ-1392	Y	

8	2		0.80	0.20	TP: Unregistered part correctly identified as unregistered	FP: Registered part identified as unregistered -or- registered part identified as incorrect register part label
2	8		0.20	0.80	FN: Unregistered part identified as registered	TN: Registered part correctly identified as registered

Accuracy = 0.80

Creative Electron: EPCS4SI8N					
Original SN	**New SN**	**Correct (Y/N)**	**Unregistered**	**Correct (Y/N)**	**Note**
XR-0820	LG-0108	Y	OH-0054	Y	Aged
MY-1006	JR-0509	Y	NV-0346	Y	Aged
AL-0914	JG-0507	Y	RM-0263	Y	
PL-0584	HV-0254	Y	JC-0887	Y	
JH-0286	ZH-0691	Y	XN-0426	Y	
VN-1515	GV-2363	GK-1489	JY-1132	N	Aged
RL-1408	BH-1805	GV-2363	WQ-1229	Y	Aged
DA-1141	GK-1489	**JY-1132**	EA-1998	Y	
JD-1913	SP-1341	XB-2039	JX-1705	Y	
RI-2049	XB-2039	SP-1341	EQ-2067	Y	

9	5	0.90	0.50	TP: Unregistered part correctly identified as unregistered	FP: Registered part identified as unregistered -or- registered part identified as incorrect register part label
1	5	0.10	0.50	FN: Unregistered part identified as registered	TN: Registered part correctly identified as registered

Accuracy = 0.70

Creative Electron: LM324					
Original SN	**New SN**	**Correct (Y/N)**	**Unregistered**	**Correct (Y/N)**	**Note**
VV-0027	TE-0329	Y	ZA-0946	Y	Aged
MP-0822	DK-0902	Y	CQ-0766	Y	Aged
JV-1042	FL-0837	Y	XE-0544	Y	
DW-0876	JO-0891	Y	BD-0631	Y	
JI-0277	GI-0320	Y	OF-0060	Y	
MM-2182	FN-2017	Y	JD-1513	Y	Aged
CA-1985	NM-1247	Y	CG-1766	Y	Aged
MN-1656	ZW-1779	Y	OQ-1694	Y	
NH-1411	TS-1219	Y	TD-1803	Y	
GX-1124	IJ-1375	Y	BS-1553	Y	

10	0		1.00	0.00	TP: Unregistered part correctly identified as unregistered	FP: Registered part identified as unregistered -or- registered part identified as incorrect register part label
0	10		0.00	1.00	FN: Unregistered part identified as registered	TN: Registered part correctly identified as registered

Accuracy = 1.00

Creative Electron: MAX232ESE					
Original SN	**New SN**	**Correct (Y/N)**	**Unregistered**	**Correct (Y/N)**	**Note**
KT-2162	NR-0710	Y	KQ-0087	N	Aged
PD-2257	XE-0157	Y	SY-0249	Y	Aged
AN-0188	FB-0704	Y	CD-0427	Y	
ZX-0297	QV-0786	**ST-0183**	ST-0183	N	
YO-0422	ZZ-0642	QV-0786	EO-0966	Y	
YJ-0132	AD-1812	BM-1387	OU-1348	Y	Aged
YE-0373	BM-1387	**KQ-0087***	AZ-1176	Y	Aged
ZU-1198	SE-1568	Y	CZ-1236	Y	
IE-1472	VG-2224	Y	MN-2360	Y	
ST-1735	KA-1251	Y	CL-1980	Y	

*This part was an unregistered clone that was matched to a registered authentic part.

8	4	0.80	0.40	TP: Unregistered part correctly identified as unregistered	FP: Registered part identified as unregistered -or- registered part identified as incorrect register part label
2	6	0.20	0.60	FN: Unregistered part identified as registered	TN: Registered part correctly identified as registered

Accuracy = 0.70

Creative Electron: SG3525AN					
Original SN	**New SN**	**Correct (Y/N)**	**Unregistered**	**Correct (Y/N)**	**Note**
VK-0451	JK-0735	Y	SO-1033	Y	Aged
PL-0307	VC-0002	Y	NE-0280	Y	Aged
ZM-0594	VT-0485	Y	TL-0951	Y	
DL-0683	EV-0265	Y	ZD-1031	Y	
SB-0460	MI-0256	Y	PX-0600	Y	
BT-2338	FJ-1177	Y	EB-2353	Y	Aged
RS-1582	RM-1898	Y	VL-2318	N	Aged
CW-2136	RM-1563	Y	RL-1120	Y	
JS-2164	AP-1276	**VL-2318**	FH-1709	N	
UB-2343	FE-1866	**FH-1709**	KJ-1764	Y	

8	2		0.80	0.20	
2	8		0.20	0.80	

TP: Unregistered part correctly identified as unregistered	FP: Registered part identified as unregistered -or- registered part identified as incorrect register part label
FN: Unregistered part identified as registered	TN: Registered part correctly identified as registered

Accuracy = 0.80

i. Summary of Creative Electron's performance in the Blind Study.

Creative Electron was included in the mix of companies based on their presentations and publications on use of artificial intelligence in counterfeit detection. The process of registration and authentication by Creative Electron is based on features revealed via x-ray images. The stress aging (i.e., surface modifications) made to a subset of the parts was not expected to make a difference in the process of identification.

Like Alitheon, Creative Electron indicated which of the parts in the authentication group matched with the previously registered parts. They identified the specific serial number to which the matching parts corresponded. They also listed the serial numbers of those parts that they did not match to previously registered parts. They successfully matched 100 of the 120 parts that they analyzed.

The results do not show a recognizable pattern at first glance. Most of the errors in matching affected misidentification of one authentic part for another authentic part. For one part number, MAX232ESE, both clones and authentic parts were mismatched, and some unregistered parts were

identified with registered parts. Worse yet, an unregistered clone was matched to a registered authentic part. It will take additional investigation to review the images and features used by Creative Electron's AI systems used for the decision making to identify the causes of these discrepancies. Creative Electron stated that the algorithm starts with the registered parts and tries to find a match within the set of new images. Thus, for each of the 10 images it looked for all 20 images for a match. For each image, a region of interest is identified and used for matching. Based on Figure 8, it appears that only the die and surrounding areas were used for matching during this study. The exclusion of most of the leadframe from that region may explain why they did not distinguish between a clone and an authentic part in the case of the MAX232ESE error discussed above.

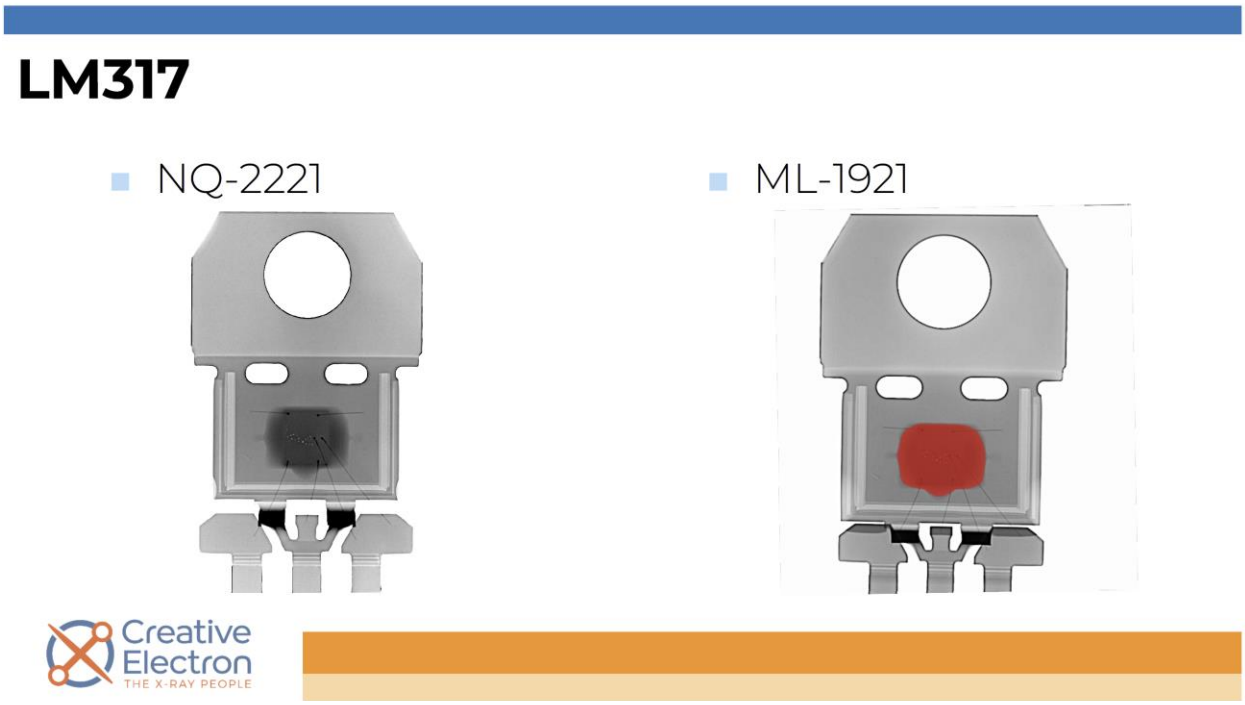


Figure 8. Example of features used for Creative Electron's Fingerprint part matching (region in red was the basis for matching).

The algorithm was designed with the goal of making differences such as parallax, brightness and contrast as irrelevant as possible during the analysis. That attempt is intended to account for the conditions of imaging 5 or 10 years apart not being identical. Creative Electron indicated that, when fully implemented, this step will make the algorithm more suitable for use.

Delays marked the communication with the company during the registration period. The four weeks it took for the initial registration caused a slip in the schedule for the Image Analysis portion of the blind study, required the scope of the study for the other companies (Alitheon and Covisus) to be modified and

reduced. Their results were provided to CALCE on December 6. Following the submission of their report to CALCE, they began to provide more frequent communications and some details of the process they used for analysis.

d. Observations and conclusions regarding the Image Analysis portion of the Blind Study:

With some technologies, such as the Covisus, customized imaging systems are required, whereas in other cases commercial imaging tools can be used to satisfy the hardware requirement. There are benefits and disadvantages for both approaches. For example, when commercial tools are used, there is a greater flexibility and possibly lower overall cost, but also a greater chance that over a period of several decades, obsolescence will cause changes to the available imaging configurations and settings and image data formats that might make comparison to collected data challenging. In addition, the software suite must be integrated with whatever hardware is selected for use. On the other hand, the use of custom equipment requires the company providing that equipment to remain viable and provide support for the duration of its use. The equipment must also retain backward compatibility in some form to configurations that were used to collect baseline images, although this may be facilitated by having a single organization responsible for that process. For example, a state-of-the-art camera 10 years from now could produce completely different image quality and features, that could complicate authentication based on an image taken today. There needs to be a plan to address these issues, such as “re-registration” of parts when tools are updated, or ensuring access to legacy tools. Neither option appears to be promising. At this point, Alitheon does not produce or require the use of specific hardware. Covisus does produce and require the use of their hardware integrated with their software. They claim that, in principle, other imaging hardware can be used, but there is no independent verification of this. Creative Electron is primarily an x-ray hardware manufacturer, although this Image Analysis-based system is not tied to the use of their hardware.

Since all testing was performed during the coronavirus pandemic, there was no opportunity for CALCE personnel to travel to the locations were testing was being performed, in order to witness the process and make an assessment of the set-up process and timing associated with testing.

Alitheon performed significantly better overall than either Covisus or Creative Electron. It is useful to reiterate, however, that Covisus performed classification as part of the registration process, which neither Alitheon or Creative Electron reported. Therefore the basis for evaluating accuracy for Covisus is quite different than the part-to-part matching that was performed by the other two companies. At present, there is no data available in this report to evaluate the accuracy of Covisus in authentication via direct matching of parts to a database of images, and neither Alitheon nor Creative Electron provided a report based solely

on their registration data. Perhaps most disturbing was the mismatching by Creative Electron of an unregistered clone to a registered authentic part.

The data reported from the Blind Study provide a snapshot of the accuracy, including false positives and false negatives, of the systems evaluated. A more detailed statistical analysis should be performed in order to predict the expected performance in a large scale deployment that might involve thousands or millions of parts.

The Image Analysis techniques that register parts into a database use the registered images as the reference for authentication of parts to specific, previously registered parts. This approach is not equivalent to counterfeit detection on the basis of comparison to a datasheet or data on a set of reference samples (i.e., exemplars or golden parts). Some of these tools can also be used to cluster or classify parts, in a similar manner to the Side Channel tools. In this mode, the results are obtained by unsupervised learning to cluster parts according to mutual similarities, or comparison to a set of reference samples. The Blind Study did not seek such results, and only Covisus provided them. Alitheon indicated that they have the capability to accomplish clustering but did not demonstrate it for this study.

When performing risk-based testing, as required by the DFARS when parts are purchased from other than the OCM or an authorized distributor or remanufacturer, there is a need to determine whether or not to accept the lot. Registration-based authentication of parts using Image Analysis only offers a means to make that determination if every part produced by an OCM has been registered into the databased used for matching. If the database is incomplete or inaccessible, then it becomes impossible to ensure that each part in a lot can be matched to the database. Secondly, if any authentication errors are made for individual parts within a lot resulting in their inability to be matched to a part in the database, then the standards require that the entire lot be rejected. This kind of false positive error can be costly both in terms of financial impact as well as readiness. Finally, even when parts can be matched to previously registered parts, authentication does not provide any information on how parts were stored, handled, used, or modified in the intervening period between registration and authentication. See Section VIII-B for a further discussion of these issues.

Alitheon claims that its tool has the capability of creating classes of parts by package type, part numbers, manufacturers, and combinations of them. However, there is no timeline for the introduction of this functionality. This can be one area for further development to make the tool useful for counterfeit avoidance. The concerns raised regarding systems that rely upon databases to determine whether a part is counterfeit must address the issues created by the passage of time (i.e., effects of storage, age, handling, and process changes) on the validity of image comparisons.

Over time, every single image taken can be considered used to augment the training data that can classify a part as belonging to a particular vintage. Ideally, Image Analysis would be broadened using incorporation of artificial intelligence to learn from the images it takes rather than simply matching them individually. This can help to compensate for incompleteness of the database or changes to part appearances due to age, storage, or handling.

Issues concerning database integrity and financial viability over the duration of several decades were discussed in the summary of the Side Channel Blind Study results above. The same concerns apply to the databases that would be used by Image Analysis tools for authentication. Furthermore, the efficiency of database access and search will need to be improved with scaling of implementation to many millions of parts. If each FeaturePrint is 100 kB in size, then a database containing 10 million unique FeaturePrints will be a terabyte in size. For the technology to be effective, the database must be comprehensive. Therefore, there will be a need to develop methods for selecting relevant portions of the database for any particular part type, data/lot code, or OCM, and for efficient search routines.

Image Analysis tools and methods can be useful as a supplement to standards-based testing. For example, AS6171-based testing is able to determine whether a part is suspect counterfeit, and can also detect defects that might be relevant to how a part was used or stored prior to testing. Image Analysis-based authentication could be a useful complement to that by indicating whether a part originated with an OCM by authentication against a database. This use of Image Analysis can only be realized after fairly comprehensive databases are created and maintained, and the Image Analysis systems are widely deployed and implemented.

Image Analysis also can be used to replace an element of standards-based testing, namely general external visual inspection (EVI) (see also Section VIII-B-1-b-ii). This use of Image Analysis would require further development of these systems to recognize defects that are indicators of suspect counterfeit devices. Automated optical inspection systems are already in use in many industries, including microelectronic, that have similar capabilities. Product development along these lines for counterfeit detection could provide this capability if the companies and/or DoD choose to support these efforts. As pointed out in VIII-B-1-b, the use of Image Analysis for Detailed EVI, or even x-ray inspection, is a more significant hurdle, but could be accomplished in theory with sufficient development effort. Candidate systems for these applications need not be limited to the three organizations that participated in the Blind Study. See Section VV. C. for a discussion of some candidate organizations and technologies.

Table 26 and Table 27 in the conclusions section include a summary of the results of Image Analysis testing along with those of Side Channel and conventional methods. Table 26 shows the detailed summary of results including both detection and clustering accuracy for clones and conventional

counterfeits separately and combined and Table 27 shows the same with both clones and combined counterfeit parts combined.

V. Task 2: Evaluation of Existing Machine-Vision and AI Technologies

A. Task 2a: Technology Readiness Assessment

CALCE performed a Technology Readiness Assessment[14] (TRA) using the U.S. Department of Defense Technology Readiness Assessment Deskbook[15] to analyze and identify each participating system's Technical Readiness Level[16]. Only aspects of the TRA Deskbook relevant (Appendix A: a template for a TRA, Appendix B: guidance on identifying Critical Technology Elements, Appendix C: guidance on assessing technology maturity) to the pilot program are used. CALCE established specific metrics for the assessment and generated a series of reports detailing the Critical Technology Elements and the Technical Readiness Level of each participating system. Those individual reports and the comparative conclusions are included in this report to DMEA.

This use of the TRL information can vary depending on the goals of the user. The US DOD and other government agencies can evaluate the return on investment in the context of research funding goals by assessing commercialization, availability, wide acceptance including standards, and IP use by the government. It is also possible that DoD would recommend using the tool to various agencies and prime contractors based on the usability in a DoD or contractor facility. The timeline and cost considerations will be different based on the use, such as inventory review, purchase from an unauthorized distributor, investigation of failure incidents (acceptability at internal adjudication, the building of cases, acceptance at the court of law). In all these cases, if the government asks a contractor to use a particular technology, the government may be committing to paying the cost, and the government may be indemnifying the company from future problems. One system may be more ready for a particular use while being unsuitable for different use. For uniformity, we made the following use assumption for TRL:

- For the Side Channel tools, the system's application is the inspection of components for counterfeit detection at the point of purchase or acceptance.

[14] An assessment of how far technology development has proceeded. It provides a snapshot in time of the maturity of technologies and their readiness for insertion into the project design and execution schedule.

[15] U.S. Government Accountability Office, "Technology Readiness Assessment Guide," 2016.

[16] A metric used for describing technology maturity. It is a measure used by many U.S. government agencies to assess maturity of evolving technologies (materials, components, devices, etc.) prior to incorporating that technology into a system or subsystem.

- For the Image Analysis tools, the assumption is that the system can identify the registered parts at any time after registration. Those parts can be loose, in their packaging (e.g., tubes, trays), on assembled boards, or taken off the boards for investigation.

Usability factors include coverage of parts and technology by functionality, package type, and required information to perform the counterfeit detection. The cost considerations include the cost of the equipment, the cost of personnel to run the equipment and analyze the data, and non-recurring engineering (NRE) costs. The NRE cost includes programming, fixtures, and machine learning training. Whether or not a method is useful also depends on the lead time and numbers and types of samples required.

A traditional technology readiness assessment evaluates technology on a stand-alone basis. For this evaluation, there is an element of comparison with the established tools and methodologies. These technologies are meant to replace (or complement) the traditional method of detection using analytical and visual tools. As a result, the technology needs to be compared among each other and the traditional methods. No TRL is available or calculated for the traditional methods for comparison. Hence, the comparison will traditional methods will need to include accuracy, cost, and time.

Another factor in the assessment is the organizations' business goals and mission. The TRL is estimated based on the assumption that a product is meant for commercialization by the developers. However, depending on the organization, the goals can include finding IP users and licensees, commercializing and selling the product for use by others, commercializing and providing detection as a service, or just publishing the findings as an academic exercise.

We have used the NASA TRL calculator (available as an open-source tool from the Defense Acquisition University (DAU). The questionnaire emphasizes an assessment of flight preparedness. For our assessment, we have considered the use conditions defined earlier to be equivalent to flight preparedness.

Since all the systems assessed have multiple subsystems and associated development items, a critical technology element[17] (CTE) for each counterfeit detection method is selected for the assessment. The TRL handbook defines that to be considered "critical," a technology must meet both of the following requirements: the system must depend on the technology to meet operational requirements and the technology element or its application must be "new or novel or in an area that poses major technological risk during detailed design or demonstration." The CTEs can be hardware or software.

[17] A technology element is "critical" if the system being acquired depends on the technology element to meet operational requirements (with acceptable development, cost and schedule; and with acceptable production and operations costs) and if the technology element or its application is either new or novel.

In a traditional technology readiness assessment, CTE's maturity during the acquisition process through each milestone of the acquisition process because knowledge of technology's maturity evolves. In this assessment, there is no active acquisition process. This TRL assessment assumes that this assessment will inform future decision making. In the absence of an active acquisition process, the suggested participants of a TRL estimation provided in the handbook do not exist, and the research team at CALCE performed the assessment. The CALCE team has used the following sources of information in this assessment:

- Company information
    - Company website
    - Company literature or literature about the company
    - Company presentations
        - Conferences
        - Public releases
    - Images or videos of the system
- Interviews by CALCE
    - Interviews with users and specialists
        - DoD
        - Subject matter experts, including members of the development team
    - Communications with company members
- Academic sources
    - Journals on the area of the technology
        - Conference papers and presentations
        - Archival journals
        - Trade magazines
- Patent landscape
    - Patent applications
    - Patents issued to companies as well as related patents

The TRL scale takes into account the operational environment defined as "Environment that address all the operational requirements and specifications required of the final system" and the relevant environment "Testing environment that simulates both the most important and most stressing aspects of the operational environment." Most test labs do not employ a "one-size-fits-all" approach but rather aggregate multiple tests, each one designed to detect a specific type of counterfeiting. For this assessment, we assume

that one single tool is used for the detection, and the technology is evaluated in isolation. Table 16 lists the definitions of the TRLs.

Table 16: Review of TRL Scale

TRL	Description
1	Basic principles observed and reported
2	Technology concept and/or application formulated
3	Analytical and experimental critical function and/or characteristic proof of concept
4	Component and/or breadboard validation in a laboratory environment
5	Component and/or breadboard validation in a relevant environment
6	System/subsystem model or prototype demonstration in a relevant environment
7	System prototype demonstration in an operational environment
8	Actual system completed and qualified through test and demonstration
9	Actual system proven through successful mission operations

1. Alitheon FeaturePrint

Alitheon FeaturePrint claims to link the physical and digital characteristics of a product. The FeaturePrint technology uses artificial intelligence and off the shelf cameras to register and subsequently identify objects that were registered earlier. Figure 9 shows the steps of the creation of FeaturePrint. First points of interest (POI) on an image are identified. An image can have hundreds of thousands of unique POI show. These POI are found in the random surface features created in the various fabrication processes. Image data is discarded after identifying the POI and the POI information is moved into an Image Analysis domain. The relative strength of each POI in the geometry and location within the boundary of the field of view is weighted. POI strength and the relationship between POI are evaluated. In the last step, the POI are transformed into a mathematical model and it is stored with specific use case metadata.

a. Basic information on the developers and technology:

- **Location:** Bellevue, Washington
- **Leadership:** Brian Crowley –President, David Ross –Chief Scientist, Director, co-founder
- **The size and portability of the method or device**: NA
- **Cost for the product**: based on the scale of the project and amount of integration – simple installation can be as low as $40,000 and price scales with volume and complexity

- **Resources and infrastructure required for testing**: connection to web servers as needed once a contract is in place. Secure on-premise solution is also available.
- **Preparations needed before testing can be performed**: conditions to take quality images of the item being tested (e.g., adequate lighting)
- **Numbers of samples needed**: None
- **The skill level and training of personnel required to operate equipment, to analyze data, and to interpret results**: Individuals can be trained on the basics of use within one or two hours. Data analysis is fully automated.

b. **Financials:**

- Annual revenue of $6.1m according to ZoomInfo in June 2020
- Annual revenue of $350k according to Dun & Bradstreet in August 2019 – they have not updated their findings since
- Annual revenue of $94k according to Dun & Bradstreet in May 2019

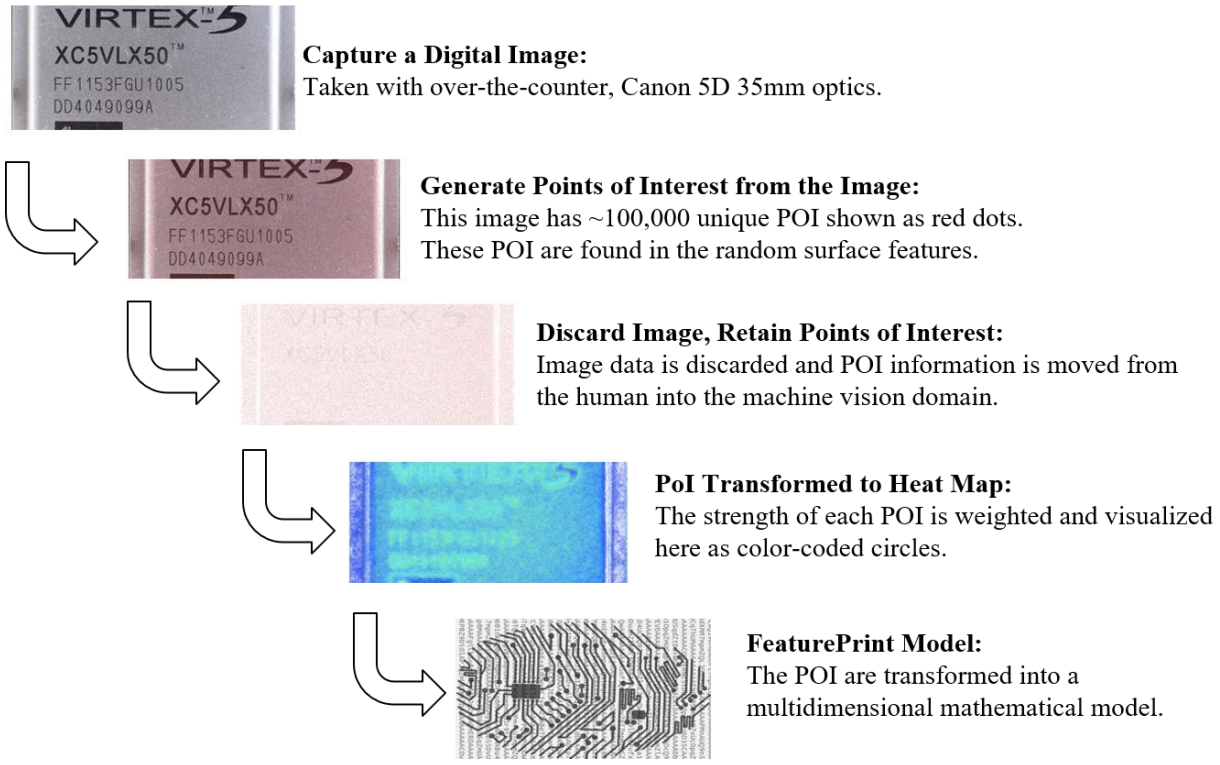


Figure 9: Schematic of the FeaturePrint System Step

Steps in use of the FeaturePrint System:

1. Capture & create a registration FeaturePrint when provenance is known

a. The object's unique physical attributes are extracted from a digital image to create the FeaturePrint

2. Log the FeaturePrint into the part registry
3. When required, create an authentication FeaturePrint for comparison
    a. Create a digital image of the target object, create the FeaturePrint, then compare the registration FeaturePrint to the authentication FeaturePrint.
4. Verify the identity and thereby the authenticity of a part when needed

c. Patents:

Table 17: Patent List Provided by the Company

	Alitheon Granted Patents	Patent Number	Date	Inventors
1	PRESERVING A LEVEL OF CONFIDENCE OF AUTHENTICITY OF AN OBJECT	10540664	1/21/2020	David Justin Ross; Justin Lynn Withrow; David Keesu Kim; Mark Tocci; Scot E. Land
2	PRESERVING AUTHENTICATION UNDER ITEM CHANGE	10346852	7/9/2019	David Justin Ross; Justin Lynn Withrow; Scot E. Land; David Keesu Kim; Mark Tocci; Robert Saxon
3	DATABASE FOR DETECTING COUNTERFEIT ITEMS USING DIGITAL FINGERPRINT RECORDS	10192140	1/29/2019	David Justin Ross; Brian J. Elmenhurst; Mark Tocci; John B. Forbes; Heather Wheelock Ross
4	PERSONAL HISTORY IN TRACK AND TRACE SYSTEM	10037537	7/31/2018	Justin Lynn Withrow; Mark Tocci; David Keesu Kim; David Justin Ross; Scot E. Land
5	DOCUMENT AUTHENTICATION USING EXTRACTED DIGITAL FINGERPRINTS	10043073	7/7/2018	David Justin Ross; Brian J. Elmenhurst; Mark Tocci; John B. Forbes; Heather Wheelock Ross
6	OBJECT IDENTIFICATION AND AUTHENTICATION	2825681	7/18/2017	David Justin Ross; Brian J. Elmenhurst
7	OBJECT IDENTIFICATION AND INVENTORY MANAGEMENT	9646206	5/9/2017	David Justin Ross; Brian J. Elmenhurst
8	DIGITAL FINGERPRINTING TRACK AND TRACE SYSTEM	9582714	2/28/2017	David Justin Ross; Brian J. Elmenhurst; Mark Tocci; John B. Forbes; Heather Wheelock Ross
9	DIGITAL FINGERPRINTING OBJECT AUTHENTICATION AND ANTI-COUNTERFEITING SYSTEM	9443298	9/13/2016	David Justin Ross; Brian J. Elmenhurst; Mark Tocci; John B. Forbes; Heather Wheelock Ross
10	DOCUMENT FINGERPRINTING	9350552	5/24/2016	Brian J. Elmenhurst; David Justin Ross
11	OBJECT IDENTIFICATION AND INVENTORY MANAGEMENT	9152862	10/6/2015	David Justin Ross; Brian J. Elmenhurst
12	AUTHENTICATION OF A SUSPECT OBJECT USING EXTRACTED NATIVE FEATURES	8774455	7/8/2014	Brian J. Elmenhurst; David Justin Ross
13	OBJECT IDENTIFICATION AND AUTHENTICATION	2967584	Pending	David Justin Ross; Brian J. Elmenhurst

i. Broader Patent List:

- **US8774455B2**
    - Document fingerprinting
    - 03/02/12 priority date
    - **US9350552B2**
        - A continuation
        - 05/29/14 priority date
- **US9152862B2**
    - Object identification and inventory management
    - 09/14/12 priority date
    - **US9646206B2**
    - A continuation
    - 08/31/15 priority date
- **CA2825681C**

    - Object identification and authentication
    - This is a Canadian patent
    - 08/30/13 priority date
- **EP2869240A3**
    - Digital fingerprinting object authentication and anti-counterfeiting system
    - 11/01/13 priority date
    - **US9443298B2**
        - USPTO equivalent
        - 11/03/14 priority date
- **EP2869241A3**
    - Digital fingerprinting track and trace system
    - 11/01/13 priority date
    - **US9582714B2**
        - The USPTO equivalent
        - A continuation of both US8774455B2 and US9152862B2
        - 11/03/14 priority date
- **US10043073B2**
    - Document authentication using extracted digital fingerprints
    - This is a division of US9582714B2
    - 02/15/16 priority date
- **EP3208744A1**
    - Multi-level authentication using a digital fingerprint of an object
    - 02/19/16 priority date
- **EP3236401A1**
    - Authentication-triggered processes
    - 04/18/16 priority date
- **EP3249581A1**
    - Controlled authentication of physical objects
    - 05/26/16 priority date
    - **US10614302B2**
        - USPTO equivalent
        - 05/19/17 priority date
- **EP3264330A1**
    - Centralized databases storing digital fingerprints of objects for collaborative authentication
    - 06/28/16 priority date
- **EP3267384A1**
    - Authenticated production
    - 07/05/16 priority date
- **US10192140B2**
    - Database for detecting counterfeit items using digital fingerprint records
    - This is a division of US9443298B2
    - 07/12/16 priority date
    - **US20180144211A1**

        - A continuation
        - 01/04/18 priority date
- **EP3270342A1**
    - Database records and processes to identify and track physical objects during transportation
    - 07/15/16 priority date
    - **US20180018627A1**
        - USPTO equivalent
        - 07/13/17 priority date
- **EP3282391A1**
    - Event-driven authentication of physical objects
    - 08/12/16 priority date
- **EP3285208A1**
    - Authentication-based tracking
    - 08/19/16 priority date
    - **US20180053312A1**
        - USPTO equivalent
        - 08/17/17 priority date
- **US10621594B2**
    - Multi-level authentication
    - 02/17/17 priority date
- **US10037537B2**
    - Personal history in track and trace system
    - 02/17/17 priority date
- **US10572883B2**
    - Preserving a level of confidence of authenticity of an object
    - 02/17/17 priority date
    - This is the exact same application number as US10290005B2
- **US10290005B2**
    - Preserving a level of confidence of authenticity of an object
    - 02/17/17 priority date
    - **US10540664B2**
        - A continuation
        - 03/25/19 priority date
- **US10346852B2**
    - Preserving authentication under item change
    - 02/17/17 priority date
    - **US20190287118A1**
        - A continuation
        - 06/04/19 priority date
- **EP3435287A2**
    - Model-based digital fingerprinting
    - 07/25/17 priority date
    - **US20190034694A1**

        - 07/25/18 priority date
        - US patent equivalent
    - **EP3514715A1**
        - Secure digital fingerprint key object database
        - 01/22/18 priority date
        - **US20190228174A1**
            - USPTO equivalent
            - 01/22/19 priority date
    - **EP3654239A1**
        - Contact and non-contact image-based biometrics using physiological elements
        - 11/13/18 priority date
        - **US20200153822A1**
            - The USPTO equivalent
            - 11/12/19 priority date

d. **Presentations:**

- David J. Ross, "Native Characteristics of Electronic Components for Identification and Authentication," in CALCE/SMTA Symposium for Counterfeit Parts and Materials, College Park, MD, June 25-27, 2019.

Information regarding the status of the product is provided in Table 18. The information presented in the table is obtained by direct communication and from the publicly available literature.

Table 18: Additional Information About Alitheon

Question	Answer
How many units are manufactured?	NA
Are units in stock or are they built against order?	NA
Do the units include software and database? Do the users have to subscribe for getting those features?	The software is included with the system and can be implemented for cloud or in-premise access.
Do you have a product data sheet?	There seems to be no datasheet, however, some general system information is provided via direct communication and through web site.
Do you offer support service?	Yes
Do you offer repair or upgrades?	Yes
What is the lead time to buy one?	Same as the time to assess the system requirement
What are you selling to customers?	Integrated implementation
What is the price of the unit?	Depends on complexity of implementation.
Are the units built outside of the company?	NA

For the purpose of this assessment, the process of generating FeaturePrint is considered as the Critical Technology Element (CTE). The TRA is performed for this CTE. Only software was considered for the assessment. It is found that the system has achieved TRL of 7 and had affirmative answers for some questions regarding TRLs 8 and 9. However, there is a need for individualized integration of the software with the vision system used by the customer and as a result, a TRL of 6 is assigned.

The company had been agile and responsive in communication and implementation. The registration step was completed for all ten parts but the process of data collection there did not make a classification among the parts. The authentication step was completed for six of the parts with a total of 120 parts, there is only one part for which it could not identify with confidence. We expect to get the results for the five other parts from them and they will be communicated to DMEA when available.

2. Covisus

Covisus is a Monrovia, CA based producer of vTag® technology for tracking and authenticating parts on the basis of surface texture (i.e., surface topographical information contained in optical images from the parts). Covisus is a subsidiary of Chromologic, Inc.

A vTag or virtual tag is a digital scan of the topographic surface features of an item. The scanned image comprises a type of "fingerprint" which can be obtained without physical contact or modification of the item, and which does not rely on the placement of a marker or tag on the item. Parts of unknown provenance can be tested against a database of known "good" images to assure authenticity and detect suspected counterfeits.

Covisus produces a vTag scanner that obtains images of parts in a manner that highlights their surface features. It accomplishes this through the use of dual or multiple light sources oriented at an angle off the normal axis from the sample surface. Alternatively, commercially available cameras or imaging optics can also be used to obtain an image, provided that they satisfy technical specifications such as resolution, exposure control, etc. However, the vTag scanner is the preferred hardware for image acquisition.

Images are analyzed using their DTEK software. The Covisus website describes their DTEK Application as using "vTag® technology to provide counterfeit mitigation at incoming receiving and inspection as part of a holistic quality system." The system extracts features of the surface that are analyzed using machine learning algorithms. vTags of the top and bottom of a part can be compared to each other or to other parts within a lot, and can be compared to those of a reference part (a known authentic part) if one is available. Covisus claims a throughput of about 1 minute per part at present. Imaging is presented as being independent of part orientation, flexible with respect to part size/magnification, and able to adapt

illumination to surface characteristics. Future capabilities are being developed under the moniker DTEK+, and will allow increased throughput, automation in the collection of vTags, and evaluation of other features of microelectronic parts such as leads and markings.

The microelectronics market for this technology is developing slowly, which has limited the manufactured volume. Several vTag scanners have been sold commercially, including at least one to a DoD prime contractor. Similar systems, including QuanTEK systems that provide traceability of parts in the supply chain, are being marketed to other industries including pharmaceuticals and machine parts/materiel.

A summary of Covisus's corporate information follows.

a. **Corporate Information**

- Incorporated in 2011 in California
- Merged on October 9, 2019 in Delaware under the same name
- Now incorporated in DE
- Headquartered at 1225 S. Shamrock Ave., Monrovia, CA 91016

- **Officers and Directors**
  - Naresh Menon – CEO
  - Theresa Nguyen – Senior Director
- **Financial Information**
  - Annual revenue of $116,515 as of February 25, 2020 according to Dun & Bradstreet
  - Has 1,000,000 shares of common stock upon merger
- **Company size**
  - Single Location in Monrovia, CA
  - Subsidiary of ChromoLogic
  - 3 employees according to Dun & Bradstreet
- **Intellectual Property Related to the Technology Under Assessment: Trademarks**
  - vTag
- **Public website: https://covisus.com/**

Covisus is a subsidiary of ChromoLogic. Naresh Menon is CEO of both organizations, and the IP pertaining to the vTag and DTEK technology is held by ChromoLogic. Corporate information and intellectual property holdings of ChromoLogic is presented here also.

- **Corporate Information**
  - Founded on July 23, 2008 in California
  - Headquartered at 1225 S. Shamrock Ave., Monrovia, CA 91016

- **Officers and Directors**
  - Naresh Menon – CEO, Managing Member, Owner
  - Theresa Nguyen – VP, Finance and Administration
  - Claude Rogers - Director
- **Financial Information**
  - $4.5m annual revenue according to ZoomInfo in June 2020
  - Between $1m - $10m annual revenue according to LexisNexis Corporate Affiliations in June 2020
  - $4.8m annual revenue according to Dun & Bradstreet in April 2020
  - At least $2m annual sales according to Experian in April 2020
- **Company size**
  - Single Location in Monrovia, California at the same location as Covisus
  - 15 employees according to LexisNexis Corporate Affiliations in June, 2020
  - 28 employees according to Dun & Bradstreet in April, 2020
  - 15 employees according to Experian in April, 2020
- **Business Analysis**
  - Given a low-medium business delinquency risk by Experian in April, 2020
    - The company is trending positively
  - Given a low business stability risk by Experian in April, 2020
  - No records of bankruptcies or adverse judgments
  - Two filings with the UCC in 2013
    - Collateral listed as equipment, furniture and fixtures, and inventory, now and after-acquired
- **Intellectual Property Related to the Technology Under Assessment: Patents**
  - For the most part their work is in ocular monitoring and membrane preservation
  - US10341555B2
    - Characterization of a physical object based on its surface roughness
    - Priority date of 10/10/12
- **Intellectual Property Related to the Technology Under Assessment: Trademarks**
  - ChromoLogic
  - Mir-Clear
  - Covisus

For the purposes of the Technology Readiness Level assessment, the Critical Technology Element (CTE) that was the basis for assessment was the hardware (vTag scanner) and software system (DTEK) as

a combination, that acquires images of the parts containing surface texture information, generates the vTag that is characteristic of the surface, and evaluates the vTag for the DUT against those of other parts under test or contained within a database.

The NASA TRL worksheet was used for the initial assessment and has been reproduced in Appendix 17, along with their product brochure. In addressing the requirements for the TRL assessment, the following assumptions or observations affected the assessment:

It is assumed that performance predictions and modeling and simulation have been performed under controlled use conditions. Some relevant end use conditions have been evaluated but not the full range of relevant end use environments for deployment across DoD in terms of associated reliability and measurement accuracy.

In discussions with Dr. Naresh Menon, the CEO of Covisus, it was understood that a desktop vTag scanner costs approximately $20,000. A handheld version is under development which would cost several thousand dollars.

The following additional information was considered, which was provided by Dr. Menon in an email communication:

Table 19. Additional Information About Covisus

Question	Answer
What is the product that you are selling to customers?	We are currently selling DTEK that identifies non-conforming parts in a lot or compared to a known golden part based on a non-contact surface texture analysis.
What is the critical technology element?	Ability to capture surface texture and use it to a) track and trace it and b) classify components
How many units have been manufactured?	~50 in different form factors (handheld, benchtop and robotic)
Are units in stock or are they built to order?	We use just-in-time builds. Parts are in stock but final assembly is customized to customer spec
What is the plan for ramping up production in the event that demand increases?	We have contractor manufacturers in place. We can build in-house 2-5/week
What is the lead time to buy a unit?	1 week
What is the price of the unit?	Depends on customer configuration (manual to full automation) and ranges from $5K to $100K
Are the units built outside of the company?	Some assemblies are built at contract manufacturers
Is the infrastructure in place to support and service 100 fielded units? 1000 fielded units?	Yes.

Question	Answer
Do the units include both software and a database of signatures of authentic parts? Do users have to pay extra or subscribe for software or database features?	We lease our hardware and have a software as a service model.
Do you have a product data sheet?	Yes
Have units been qualified for office/laboratory use, including measurement quality and reliability?	Yes. They have been deployed at NSWC Crane, and other sites
Have units been qualified for outdoor/uncontrolled environment use, including measurement quality and reliability?	No. However, we have no fundamental challenges to use it outdoors
What support services are offered?	Software support, warranty and product maintenance service
Do you offer repair or upgrades?	Yes. Multiple options are available.
What is the typical preparation time to test a new part/package type (including fixturing, testing, and training)?	20 minutes or less with training.

Based on the inputs to the NASA TRL Calculator, a TRL of 4 has been fully achieved by the Covisus vTag scanner/DTEK system, with a partial TRL of 5 (partially satisfied, or Yellow Level). The supplemental information listed above resulted in an upward modification to this assessment by one level, producing a final TRL of 5 (complete) with a partial TRL of 7.

3. Creative Electron X-Ray Fingerprinting

Creative Electron uses x-ray images as the unique fingerprint for an electronic component or PCBA. These features in the x-ray image can be used in tandem to create a unique fingerprint for a single component or an entire PCBA. This technique can also be expanded to mechanical objects by utilizing other idiosyncratic features of the part – such as defects and porosity – to generate the x-ray image fingerprint.

The x-ray image fingerprint is calculated using unique algorithms and inserted into a custom database. Unlike taggants, the x-ray image technique does not allow for any adulteration because we do not add any material to the component. Instead, the x-ray image fingerprint technique uses features of the material itself to generate the fingerprint.

Later in the supply chain, to read back these features to verify the authenticity of the component or PCBA, the user needs to image the part back with a compatible x-ray machine. The type of the part under inspection will determine which locations and features are to be used to retrieve the fingerprint from the database. The same algorithms are then used to determine if any changes have occurred to the part, and if the part is the same as introduced in the database.

a. Basic information on the developers and technology:

- **Location:** San Marcos, CA
- **Leadership:** Dr. Guilherme (Bill) Cardoso – President, CEO, CFO, director
- **The size and portability of the method or device**: Not applicable
- **Cost for the product**: Scalable
- **Resources and infrastructure required for testing**: connection to web servers as needed for comparison.
- **Preparations needed before testing can be performed**: conditions to take x-ray images of the item being tested
- **Numbers of samples needed**: not a set value
- **The skill level and training of personnel required to operate equipment, to analyze data, and to interpret results**: Individuals can be trained on the basics of use in a short time. Data analysis is automated.

b. Foundation and General Information

- Incorporated in California on May 30, 2008
- Headquartered at 201 Trade St., San Marcos, CA 92078
- Well-known for their manufacture of x-ray tech

Size

- Number of employees
- 42 according to ZoomInfo in June 2020
- Between 101 and 500 according to NetWise Company Profiles in September 2019
- Seems to only have one location in San Marcos, CA

Competitors

- Astrophysics, Inc.
- ETM Electromatic Incorporated
- Machine Vision Products, Inc.
- Rapiscan Systems, Inc.
- Saki Corporation
- SARA, Inc.
- The Gendex Corporation
- YESTech, Inc.

c. **Financials**

- $2.9m annual revenue according to Dun & Bradstreet in June 2019
- Between $1m and $5m annual revenue according to Experian in April 2020

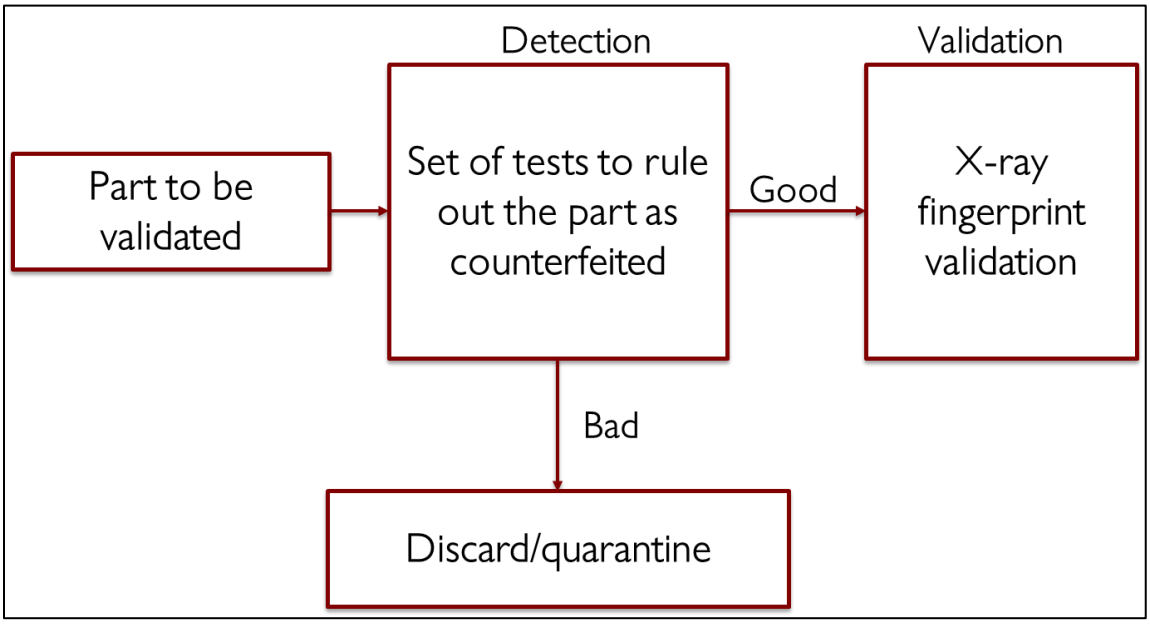


Figure 10: Schematic of the Fingerprinting System

Steps in use of the Fingerprint System:

1. Parts are X-rayed, 100% of lot should be done
2. AI looks for features including:
    a. Inconsistent die size
    b. Inconsistent lead frame
    c. Wire bond issues (missing, broken, incorrect diagram)
    d. Missing die
    e. Inconsistent die attach voiding
3. A fingerprint is created based on the defects found which are unique to the part or PCB
4. Features used for establishing the fingerprint:
    a. Wire bonds
    b. Die attach voids
    c. Component solder voids
    d. Pin alignment
    e. Solder distribution
    f. Fillets on pads

g. Through-hole via fills

5. Machine learning algorithms measure relative distance between reference images and test part

d. Patents:

- Have patents related to X-ray devices, but nothing related to the Image Analysis aspect.
- No new patents since 2015

e. Presentations:

- B. Cardoso, "A New Method to Authenticate Components and PCB Assemblies Using Fingerprint from X-Ray Images," International Symposium for Testing and Failure Analysis, Phoenix, AZ, 2018.
- B. Cardoso, "Can AI Help Us in the Fight Against Counterfeit Components?" in Symposium on Counterfeit Parts and Materials, College Park, MD, 2019.

f. Articles:

- B. Cardoso, "A New Method to Authenticate Components and PCB Assemblies Using Fingerprint from X-Ray Images," International Symposium for Testing and Failure Analysis, Phoenix, AZ, 2018.

Additional information regarding the status of the product is provided in Table 20. The information presented in the table is obtained by direct communication with the company and from publicly available literature.

Table 20: Additional Information About Creative Electron

Question	Answer
How many units are manufactured?	NA
Are units in stock or are they built against order?	NA
Do the units include software and database? Do the users have to subscribe for getting those features?	The software is included with the system and can be implemented for cloud or in-premise access.
Do you have a product data sheet?	There seems to be no datasheet, however, some general system information is provided via direct communication and through web site.
Do you offer support service?	Yes
Do you offer repair or upgrades?	Yes
What is the lead time to buy one?	NA

Question	Answer
What are you selling to customers?	Implementation
What is the price of the unit?	Depends on complexity of implementation.
Are the units built outside of the company?	NA

The FingerPrint development software is considered as the Critical Technology Element (CTE) and the TRA is performed for this CTE. Only software was considered for the assessment. The system has achieved TRL of 5 as per this assessment.

Delays marked the communication with the company in the registration period. The four weeks it took for the initial registration caused a slip in the schedule for the Image Analysis portion of the blind study. The study results had been mixed, and as shown in the results summary, the detection is far from perfect. While CALCE is performing additional studies on the reasons for those discrepancies, it is still a concern, and based on that, we choose to adjust the TRL to 4.

4. Summary of TRL Assessment of Image Analysis Technologies

Table 21: TRL Summary (Image Analysis)

Company	Critical Technology Element	Focus of Assessment	TRL Complete (Partial)
Alitheon	The process of generating FeaturePrint	Software	6 – (up to 9)
Covisus	Covisus vTag scanner/DTEK system	Hardware Software	5 (7) 5 (7)
Creative Electron	The FingerPrint development software	Software	4

B. Task 2b: Evaluation of Effectiveness, Strengths, and Weaknesses of Technologies

For further in-depth discussion of the limitations and recommendations regarding Image Analysis technology, including how the technology should be further developed, see Section IV-B, subsection titled "Observations and conclusions regarding the Image Analysis portion of the Blind Study".

Table 22: Alitheon

Hardware Assurance Issue that is being addressed	How the technology is being applied
Conventional counterfeit	Can detect, if registration process is in place across the supply chain, and provided that counterfeit parts are not registered due to a security failure

Cloned counterfeit	Can detect, if registration process is in place across the supply chain, and provided cloned counterfeit parts are not registered due to a security failure
Tampering	Internal hardware modification is not covered
Tracking and tracing	The primary application for which the technology was developed, and it is possible to track movement of individual items through the supply chain from manufacturing through use and disposal
Limitations	**Recommendations on how the technology should be further developed to help solve existing, as well as future Hardware Assurance Issues**
Lack of classification by product	Development of the capability of creating classes of parts by package type, part numbers, manufacturers, and combinations of these
Lack of original manufacturer participation	Integration with track and trace activities that part manufacturers are already willing to undertake today, and that they will expand into in the future (such as Industry 4.0 and IPC 1782 traceability standard)
Integration with production process and ability to use for inline, real-time decision making	Implementation to allow synchronization with the manufacturing and assembly steps where imaging takes place; and Development to improve the efficiency of the registration and authentication steps to keep up with the speed of the manufacturing process
Lack of defect identification/ inability to satisfy requirements of industry standards for visual inspection[18]	Development of this technology to recognize physical defects that are indicators of suspect counterfeit devices, and to comply with requirements for General, and possibly Detailed, External Visual Inspection (e.g., AS6171/2A, AS6081)
Data security	Demonstrated methods to detect and eliminate data security breaches, and restore original data (including distributed ledger implementation)
Business stability (e.g., change of focus, merger/acquisition, or financial insolvency)	Development of business and data sharing model where customers (including DoD) will have continued access to data necessary for continued use of system over several decades
Efficiency of database access and search with scaling of implementation	Develop methods for selecting relevant portions of a database that is possibly many terabytes, and for efficient search routines
Impacts of imaging technology changes	Development of backward compatibility with configurations that were used to collect baseline images, or development of methods of recalibration to account for technology changes

[18] See Section VIII-B-4-a.

Table 23: Covisus

Hardware Assurance Issue that is being addressed	**How the technology is being applied**
Conventional counterfeit	Can detect, if registration process is in place across the supply chain, and provided that counterfeit parts are not registered due to a security failure
Cloned counterfeit	Can detect, if registration process is in place across the supply chain, and provided cloned counterfeit parts are not registered due to a security failure
Tampering	Internal hardware modification is not covered
Tracking and tracing	The primary application for which the technology was developed, and it is possible to track movement of individual items through the supply chain from manufacturing through use and disposal
Limitations	**Recommendations on how the technology should be further developed to help solve existing, as well as future Hardware Assurance Issues**
Lack of classification by product	Development of the capability of creating classes of parts by package type, part numbers, manufacturers, and combinations of these
Lack of original manufacturer participation	Integration with track and trace activities that part manufacturers are already willing to undertake today, and that they will expand into in the future (such as Industry 4.0 and IPC 1782 traceability standard)
Integration with production process and ability to use for inline, real-time decision making	Implementation to allow synchronization with the manufacturing and assembly steps where imaging takes place; and Development to improve the efficiency of the registration and authentication steps to keep up with the speed of the manufacturing process
Lack of defect identification/ inability to satisfy requirements of industry standards for visual inspection[19]	Development of this technology to recognize physical defects that are indicators of suspect counterfeit devices, and to comply with requirements for General, and possibly Detailed, External Visual Inspection (e.g., AS6171/2A, AS6081)
Data security	Demonstrated methods to detect and eliminate data security breaches, and restore original data (including distributed ledger implementation)
Business stability (e.g., change of focus, merger/acquisition, or financial insolvency)	Development of business and data sharing model where customers (including DoD) will have continued access to data necessary for continued use of system over several decades

[19] See Section VIII-B-4-a.

Efficiency of database access and search with scaling of implementation	Develop methods for selecting relevant portions of a database that is possibly many terabytes, and for efficient search routines
Impacts of imaging technology changes	Development of backward compatibility of upgrades to the hardware with configurations that were used to collect baseline images, or development of methods of recalibration to account for technology changes

Table 24: Creative Electron

Hardware Assurance Issue that is being addressed	**How the technology is being applied**
Conventional counterfeit	May be able to detect the defects that are visible in x-ray images
Cloned counterfeit	May be able to detect the defects that are visible in x-ray images. Can detect if registration already took place for the same component but registration of cloned components will be an evidence of failure of the process
Tampering	Internal modifications in package level interconnects may be detectable
Tracking and tracing	Not as good as other two tools
Limitations	**Recommendations on how the technology should be further developed to help solve existing, as well as future Hardware Assurance Issues**
Lack of classification by product	Development of the capability of creating classes of parts by package type, part numbers, manufacturers, and combinations of these
Lack of original manufacturer participation	Integration with track and trace activities that part manufacturers are already willing to undertake today, and that they will expand into in the future (such as Industry 4.0 and IPC 1782 traceability standard)
Lack of defect identification/ inability to satisfy requirements of industry standards for X-ray inspection	Development of this technology to recognize physical defects that are indicators of suspect counterfeit devices, and to comply with requirements for X-ray Inspection (e.g., AS6171/5, AS6081)
Data security	Demonstrated methods to detect and eliminate data security breaches, and restore original data (including distributed ledger implementation)
Business stability (e.g., change of focus, merger/acquisition, or financial insolvency)	Development of business and data sharing model where customers (including DoD) will have continued access to data necessary for continued use of system over several decades
Efficiency of database access and search with scaling of implementation	Develop methods for selecting relevant portions of a database that is possibly many terabytes, and for efficient search routines

Impacts of imaging technology changes	Development of backward compatibility with configurations that were used to collect baseline images, or development of methods of recalibration to account for technology changes

C. Task 2c: Recommendations on How the Technology Should Be Further Developed to Help Solve Existing and Future Hardware Assurance Issues

In the course of the Blind Study and related investigations, Image Analysis and related Side Channel technologies were found to have certain limitations, uncertainties, and inconsistencies, whose resolution could improve the potential for those technologies to fulfill the objectives of counterfeit detection and prevention. In this section, CALCE has proposed immediate and incremental topics of study to achieve these goals.

1. Correlation of Image Analysis and Side Channel results with physical defects:

The results produced by Side Channel methods, and to some extent the Image Analysis methods, are essentially black box outputs. They do not reveal specific physical defects associated with counterfeit parts in the way that conventional, standards-based tests are capable of. Consequently, the acceptance of a finding of counterfeit for a lot in an actual purchasing transaction may not be accepted by all parties, and yet cannot be easily justified without recourse to conventional testing. Even after these tools have attained a high level of technology readiness and reliability, it will continue to require a leap of faith to accept findings that are based purely on the application of mathematical algorithms to data. This development of correlation will help develop that confidence level. In particular, this kind of correlation can help to explain differences in accuracy of detection or classification between two technologies for the same part number (e.g., differences between the KILO and ECHO criteria used by Covisus, or the different success rate for the same part number between the Sandia PSA and Battelle Barricade tools).

2. Development of Assembly-level (PCB-level) applications of Image Analysis:

DoD needs to manage the authenticity and integrity of the next level of hardware integration, such as circuit cards and modules. The use of COTS items at this level offers a different challenge to counterfeit detection. Since the bill of materials and construction details for assemblies are hard to access, the detection of counterfeit parts through traditional inspection methods is difficult. The Image Analysis-based tools can provide tracking of assemblies as well as the individual components mounted on those assemblies. Components in an assembly that are tagged as different from other assemblies can be an indication of problems with supply chain/quality control with the manufacturer of the assembly, but they can also be evidence of unauthorized repair/refurbishment or even tampering.

3. Iteration of the Blind Study with separate, homogeneous lots, and larger sample size:

The selection of the samples for the MASER Blind Study were limited to the availability of previously identified counterfeit parts. In addition, this was a pilot study of limited scope, size and duration. An expanded study would be designed as a true round-robin, with a single set of parts being evaluated by all participating companies. That will provide a better comparative evaluation of the methods, including the required logistics, non-recurring engineering (NRE) preparation, and costs, as well as their accuracy. Evaluation of the complexity, costs, and time required for development of fixtures and sockets would be part of the NRE assessment.

4. Analysis of Battelle Barricade data reference samples:

Battelle procured "authentic" reference parts for use in training their algorithms prior to classification of the Blind Study test samples. A re-analysis of the Blind Study data should be performed by Battelle without the use of the data on the reference parts, employing unsupervised learning to cluster the test parts, comparable to the process used by Sandia and PFP.

5. Authentication study with more aggressive physical damage:

Assessment should be performed of other stress aging methods that can impact side-channel performance and Image Analysis such as thermal cycling, mixed flowing gas, temperature-humidity, and high temperature operation. In the MASER Blind Study, the severity of the surface damage was mild for the parts evaluated by Alitheon. Such external damage also did not have any bearing on the performance of Creative Electron. An extension of the MASER study with more aggressive stress exposure will be able to find the limits of the detection and authentication capabilities for these methods.

6. Follow-up TRL Assessments:

Technology Readiness Level is an evolving characteristic of an organization. A number of the organizations that were included in the TRL assessments in this study are in a transitional or active development phase. Some of the organizations expressed their intention of using outside companies to commercialize their technologies. TRL assessments of organizations from this study that are of continuing interest to DoD, as well as of other organizations with promising technological solutions for counterfeit detection and prevention, should be performed as a follow-up to this effort. Future TRL assessments will include the site visits that could not be conducted due in 2020 due to the coronavirus outbreak. DoD practices indicate that use of the same SMEs for follow-up assessment is preferred in order to ensure consistency of the findings.

7. Analysis of defects from conventional testing Blind Study:

The Blind Study of conventional testing included the completion of spreadsheets containing a list of counterfeit defects for each test method, by individual parts. This is a valuable set of data that has never been gathered before in a similar study. An analysis of these defect sheets can potentially lead to quantification of test method efficacy; a statistical Pareto of the distribution of defects by counterfeit type; development of the optimal order by which tests should be performed; counterfeit defect coverage (CDC) and counterfeit type coverage (CTC) by specific methods; and discovery of potential new defects or modification of the definition of existing defects. This process can revolutionize the traditional test methods and inform the various international standards committees.

8. Exploration of thermal methods for counterfeit detection:

A promising method for nondestructive testing of counterfeit electronics is infrared thermography (IRT). Thermography is one class of thermal-based methods that involves the analysis of the thermal characteristics of a component. Some other thermal-based tools include thermoreflectance and characterization of the thermal structure-function based on the thermal impedance of the various layers and interfaces that make up the package, such as the die attach or molding compound. Certain counterfeit defects can manifest themselves with changes in thermal characteristics and interface layers. Selection of promising thermal characterization technologies and evaluation of their efficacy for counterfeit defect definition and detection will be beneficial.

9. Additional technologies that should be considered in future evaluations.

i. MIT-Lincoln Laboratories SICADA

Although MIT-Lincoln Laboratory's SICADA system is a relevant Side Channel method, they were not able to participate in the blind study. The following is a statement from Eric Koziel providing the administrative reasons why they could not participate. This is a technology that should be evaluated in any future studies of Side Channel technologies for counterfeit detection or supply chain security.

> "MIT Lincoln Laboratory's SICADA platform was a candidate for study this year, however several circumstances limited their ability to participate. One major issue was the availability of staff time under the current STE constraints, as outlined in DoDI 5000.77 Section 8. Simply put, there's a limit to how much staff time can be applied to DoD funding within a year, and Laboratory management determines which programs get priority for expending STE. SICADA was de-prioritized in 2019 to give further focus to other ongoing programs. Additionally, several technical challenges exist in adapting SICADA to perform

on any given set of parts. At present, SICADA has not created a general-purpose testing fixture that can be applied to a broad range of packages or pinouts. Each current fixture is created to match the particular package and pinout for the device family to be tested. To satisfy study requirements, MITLL would need engineering time to create fixtures for all parts to be tested, or alternatively spend significant engineering time to develop one or more flexible modular fixtures.

"For MITLL to be included in future studies, a government entity such as DMEA would need to reach an agreement with MITLL management that SICADA be prioritized for further development time. With sufficient additional development time, the SICADA team could develop the fixtures and stimulus necessary to complete testing across the range of parts included in the study."

ii. Cybord:

CALCE has communicated with an Image Analysis-based solutions provider from Israel, Cybord (https://cybord.ai/), having spoken with its CEO Zeev Efrat and CTO and founder, Dr. Eyal Wiess. This company obtains optical images of components during reel to reel transfer and during the pick and place operation from carrier to board, getting both top and bottom images. These images are used to build databases and machine learning algorithms, which are then used to flag components for later evaluations. It also created libraries for some common counterfeit-related defects that can be used to flag parts based on the presence of such defects.

iii. Sciotex and Keyence:

CALCE has communicated with an automated inspection company called Sciotex. Sciotex employs imaging equipment and collaborates with Keyence, an advanced microscopy company. Sciotex claims to have Image Analysis systems tuned for Quality Inspection, Detecting Defects, Grading and Scoring Product, Pallet Inspection, Counting and Identification, and Gauging and Measurement. After the discussion with CALCE, Sciotex has shown a willingness to work in the future with CALCE to identify and collect test targets that are representative of micro-electronic components. Once a study has been designed and funded, Keyence and Sciotex will assemble the proper equipment for testing and perform an early stage evaluation, using software that will be written by Sciotex specifically for the trial. The generated data will be used to develop a test report highlighting system capability and gather cost estimates.

iv. Imaris/Oxford Machine Vision System

Swiss corporation Oxford Instruments owns Bitplane, a Concord, MA-based company that produces IMARIS software. This software provides 3D/4D viewing of microscopy images. The software is intended for biological researchers, although it should be adaptable to other applications. IMARIS software has been used extensively in processing microscopy images of biological applications, which have comparable complexity to images generated of microelectronic components. However, it has not been tested on electronic components. Oxford has expressed a willingness to explore applications in microelectronics.

VI. Task 3: Evaluation and Development of Solutions for the Microelectronics Supply Chain for Possible Implementation by Program Managers

The threats posed to the Defense microelectronics supply chain include those associated with conventional counterfeit parts (e.g., remarked or resurfaced, or used parts sold as new); clones (which can be categorized as advanced counterfeits); and tampered parts (another type of advanced counterfeit, consisting of parts containing undisclosed and/or malicious functionality). As discussed in Section VIII-A, these threats are currently being addressed through a combination of measures including policies regarding part procurement, risk-based testing for counterfeit detection, reporting of suspect counterfeit devices, segregation of suspect counterfeit devices, and enforcement. Although standards-based testing, embodied by the methodology in SAE AS6171, has the ability to detect all three forms of counterfeit device listed above, the current form of the standard claims low coverage of both clones (less than 10% counterfeit type coverage with all but the most elaborate test sequences involving design recovery, AS6171/11), and tampered devices (which are not within scope of the standard, and would again only be covered in the existing standard to any appreciable degree by design recovery). The results of the Blind Study using conventional testing that has been reported here in Section IV IV. B. provide strong support for upward revision of clone coverage. It should be noted that revisions to AS6171 are actively underway that would add tampered devices to the scope, together with new and revised test methods that would target tampered devices and improve coverage of clones as well as conventional counterfeits.

Tampered devices straddle the boundary between counterfeits and hardware integrity-related threats, in that they are misrepresented to the purchaser or end user in the same way as other counterfeit devices, but may possess a level of technological sophistication associated with malicious intent rather than pure financial motivations. Clones could fall into a similar category of security threat if they are designed and produced with malicious intent by nation-states or other technologically capable actors.

All of the above threats are addressed by DoD Instruction 5200.44. As described in Section VIII-A-4-d, this Instruction implements DoD's Trusted Systems and Networks ("TSN") strategy to manage risks to system integrity and trust. It articulates a cybersecurity policy that integrates counterfeit detection and prevention with other supply chain risk management and hardware/software assurance disciplines. It further calls for implementation of item unique identification (IUID) for national level traceability of critical components in accordance with DoDI 8320.04. In the latter instruction, the IUID is defined as "A system of establishing globally ubiquitous unique identifiers on items of supply within DoD, which serves to distinguish a discrete entity or relationship from other like and unlike entities or relationships." Among the items for which IUIDs are required are those that satisfy a management need, as determined by relevant DoD components, for "Counterfeit prevention for critical materiel identified as susceptible to counterfeiting."

Image Analysis and related Side Channel technologies offer a potential, or at least partial, solution to the requirement for IUIDs on microelectronic devices, insofar as they are able to classify devices as members of a group of authentic parts originating with a particular OCM, and in some cases are able to match individual parts uniquely based on device-specific signatures. These potential solutions need to be viewed in light of the concerns and caveats expressed elsewhere in this report, in Section IV-IV. A. , where Side Channel TRL assessments have been presented; in Section V-V. A. , where Image Analysis TRL assessments have been presented, in Section IV-IV. B. , where blind study results have been presented, and in Section V-V. B. , where strengths and weaknesses of the Image Analysis technologies have been described.

A. Task 3a: Demonstration of Near-term Solutions

1. Known Good Virtual Golden Samples

A series of tests was performed to demonstrate the use of the Battelle Barricade system and its associated database for securing the microelectronic supply chain by authenticating parts against previously acquired data. The Barricade system has been developed with the objective of providing a means to classify microelectronic devices as members of a group of known good virtual golden samples; i.e., using a database of previously tested parts of known provenance to the OCM or an authorized source, which can therefore be considered authentic and known good, one can determine whether a device under test is sufficiently similar in its characteristics to be considered a member of that class, and thus can be labeled authentic, or is not sufficiently similar, and thus may be labeled suspect counterfeit. The demonstration was meant to simulate a scenario in which parts had been tested when they were known to be authentic, and then several years later, using a different Barricade system that might be located at a distributor, depot, or contractor

location, the same kind of parts were tested after they had been purchased from a supplier on the open market (i.e., not from an OCM or authorized source), in order to determine whether the parts were authentic.

Initial testing by Battelle:

Battelle tested the 10 authentic (marked as 08394 = date code 1839) and 12 cloned (marked as 07024 = date code 1702) Altera EPCS4SI8N parts that were used in our blind study on their Barricade system (Figure0). The results were compared to the data that SMT Corp. had collected using their Barricade system in September 2018 on authentic and cloned parts of the same part number (Figure 11), in a collaboration from that time period with SMT Corp. The testing was thus performed using identical fixtures and test methods but two different Barricade units. The SMT data included different lot/date codes of both clone and authentic parts. There were several hundred test points in the SMT data, including test points that had been collected on authentic parts from two different date codes (07174 and 07134). Upon analysis and comparison of the results (Figure), Battelle found that the new data from neither the clones nor the authentic parts matched up with any of the clusters from the previously collected SMT data. In fact, Battelle stated that the new data were more similar to each other than they were to any of the previously collected data, although the new data could easily be separated into two groups, and the old SMT data clearly exhibited two clusters (one along the diagonal, and the other above and to the left of the diagonal cluster).

When Battelle performed the Blind Study, they used multiple tests on each part, consisting of different test vectors, to collect a diverse set of features that could be analyzed using bagging algorithms to improve classification. Since the old SMT data was collected with just one test per part, because the bagging algorithm has been introduced more recently, Battelle used just one test per part and did not attempt bagging for the purpose of this demo.

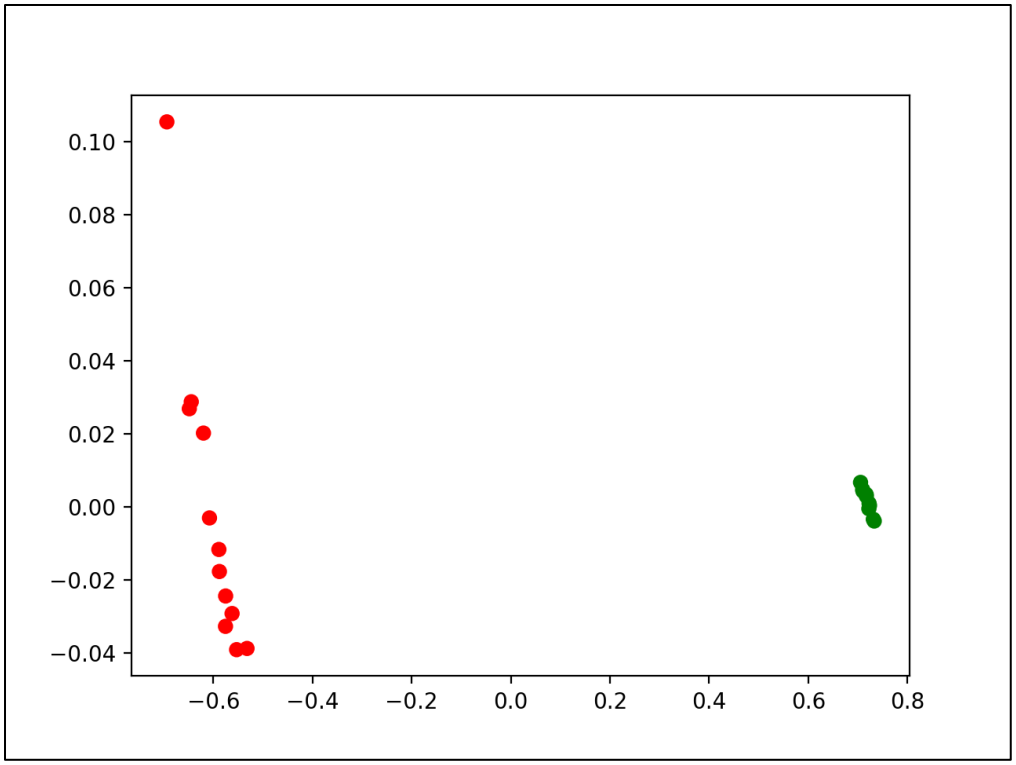


Figure 10. Principal Component Analysis (PCA) Plot of Data Captured by Battelle in 2020 on Altera EPCS4SI8N parts. Red: Clones (07024); Green: Authentic (08394)

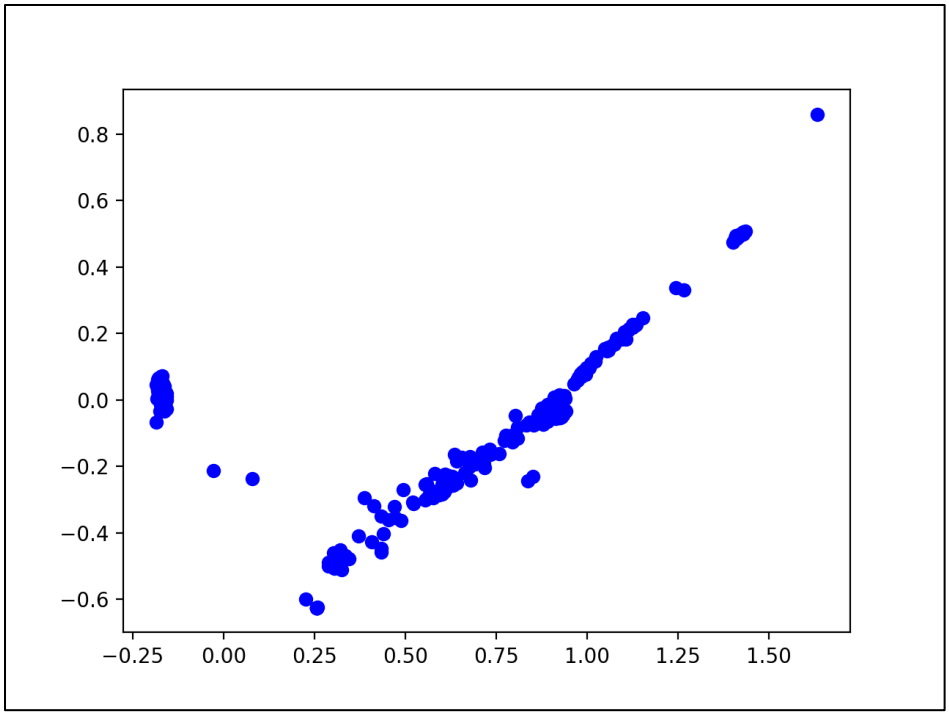


Figure 11. PCA Plot of Data Captured by SMT in 2018 on Altera EPCS4SI8N parts (both clones and authentic).

This attempt to simulate an authentication ran into trouble because the configuration of Battelle's current system is different from the older system that was used by SMT to collect the original data. Between the time that SMT ran their testing in 2018 and Battelle performed their testing, they installed a filter in the Barricade system. The frequencies are the same but the peak-to-peak is attenuated in the recent data, which reduces saturation and allows Battelle to better observe change in current draw throughout the clock cycle. This also explains the better separation in the newer data. As a result, Battelle suggested a second round of testing during which SMT would test parts using their system and Battelle would perform the analysis against data collected by SMT in 2018. This would address the configuration problem since SMT's system had not undergone any software, firmware, or hardware upgrades during the past several years, so it was expected to be configured the same way as the earlier tests. Battelle's system had had upgrades to both software and firmware, and possibly hardware, in the intervening period.

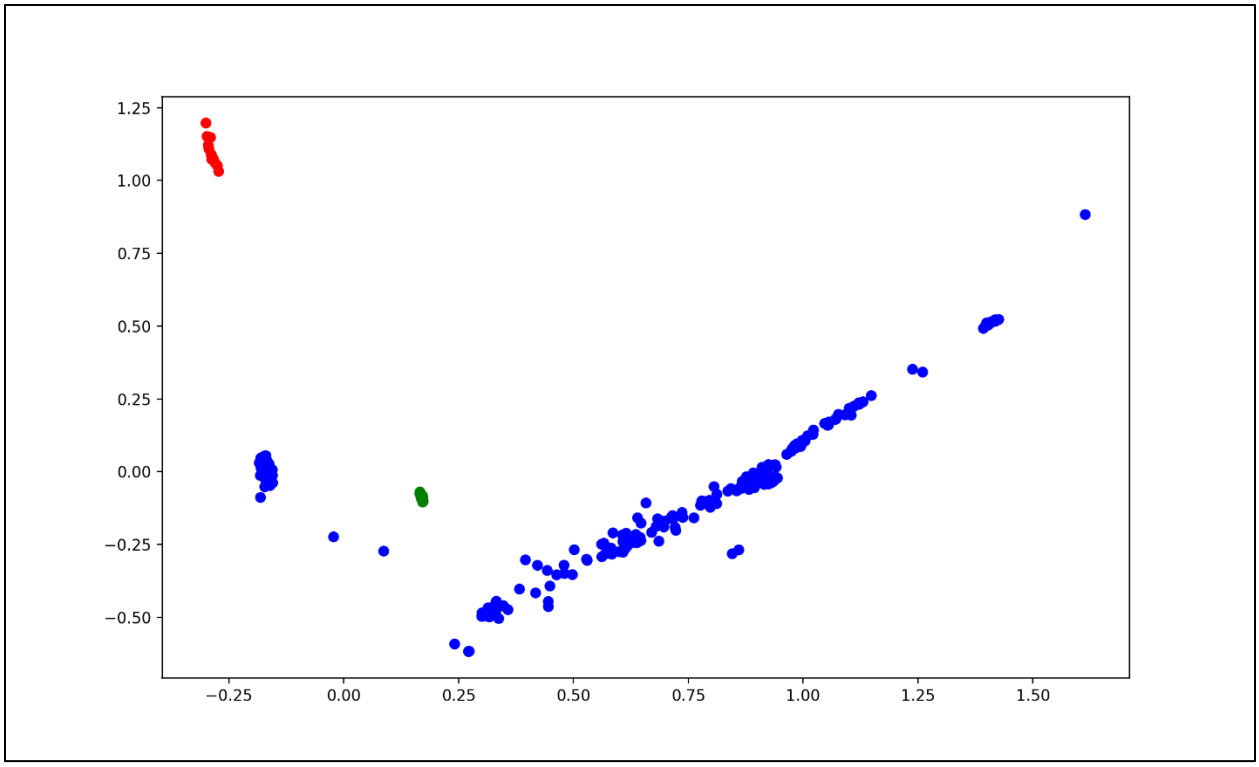


Figure 12. PCA Plot of Data Captured by Battelle (2020) in red and green and SMT (2018) in blue on Altera EPCS4SI8N parts.

Testing by SMT (first round of tests in 2020):

The new data collected by SMT on 10 authentic and 10 counterfeit parts with the same date codes as those used for the Blind Study are plotted in Figure 113. This plot actually contains 26 data points, although 6 represent an initial set of tests that were considered invalid but could not be omitted from the data.

The comparison of the new SMT data to the old SMT data is presented in Figure4. The plot shows the 2018 SMT in blue and the 2020 data in red. The cluster at about (0.15,-0.1) represents data from the authentic parts but should be ignored because it was collected during initial setup and was not considered valid. The results show that both clusters of new test points align with the large diagonal cluster, which is believed to represent the authentic parts, but far from the center of that cluster. The data from the cluster at about (1.6,0.4) are from the clones. The cluster that lies closer to the tip of the diagonal at about (1.65,0.65) is from the authentic parts. Neither of the new clusters lie close to the second, tighter cluster at about (0.20,0.00), which is believed to represent the clones.

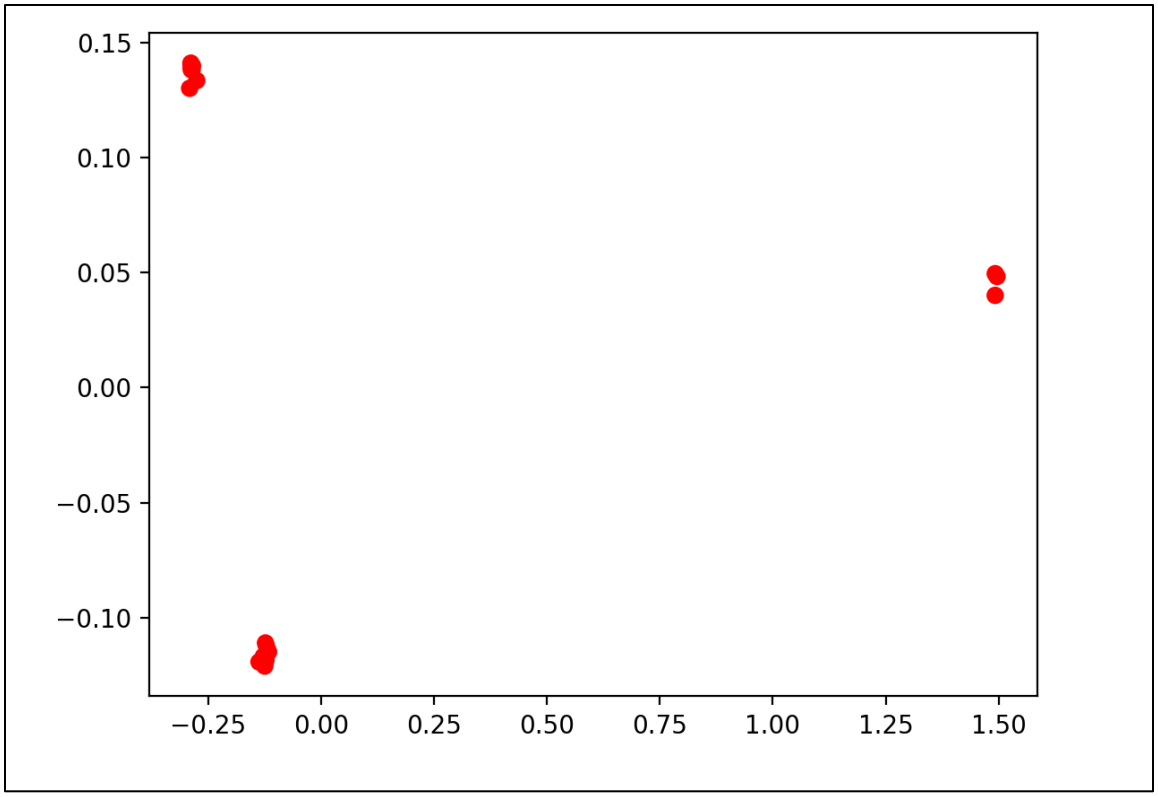


Figure 113. PCA Plot of Data Captured by SMT in 2020 on Altera EPCS4SI8N parts (both clones and authentic).

Testing by SMT (second round of tests in 2020):

One additional set of tests was performed by SMT Corp. on the same parts, to obtain a measure of repeatability and potentially provide better matching to the old SMT results. In this last set of tests, SMT performed 3 scans of each sample, producing a total of 30 scans for the clones and 30 for the authentic parts. These new data (in green) are plotted along with the recently collected SMT data (in red) in Figure 125. The results show excellent repeatability between the two sets of runs for both clusters of data. A plot of all the 2020 SMT data with the 2018 SMT data is presented in Figure 136. As seen earlier, the 2020 data fall near one extremum of the large diagonal cluster, and the second cluster from 2018 that is believed to represent the clones lies quite far away.

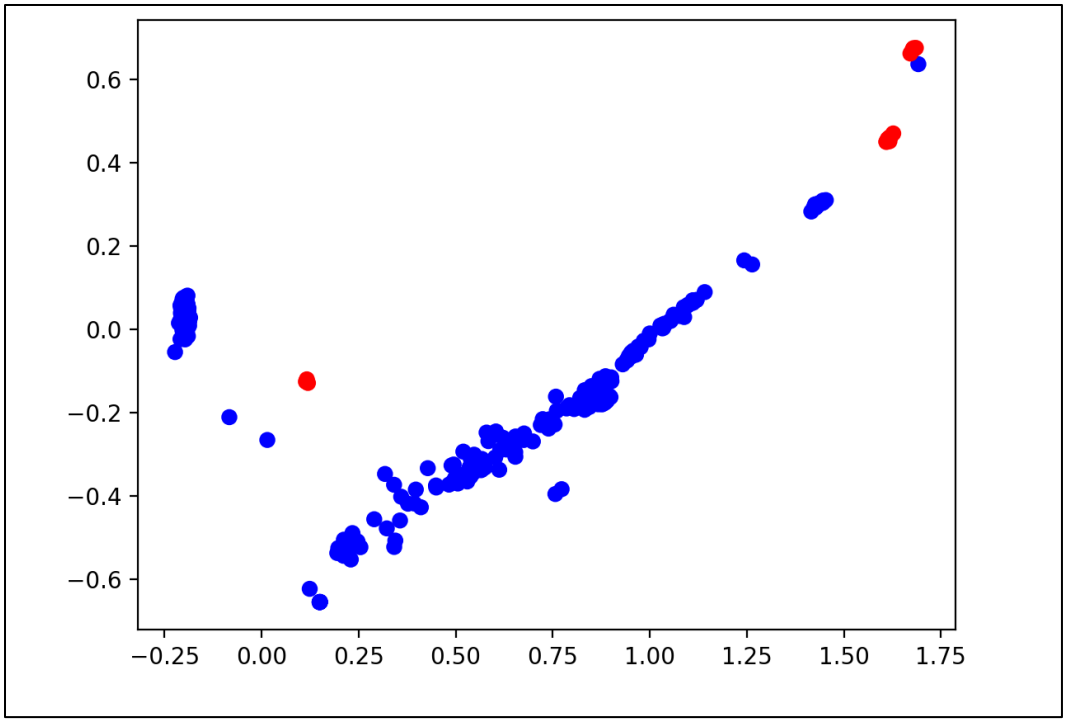


Figure 14. PCA Plot of Data Captured by SMT in 2018 (blue) and 2020 (red) on Altera EPCS4SI8N parts (both clones and authentic). The cluster at about (0.15,-0.1) should be ignored due to test errors.

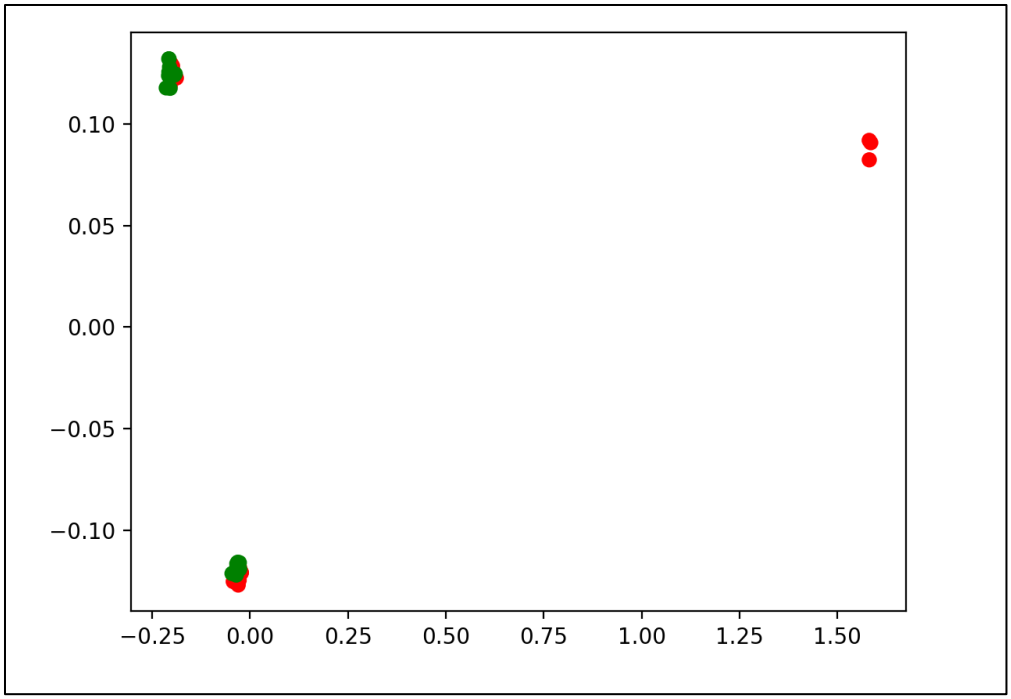


Figure 125. PCA Plot of data captured by SMT in 2020 on Altera EPCS4SI8N parts (both clones and authentic). Initially captured data is in red and second set of data captured is in green. The cluster at about (1.6,0.1) should be ignored due to test errors.

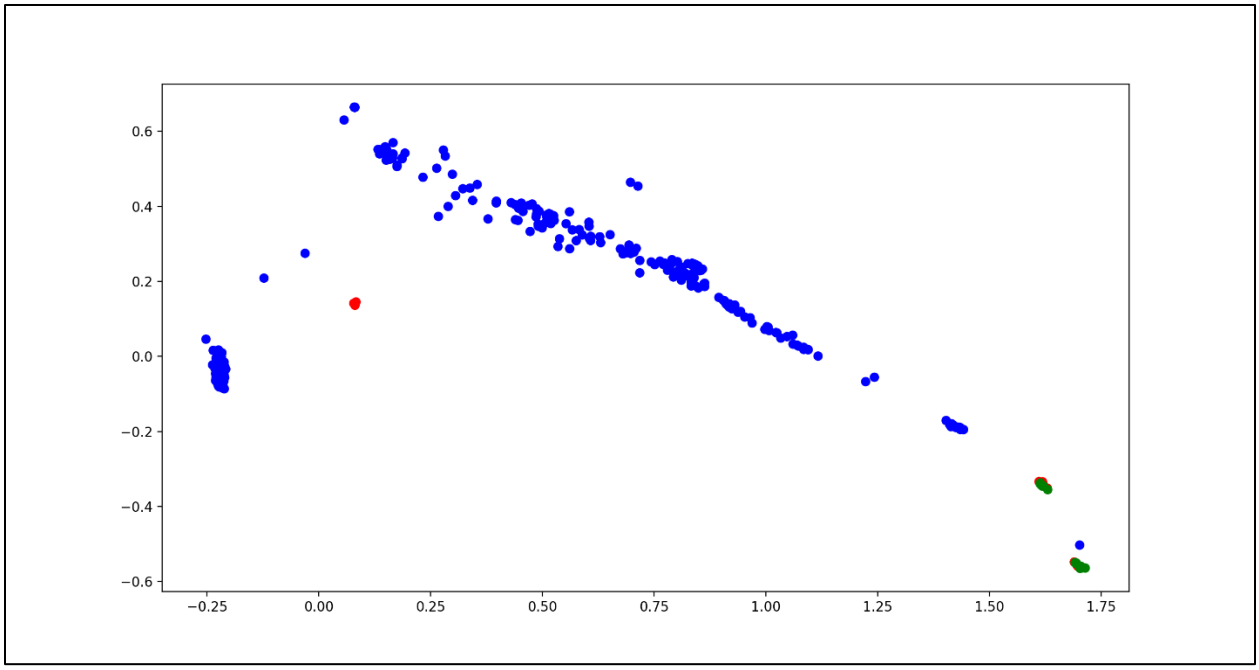


Figure 136. PCA Plot of Data Captured by SMT in 2018 (blue) and 2020 (red and green) on Altera EPCS4SI8N parts (both clones and authentic). The cluster at about (0.1,0.1) should be ignored due to test errors.

a. Summary

This exercise was designed to demonstrate how a database of virtual known good parts that had been collected at an earlier time on one test system could be used to authenticate an unknown set of parts obtained at a later date and tested on a different test system. The absence of good agreement between any of the cluster of new data collected by Battelle with the clusters of old data collected by SMT suggest that changes in test configuration are most likely responsible for the lack of agreement. If only one of the new clusters had shown agreement with the old data, one could infer that either the clones or authentic parts in the Blind Study were different from those tested earlier. The absence of agreement between both the clones and authentic parts indicated to Battelle, with concurrence from CALCE, that differences in hardware, software, and/or firmware between the current Battelle system and the old SMT system are likely to have contributed to the lack of agreement.

However, reasons for the lack of agreement between data collected during the follow-up testing performed by SMT in 2020 and the old SMT data from 2018 are not as clear-cut. It is possible that there have been some changes to the SMT system, but that could not be determined during the study.

This study demonstrates that configuration control is essential for the success of an authentication application for Side Channel technologies, and by extension all Image Analysis or other test technologies,

which rely upon comparison with data obtained at a different time and place. Systems used to produce new data for comparison to a database of known good parts (i.e., registration data or data on reference parts) must either be configured in the same way as the original systems that collected the data, or there must be provisions made for calibration, to align the results of the two data collection instances. These provisions for backward compatibility must extend over multiple deployed systems, and potentially over decades in time, if authentication using these methods is going to successfully prevent the use of counterfeit parts in long life cycle systems.

2. FeaturePrint

Tracking and tracing the provenance of parts through their life cycle remains a goal for all supply chain management professionals. The capability to register and enroll a part and follow it through the supply chain can potentially deliver supply chain intelligence and ensure product authenticity. A successful implementation of this type of technology can make it possible to obtain the history of manufacture, transactions, and in-service use of any component or raw material within an assembly. When such a goal is attained, it may attract a virtually unlimited number of participants. When such a supply chain is created, managed, and maintained, counterfeit part avoidance can be achieved. In this section of the report, the FeaturePrint technology from Alitheon is discussed, including its potential applications, and Alitheon's participation in the blind study associated with this project. Some of the technological and business model claims made by the company in trade literature are examined. Finally, findings are presented regarding what will be necessary to create a supply chain infrastructure that includes FeaturePrint as an element.

The FeaturePrint tool, as currently developed and promoted, focuses on identifying individual objects. The basic two steps are to register an object and recognize that object later. The object's unique physical attributes are extracted from a digital image to create the object's FeaturePrint, and that registration FP is stored. For identification purposes, one needs to create a digital image of the target object, transform the image into a FeaturePrint, and then compare the registration FP to this target FP. The first step is similar to enrolling a component ID. The imaging for identification can take place farther down the manufacturing path or during failure analysis. The system will authenticate the device, confirming whether or not it has seen that unit before. The company advises that the registration be performed before the last transaction point, where provenance can be verified.

Ideally, this digital fingerprint can remain valid over the service life of a product. For some applications, this service life might only the time needed to move a part across an assembly hall. For other cases, it could be decades for long-term storage, warranty service, or recycling. The company claims that nested authentication with FeaturePrinting throughout the manufacturing process, linked in a blockchain, at each

pivotal point is possible to implement. For many applications, this kind of blockchain-enabled solution has advantages.

Figure 17: Nested Authentication Framework for Electronic Components Visualized by Alitheon

From the results submitted by Alitheon in the Blind Study and previously published reports, its success rate is good. It has successfully identified 119 of the 120 parts that were used in the blind study during the authentication step. Alitheon claims to have built-in tolerances for issues like wear and corrosion. Alitheon demonstrated this concept with Moog[20]. Twenty mechanical parts were produced at Moog via additive manufacturing. All 20 parts were sent to Alitheon, which created a FeaturePrint for each. Upon return to Moog, it inspected and confirmed the identity of each item. Moog selected 9 parts of the 20 and subjected them to various types of wear to simulate various conditions and sent all the parts back to Alitheon, which could successfully match each part.

However, success in the mathematical and algorithmic capabilities does not make the FeaturePrint system ready to use the system for counterfeit avoidance and detection. The first set of issues come from the nature of the technology which identifies and registers units as individuals. The second set of issues comes from the need for industry-wide implementation for exploiting the full potential of the system. The rest of this section highlights the concerns and selection of hurdles that need to be overcome.

In the counterfeit detection arena, the demand is for acceptance or rejection of a part batch, or lot, as purchased. If parts are not registered upstream at the manufacturer or distributor, this method does not

[20] Paul Guerrier & Tim Abbott, Moog Inc. "VeriPart™ – Linking Digital to Physical" https://www.moog.com/news/blog-new/Innovation/VeriPart-linking-digital-to-physical.html

offer a way for the purchaser to determine if the parts are counterfeit. That can only be achieved if there is a bulk way to determine if a batch of parts are "similar" to the parts that were known to be authentic. If that functionality is to be achieved, the performance will be determined by the availability and quality of reference baselines. The most straightforward way to produce the necessary baselines is by collecting them directly from samples from the manufacturers. When such samples are available, the signals can be obtained directly from the images and stored for later use. In many cases, such samples are not available, and tools need to be developed for creating baselines without such samples. Alitheon claims that the tool has the capability of creating classes of parts by package type, part numbers, manufacturers, and combinations of them. However, there is no timeline for the introduction of this functionality. This can be one area for further development to make the tool useful for counterfeit avoidance.

Alitheon claims that it can register devices at relatively high speeds because that speed is limited only by the imaging system and communication of data. The creation of FeaturePrint can happen asynchronously. Authentication takes longer because an image must be captured and then verified against the database of FeaturePrint before the device can be accepted. While it may be possible to register tens of images per second, it is not evident whether authentication could happen that quickly. In a high-speed manufacturing environment, the acquisition and processing of such images could slow down the line to an unacceptable extent[21]. Furthermore, the efficiency of database access and search will need to be improved with scaling of implementation to many millions of parts. If each FeaturePrint is 100 kB in size, then a database containing 10 million unique FeaturePrints will be a terabyte in size. For the technology to be effective, the database must be comprehensive. Therefore, there will be a need to develop methods for selecting relevant portions of the database for any particular part type, data/lot code, or OCM, and for efficient search routines.

The Alitheon analysis tools are not tied to any specific data collection system. The type of data needed for the analysis are specialized for the first group of companies requiring the need for such tools but that requirement put them in a disadvantage since most of the tools are still in laboratory or prototype stages of development and they are not yet ready for a large volume production. Separation of the collection and analysis tools provides the opportunity to the users to continue to use their own tools such as imaging system for Alitheon (parameter analyzers, or x-ray equipment for other companies). The user does not need to invest in separate hardware for the purpose of part registration or counterfeit detection in these cases.

[21] Bryon Moyer, "Uniquely Identifying PCBs, Subassemblies, and Packaging: New approaches to preventing counterfeiting across the supply chain," November 18th, 2020. https://semiengineering.com/uniquely-identifying-pcbs-subassemblies-and-packaging/

However, that means that the Alitheon will require to invest time for integration of their software and algorithm with the hardware of the users and the delivery of the software cannot be made out of the box. It will be necessary that Alitheon develops and shares methods for consistent capture of the images. There may be opportunity to work with imaging hardware companies to integrate with the software.

Many industrial manufacturers already capture images used for metrology, product confirmation, and packaging. It is possible to leverage those common types of optics to convert any product into a digital format. Hence, FeaturePrint can be created as part of an acceptance, manufacturing, or laboratory test to enroll a part to the system. While the inspection system will be collecting data for quality assurance purposes, the image captured will be used for FeaturePrint generation. Ideally, the part manufacturer would integrate the enrollment process with its inspection system for the final product for large component volumes. The system can store FeaturePrint results for subsequent decision making. There can be logistics issues to identify and overcome with this registration process since the final packaging assembly is often performed at companies that are outside the direct control of the semiconductor companies.

Typically, a company that registers the parts will have access to the data at a later stage. The company that registers the parts will also need to inform the forward supply chain of its products so that they are aware of the registration unless there is a security need to keep the information compartmentalized. For the supply chain level implementation, the tools need to have forward and backward compatibility. Since the data analysis and visualization can vary from software version to version, and the machine learning tools may evolve between implementations, raw data should also be saved as backup.

The participants should be able to choose levels of data sharing and collaboration with other customers of the systems, but it cannot be mandated. There needs to be a high level of cybersecurity since lost, stolen, compromised data will lead to loss of trust in the system. Compromised data can lead to incorrect detection of counterfeit parts for the affected parts. Compromise of data can be an injection of spurious data, swapping of data, or mislabeling. The compromises can be caused by mistakes made by the companies or by malicious external actions. Demonstrated methods to detect, eliminate, and restore original data are essential.

The time difference between the recording of parts into a system and the need for possible counterfeit detection of the same parts can long. There will be changes in the business models, companies, ownership of data, and other unforeseen issues. There can be access issues due to hardware or software obsolescence. There are chances of the companies providing the services going out of business, leaving the customers in a lurch. DoD needs to consider the possibility of having to take over an operation including database management. If the tool's acceptance depends on the mandates from the government or large customers, the implementation becomes dependent on the policy priorities over time. Alitheon claims that

the user owns the data, and in case there is a need to cease the service (for a customer or globally), it can hand off the FeaturePrint the software to the user for continued use.

There should be an incentive structure to encourage companies to register/enroll all parts that they purchase even if they are not considered counterfeit risks today. The companies who take part in these steps may never need the counterfeit detection services for the parts, but their participation will help the other companies who need such services. Such registration/enrollment needs to be repeated when there are changes in the parts made by the manufacturers.

Without participation by the original component manufacturers, no supply chain level solution will be complete for counterfeit avoidance. At the same time, the original component manufacturers have no incentive to participate in such a process if the purpose of the setup is only to avoid counterfeit parts. The manufacturers need to be informed of some of the benefits that come with avoiding counterfeiting. The technology needs to offer other benefits to the component manufacturers beyond counterfeiting: track and trace, avoiding unauthorized use, export control, linking with lower-level supply chain and other such uses. If such applications entice the OCMs to adopt the tool, then there is an opportunity to take advantage of the adoption for counterfeit avoidance and authentication. Alitheon claims that is has business plans to entice component manufacturers to enroll parts. One idea floated by Alitheon is to register parts for free and for the users to authenticate the parts through Alitheon for a fee later.

Alignment with emerging IPC traceability standards can give part, assembly, and system manufacturers additional incentive to participate in the registration processes. It will help them be compliant with the standard that is taking hold in some sectors, particularly automotive.

Automotive is one of the industries that require traceability. However, subsystem components such as the production methods are decades old and do not contain a digital layer[22]. FeaturePrint can offer traceability that comes into play in systems such as defense projects or embedded electronics. In those cases, sourcing components can involve mandatory paperwork to establish provenance.

Alitheon also claims that it can image circuit boards and, when authenticating, determine if any of the components on the board are altered or replaced. It can identify areas on the board and use images of critical components to create FP and authenticate them as needed. Ideally, this could eliminate the need for incoming authentication for those components saving steps and time.

---

[22] Paul Seredynski, "Alitheon's vision is easy digital traceability," https://www.sae.org/news/2020/06/alitheon-vision-is-easy-digital-traceability, 2020-06-24

The technology developers need to look beyond defense and security-related applications and make the technology suitable for commercial companies. One should consider the DNA tagging company's direction, Applied DNA Sciences, in this topic. While the DNA tagging technology did not become an important tool in the defense microelectronic market, it has found a broader application in the larger consumer and industrial good market. Such a broader market base can keep a company solvent and the technology available.

B. Task 3b: Development of Long-term Solutions

This project has identified the limitations of the systems that were evaluated through the Blind Study and other communications. In this section, longer term technology development concepts have been recommended for investigation and investment to improve the security of the DoD supply chain.

1. Development of classification process for registration based systems:

Development of the capability of classifying of parts by package type, part numbers, manufacturers, and combinations of these characteristics is an area for further development to make machine vision tools useful for counterfeit avoidance, rather than just authentication.

2. Defect detection using Image Analysis systems:

Lack of defect identification/ inability to satisfy requirements of industry standards for visual inspection is a limitation of the Image Analysis-based methods. Image Analysis could potentially be used to replace an element of standards-based testing, namely general external visual inspection (EVI) (see also Section VIII-B-1-b-ii). This use of Image Analysis would require further development of these systems to recognize defects that are indicators of suspect counterfeit devices. Automated optical inspection systems are already in use in many industries, including microelectronic, that have similar capabilities. This technology should be developed to recognize physical defects that are indicators of suspect counterfeit devices, and to comply with requirements for General, and possibly Detailed, External Visual Inspection (e.g., AS6171/2A, AS6081).

3. Processes of throughput improvement for machine vision:

Machine vision systems should be implemented in the manufacturing and assembly process where imaging already takes place. Development is needed to improve the efficiency of the registration and authentication steps to keep up with the speed of the manufacturing process. If each digital signature file is 100 kB in size, then a database containing 10 million unique signatures will be a terabyte in size. For the technology to be effective, the database must be comprehensive. Therefore, to maintain high throughput,

there will be a need to develop methods for selecting relevant portions of the database for any particular part type, data/lot code, or OCM, and for efficient search routines.

4. Adaptation of machine vision technologies from other domains:

Image Analysis can be used to replace an element of standards-based testing, namely general external visual inspection (EVI), and possibly with greater product development, even detailed EVI. This use of Image Analysis would require further development of these systems to recognize defects that are indicators of suspect counterfeit devices. Automated optical inspection systems with comparable imaging and defect detection capabilities are already in widespread use in many industries, including microelectronic manufacturing. Product development along these lines for counterfeit detection could provide this capability if the companies and/or DoD choose to support these efforts. Some of the companies who may have relevant technology of this type include Cybord, Sciotex, and Oxford Instruments.

5. Identification of new technologies from other fields for securing the supply chain:

Opportunities for identifying and adapting leading-edge technologies from other fields for anti-counterfeiting purposes can be aided by intelligence gathering using patent and literature studies, both domestic and international. Immediate technologies of interest include Image Analysis and Side Channel. Other fields of interest could include imaging, robotics, artificial intelligence, computer science, informatics, materials science, etc.

6. Hardware assurance study with a focus on FPGAs and tampered parts:

A dedicated study should be conducted to evaluate hardware assurance methods for FPGAs, which are a special class of microelectronic part that is of particular relevance for DoD weapons systems and security-sensitive applications. Tampered parts, having simulated Trojans, and items with altered firmware, could be included in such a study, in which Side Channel methods could be compared to other electrical and physical analysis techniques.

7. Reduction of false positives through the determination of appropriate exemplars:

Most of the methods evaluated rely upon an authentic part for comparison. Exact matches, in terms of date/lot code, manufacturing site, and other part characteristics, to test parts are virtually impossible to obtain, especially after parts have become obsolete. Side Channel methods have been shown to exhibit sensitivity to date/lot codes, and can produce different results for parts exhibiting differences in die or die attach, wirebond material and configuration, and other packaging factors. Image Analysis methods are sensitive to surface characteristics, that can be influenced by changes in molding compound, marking technology, packaging location and mold. The success of conventional methods depends on knowledge of

materials of construction, part layout and dimensions, and other physical and electrical characteristics. All of these methods have the potential to produce false positives if the wrong exemplar is used for comparison. For each method, a clear definition is needed of the characteristics of an appropriate exemplar that will minimize the occurrence of false positives. A study of the sensitivity of each method to variations in exemplars may have the added benefit of revealing strategies for optimizing the data analysis algorithms to produce improved accuracy overall.

8. Thermal-Based Counterfeit Detection Methods:

Traditionally, the detection of counterfeit parts is done through conventional lab testing, including the use of X-ray imaging and visual inspection. However, these conventional methods often suffer from being expensive, time consuming, destructive, or requiring skilled operators. A promising method for nondestructive testing of counterfeit electronics is infrared thermography (IRT). Thermography is one class of thermal based methods which involves analysis of the thermal characteristics of a component. Some other thermal based include thermoreflectance and characterization of the thermal structure function based on the thermal impedance of the various layers and interfaces that make up the package. Thermography has been used extensively to detect defects in composites and electronics in the past few decades, including detection of missing solder bumps in flip chips. The application of thermography to the detection of counterfeits however has been fairly limited in scope. Studies utilizing thermal imaging, including thermography techniques, have shown reasonable accuracy at detecting counterfeits at the board level. Testing on individual components has been limited. Pulse thermography has been used to detect counterfeit dual-in-line (DIP) package components both individually and in batches. The effectiveness of thermography on counterfeits such as clones or used parts has not been explored. Additionally, testing on a variety of package types has not been conducted, with most studies testing on simple parts or at the board level. All pertinent literature reviewed made use of machine learning algorithms, such as principal component analysis, to process and detect defects or counterfeits. Machine learning is being used increasingly in the field of counterfeit detection and is an integral part to analyzing thermograms in particular.

VII. Summary, Conclusions, and Recommendations

A. Sections IV to VI

In a relatively short time, interrupted by a global pandemic, this project produced a large and unique dataset on a diversity of counterfeit detection methods, including their applications to both advanced and conventional counterfeit parts. This study found that some of the IA and SC technologies are quite

advanced, and the organizations have highly skilled and educated scientists and engineers. **However, none of the technologies are yet ready as a deployable, standalone method for counterfeit prevention.**

For Side Channel methods, the process of data collection (e.g., fixturing, test configuration setup) remains a bottleneck that can lead to long lead times for testing and higher costs. Inadequate fixturing has also been observed in some instances to introduce noise and uncertainty into the measurements and requires engineering time and skill to stabilize and achieve suitable test conditions. This dependence on the fixtures raises questions about the consistency of measurement quality across time, numerous parts, operators, and usage environments. This is one reason why the TRL Assessments of Side Channel technologies show that none have achieved a high TRL for counterfeit detection (see Table). The companies' TRL levels show that they are still in their development phases and going through engineering improvements. The review of the parts previously evaluated by the SC companies, included in the TRL reports, shows that the technologies have not been evaluated and validated on a wide enough array of parts or in a wide enough range of operating environments to claim broad capabilities. This finding on TRLs is unfortunate because the methods are technically sophisticated and are supported by a committed and skilled group of engineers.

Table 25: TRL Summary

Company	Critical Technology Element	Focus of Assessment	TRL Complete (Partial)
Alitheon (IA)	The process of generating FeaturePrint	Software	6 – (up to 9)
Covisus (IA)	Covisus vTag scanner/DTEK system	Hardware Software	5 (up to 7) 5 (up to 7)
Creative Electron (IA)	The FingerPrint development software	Software	4
Battelle (SC)	Barricade hardware system used to test device and collect data as well as the software algorithm which performs classification	Hardware Software	4 – (up to 8) 5 – (up to 8)
Nokomis (SC)	ADEC Hardware for electromagnetic signal capture	Hardware	4 – (up to 6)
Sandia (SC)	The process of generating and gathering the raw power spectrum (amplitude-versus-frequency plot)	Hardware	4 – (up to 5)
PFP (SC)	PFP analytics software	Software	4 – (up to 7)

The Side Channel technologies cannot be viable by serving *only* defense microelectronics needs. The developers need to find applications to cover broader aspects of electronics beyond components and serve the commercial electronics industry. Unlike a Image Analysis system that can cater to the needs of the non-electronics market, the Side Channel methods are limited to use in electronic systems that can be powered up to collect signals. If mature and widely available at a reasonable cost, Side Channel methods

could have benefits beyond counterfeit detection to areas such as microelectronics quality control, inventory management, process control, and reliability improvement.

The Image Analysis technologies that were evaluated have the advantage that they can perform individual part authentication and matching without contact and without any modification of the part. They may also satisfy, at least in part, the IUID requirement in DODI 5200.44, if they were fully implemented. The business case may not exist for authentication at the original component manufacturers or authorized distributors, and without cooperation from those sectors, it is hard to achieve a critical volume of business. In the absence of that, business survival and continued maintenance of the database and application area remain precarious. These companies need to expand their market beyond DoD and even electronics in order to grow and support their infrastructure. Some IA companies are already targeting these other markets, and the DoD should encourage and facilitate such expansions.

On the other hand, the IUID technologies are not designed for classification or for counterfeit detection. The ability for authentication by itself does not make these companies ready to provide a counterfeit detection solution. There is a need to develop the capability of classifying parts by package type, part numbers, manufacturers, and combinations of these characteristics. This report identifies the further development steps that are needed to make them suitable for counterfeit detection.

For both Side Channel and Image Analysis systems, the time lag between the recording of parts into a system and the need for possible counterfeit detection of the same parts can be many years. There will be changes in the business models, companies, data ownership, and other unforeseen issues. There can be access issues to information due to hardware or software obsolescence. There are chances of the companies providing the services going out of business, leaving the customers, including DoD, unable to access data or services. Therefore, in addition to descriptions of the technology, the TRL assessment reports in Sections IV-A and V-A include summaries of business information and patent portfolios. This information can help DoD perform further evaluation of these organizations and technologies regarding their business situations.

If and when they achieve success, these technology companies will acquire and need to manage vast amounts of sensitive data from all their customers. The companies that developed that technology will need to become database management/information systems specialists. They will be responsible for managing such sensitive data with both national security and business implications for their customers. Lost, stolen, or compromised data will lead to a loss of trust in the system. Compromised data can lead to incorrect detection of counterfeit parts for the affected parts. Threats to data integrity include the injection of spurious data, swapping of data, or mislabeling. The compromises can be caused by mistakes made by the companies or by malicious external actions. Demonstrated methods to detect and eliminate intrusions

and the ability to restore original data are essential. DoD needs to evaluate the cybersecurity capabilities of these companies before making any final choice of technology. DoD may also need to help the companies achieve the required levels of cybersecurity before their deployment.

Both types of tools also remain vulnerable to issues of technology upgrades and obsolescence including that of compatibility. It is even more critical since these technologies are not yet mature as seen the TRA. The data and images being collected now may not be accessible for comparison purposes with data collected with newer and updated tools. Both known-good virtual golden samples study with the Battelle Barricade system and the assessment of Alitheon's FeaturePrint system confirmed that risk.

In the final analysis, machine vision is attractive in many respects but not quite ready for deployment. It will require some development before it can be successfully used. In order to address concerns about the business case for adoption, there is an opportunity to motivate adoption through the development of IA to satisfy industry standards on inspection. This would get technology and tools widely deployed in a broader marketplace, creating incentives to employ them for authentication and tracking as well. Unlike IA, CALCE does not have a specific recommendation for an application that would motivate widespread adoption of SC tools. It is conceivable that they can find use in areas where quality control, process control, and inventory management. SC methods can potentially achieve those functions faster and in a less expensive manner.

Based on the overall experience of performing the Blind Study, combined with other opportunities for evaluation and communication with the various organizations, CALCE found Battelle to be the most ready among the aide-channel companies, and Alitheon to be the most advanced among the Image Analysis companies, concerning applications of their technology to counterfeit prevention and detection in the defense supply chain.

Conventional testing was included in the Blind Study because it complies with industry standards and is in widespread use for counterfeit detection. The result of the Blind Study revealed that this method remains consistently accurate in the detection of variations among parts in a lot and in the determination of which parts were counterfeit even in the absence of an exemplar, based on detection of counterfeit-related defects.

1. The Blind Study findings support the recommendation that DoD should continue to rely upon standards-based testing for counterfeit detection.
2. DoD should also take a more active role in standards organizations that are developing anti-counterfeit standards, for both awareness within DoD as well as for influencing the development of standards in a way that addresses DoD's needs.

As indicated by Tables 26 and 27 at the end of this section, Image Analysis and related Side Channel methods varied in accuracy but each included technologies that performed to 99% accuracy or above in their ability to discriminate between counterfeit and authentic, or to match previously registered parts specifically. The potential exists with both types of technology for both false positives and false negatives in the analysis of clones, although all three of the SC methods evaluated produced low rates of false positives. On the other hand, one IA method (Covisus) produced false negatives but none of the SC or IA methods produced false positives with conventional counterfeits.

DoD should undertake the following short-term investments and development efforts regarding Image Analysis and related Side Channel technologies for more effective anti-counterfeit applications. Additional descriptions of these recommended studies are provided in Section V-C. Please refer to **Section**

B. Section V. Task 2: Evaluation of Existing Machine-Vision and AI Technologies for specific details.

1. Correlation of Image Analysis and Side Channel results with physical defects
2. Development of assembly-level (PCB-level) applications of Machine Vision
3. Iteration of the Blind Study with separate homogeneous lots, or mixed lots of varying heterogeneity, and larger sample size
4. Analysis of Battelle Barricade data reference samples
5. Authentication study with more aggressive physical damage to part surfaces following registration
6. Follow-up TRL Assessments by the same team after achievement of new development milestones
7. Analysis of defects from conventional testing Blind Study to determine the consistency and effectiveness of each test method for different part types
8. Exploration of thermal methods for counterfeit detection

Several longer-term technology development concepts are also recommended for investigation and investment to improve the security of the DoD supply chain. Additional descriptions of these studies are provided in Section VI-B.

1. Development of classification process for registration based systems
2. Development of defect detection capabilities using machine vision systems to make them compatible with standards-based testing, improve interpretability, and reduce false positives
3. Improvement of throughput for Machine Vision technologies
4. Adaptation of Machine Vision technologies from other domains
5. Identification of new technologies from other fields for securing the supply chain

6. Application of the methods used in this study to a hardware assurance study with a focus on FPGAs and tampered parts
7. Application of the methods used in this study to evaluate techniques for counterfeit materiel detection and prevention, including batteries
8. Reduction of false positives through the determination of requirements for appropriate exemplars
9. Investigation of thermal signature-based counterfeit detection methods

The findings of the study on anti-counterfeit measures and policies in which the Carey School of Law at UMB played a central role, indicated that DoD components are largely siloed and do not implement a consistent set of policies and practices. Furthermore, awareness of counterfeit prevention policies and standards throughout DoD needs improvement. We recommend that a training program on anti-counterfeit measures and supply chain security be required for all program managers, contract officers, purchasing, maintenance, and sustainment personnel.

The trends in counterfeit products entering both civilian and military supply chains show that the scope of risk is expanding beyond electronic components. Materiel, including complete assemblies and batteries, are frequently reported as counterfeit. One factor in selecting a potential counterfeit detection method should be the possibility of adapting the method to the avoidance of these emerging threats.

This study would not have been possible without the active participation of SMT Corporation. SMT Corporation provided known advanced counterfeit components and clones for use in the study, along with corresponding authentic parts, and it provided detailed test reports on both types of parts that confirm their identity as either counterfeit or authentic. Their reports served as the reference for evaluating the counterfeit detection methods investigated in the blind study. SMT handled shipping and tracking of parts to all partner organizations. They also performed testing on their own Battelle Barricade system for the Known Good Virtual Golden Samples Demonstration. The whole organization, and in particular, Mr. Tom Sharpe was a supportive, knowledgeable, and helpful partner, and Mr. Jason Romano provided all the logistical support needed to conduct this blind study.

Table 26: Detailed Summary of Results Including Both Detection and Clustering Accuracy for Clones and Conventional Counterfeits Separately

Company	System Name	Testing Type	Clone					Conventional Counterfeit				
			Counterfeit Detection Accuracy	Clustering Accuracy	FP	FN	Part Numbers Tested	Counterfeit Detection Accuracy	Clustering Accuracy	FP	FN	Part Numbers Tested
SMT Corp		CT	-	-	-	-	-	-	-	-	-	-
CALCE		CT	1.00	1.00	0.00	0.00	3	1.00	1.00	0.00	0.00	2
Micross		CT	N/A	1.00	0.00	0.00	1	*RNP*	*RNP*	*RNP*	*RNP*	0
Integra		CT	0.50	1.00	0.00	0.00	3	0.50	1.00	0.00	0.00	2
Battelle	Barricade	SC	0.94	0.94	0.00	0.12	8	-	-	-	-	0
Sandia	PSA	SC	N/A	1.00	0.00	0.00	5	N/A	1.00	0.00	0.00	1
Nokomis	ADEC	SC	*RNP*	*RNP*	*RNP*	*RNP*	0	*RNP*	*RNP*	*RNP*	*RNP*	0
PFP Cybersecurity	Power Fingerprinting	SC	N/A	0.99	0.03	0.00	4	-	-	-	-	0
Covisus	vTag/DTEK	IA	N/A	0.90 | 0.83	0.00 | 0.15	0.20 | 0.20	4	N/A	0.80 | 0.75	0.00 | 0.00	0.40 | 0.50	2
Creative Electron	Fingerprint	IA	N/A	0.83	0.22	0.12	6	-	-	-	-	0
Alitheon	FeaturePrint	IA	N/A	0.99	0.02	0.00	6	-	-	-	-	0

KEY:

CT: Conventional Testing
SC: Side Channel
IA: Image Analysis

FP normalized = FP/(FP+TN) = incorrectly classified negatives/all negatives
FN normalized = FN/(TP+FN) = incorrectly classified positives/all positives
CT clustering: Identifying differences between the two sample sets; RNP: Results not provided; Accuracies are provided as fractions

Company	Comments
SMT Corp	Source of known authentic, and known counterfeit components, advanced (clones), and basic. See Appendix 3 for Component Inspection Reports.
CALCE	No exemplars were used for counterfeit detection.
Micross	Micross only submitted results for 1 of 5 part numbers. No exemplars were used for counterfeit detection.
Integra	Identified differences in EPCS4SI8N but did not attempt to determine which parts were counterfeit. Identified 2 counterfeits correctly and 2 incorrectly. No exemplars were used for counterfeit detection.
Battelle	Identified suspect parts for 7 of the 8 parts tested. Was not able to separate LM324N parts. Battelle purchased exemplars for each part number.
Sandia	Performed grouping by comparing to selected reference parts.
Nokomis	No results were submitted by Nokomis.
PFP Cybersecurity	Overall final grouping; there are two additional values for comparison to an individual part not included in this table.
Covisus	Results are reported as Echo | Kilo. Participated in the phase 1 registration process only.
Creative Electron	Matched phase 1 registered serial numbers to phase 2 serial numbers.
Alitheon	Matched phase 1 registered serial numbers to phase 2 serial numbers.

Table 27: Detailed Summary of Results Including Both Detection and Clustering Accuracy for Clones and Conventional Counterfeits Combined

Company	System Name	Testing Type	Counterfeit Detection Accuracy	Clustering Accuracy	FP	FN	Part Numbers Tested	Comments
SMT Corp.		-	-	-	-	-	-	Source of test samples.
CALCE		CT	1.00	1.00	0.00	0.00	5	No exemplars were used for counterfeit detection.
Micross		CT	N/A	1.00	0.00	0.00	1	Micross only submitted results for 1 of 5 part numbers. No exemplars were used for counterfeit detection.
Integra		CT	0.50	1.00	0.00	0.00	5	Identified differences in EPCS4SI8N but did not attempt to determine which parts were counterfeit. Identified 2 counterfeits correctly and 2 incorrectly. No exemplars were used for counterfeit detection.
Battelle	Barricade	SC	0.94	0.94	0.00	0.12	8	Identified suspect parts for 7 of the 8 parts tested. Was not able to separate LM324N parts. Battelle purchased exemplars for each part number.
Sandia	PSA	SC	N/A	1.00	0.00	0.00	6	Performed grouping by comparing to selected reference parts.
Nokomis	ADEC	SC	*RNP*	*RNP*	*RNP*	*RNP*	*RNP*	No results were submitted by Nokomis.
PFP Cybersecurity	Power Fingerprinting	SC	N/A	0.99	0.03	0.00	4	Overall final grouping; there are two additional values for comparison to an individual part not included in this table.
Covisus	vTag/DTEK	IA	N/A	0.87 | 0.80	0.00 | 0.10	0.27 | 0.30	6	Results are reported as Echo | Kilo. Participated in the phase 1 registration process only.
Creative Electron	Fingerprint	IA	N/A	0.83	0.22	0.12	6	Matched phase 1 registered serial numbers to phase 2 serial numbers.
Alitheon	FeaturePrint	IA	N/A	0.99	0.02	0.00	6	Matched phase 1 registered serial numbers to phase 2 serial numbers.

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

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.[23] Eight of those individuals have agreed to contribute a written interview summary in support of this report.[24] 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.[25] 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

[23] 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.

[24] 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.).

[25] SAE International, AS6171A, *Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts* (2018).

from the manufacturer); overproduced parts (a part from a contracted facility which was fabricated 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.[26]

Table 28: List of counterfeit Electrical,

Electronic, and Electromechanical (EEE) part types.[27]

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

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

[26] *Id.* at 7-9.

[27] 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.

> 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.[28]

The Department of Homeland Security's Appendix to the U.S. Intellectual Property Enforcement Coordinators 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 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.[29]

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."[30]

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.[31] 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

---

[28] 84 Fed. Reg. 64680, at 64681 (November 22, 2019).

[29] United States Intellectual Property Enforcement Coordinator, *Annual Intellectual Property Report to Congress*, Appendix at 51 (February 2019).

[30] *Id*., Appendix at 51.

[31] Kirsten M. Koepsel, COUNTERFEIT PARTS AND THEIR IMPACT ON THE SUPPLY CHAIN (2d ed. 2019), at 28-29.

purchases were not made,[32] the DoD and defense contractors may be forced to purchase replacement parts from outside the authorized supply chain, including from brokers and independent distributors.[33] 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.[34] Other factors include the military's past focus on lowest cost suppliers rather than quality of parts obtained.[35]

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

[32] 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).

[33] Koepsel, *supra* note 9, at 29.

[34] Rob Spiegel, *Supply Chain* (March 3, 2011).

[35] *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.

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.[36]

This stands in stark contrast to the ultra-clean, environmentally controlled, high tech wafer fabs where manufacturing of new semiconductor devices takes place.[37] 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.[38] 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, there is no way to predict how well they will perform, how long they will last, and the full impact of failure."[39]

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.[40]

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

---

[36] 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.

[37] *Id.* at 9-11.

[38] *Id.* at 11.

[39] U. S. Senate, Committee on Armed Services, *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain* (2012), at 7.

[40] 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.

passed off as authentic product.[41] 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.[42]

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 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.[43]

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.

---

[41] Dr. Brian Cohen Interview Summary (Appendix 19), at 2.

[42] *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.

[43] *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).

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,[44] 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.

2. 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 source from the DoD recalled a problem with counterfeit fasteners in the late 1980s,[45] which ultimately led to the enactment of the Fastener Quality Act of 1990.[46] 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.[47]

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

---

[44] National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, 125 Stat. 1298 (2011) [hereinafter "FY 2012 NDAA"].

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

[46] *Id.*

[47] 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, screws, not to electronic components.

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,[48] around the time that China joined the World Trade Organization.[49] According to ERAI's online Awareness Timeline,[50] 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.[51]

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."[52] By the spring of 2003, reports of counterfeit parts were also being filed with the Government-Industry Data Exchange Program ("GIDEP").[53] Shortly thereafter, the Secretary of Defense issued a memo entitled "Encouraging Participation in the Trusted Foundry Pilot Program."[54] The memo recognized that counterfeits are not the only problem and mentioned backdoor threats as well.

3. 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

---

[48] Richard Smith Interview Summary (Appendix 19), at 1.

[49] 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.

[50] 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.

[51] *Id.*

[52] *Id.*

[53] 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 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.").

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

from customers.[55] In 2007, the Semiconductor Industry Association ("SIA") formed an Anti-Counterfeiting Task Force to combat counterfeit chips,[56] and SAE International formed its G-19 Counterfeit Electronic Components Committee to respond to the threat of counterfeit electronic parts.[57] In the spring of 2007, ERAI issued a special report entitled "A Time for Change,"[58] following two investigative trips to China by its representatives in January 2004 and December 2006.[59] 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.[60] 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."[61]

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."[62] 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

---

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

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

[57] 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.

[58] 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.

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

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

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

[62] *Id.* at 10.

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.[63]

4. 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.[64]

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 Navy's ability to sustain platforms with extended life-cycles and maintain weapons systems in combat operations."[65]

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.[66]

---

[63] *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).

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

[65] U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, *Defense Industrial Base Assessment: Counterfeit Electronics* (January 2010), at i.

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

In January 2010, the Department of Commerce Bureau of Industry and Security ("BIS") issued its *"Defense Industrial Base Assessment: Counterfeit Electronics"* report.[67] 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."[68] 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."[69]

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.[70] Nevertheless, there was a lack of dialogue about counterfeits between all organizations in the U.S. defense supply chain.[71] Most organizations assumed that other parties in the supply chain were testing parts, and therefore they conducted little testing themselves.[72] There was a lack of traceability in the supply chain, as well as insufficient accountability within organizations and limited record keeping on counterfeit incidents.[73] Further, few organizations understood legal requirements and liabilities relating to counterfeits, and few knew what legal or other authorities to contact about counterfeit parts.[74] The report determined that stricter testing protocols and quality controls were needed by contractors and suppliers, and DoD

---

[67] 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"].

[68] *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.

[69] *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.

[70] *Id.* at 7.

[71] *Id.* at 5.

[72] *Id.* at 6.

[73] *Id.* at 6.

[74] *Id.* at 6-7.

organizations needed additional procurement and testing protocols to prevent counterfeit parts from entering their supply chain.[75] 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.[76]

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."[77] 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."[78] 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."[79] 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."[80]

Most DoD organizations felt the DFARS was inadequate to address the counterfeit problem because it did not specifically discuss counterfeit electronics.[81] At that time, counterfeit parts were simply treated as nonconforming items, and the terms "counterfeit" and "nonconforming" were often used interchangeably. The FAR defined three specific types of nonconformance: critical, major, and minor.[82] 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

[75] *Id.* at 7.
[76] *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.
[77] *Id.* at 157.
[78] *Id.* at 157.
[79] *Id.* at 157.
[80] *Id.* at 157.
[81] *Id. at 157.*
[82] 48 C.F.R. § 101 (eff. June 4, 1996).

effective use or operation of the services or supplies."[83] The seriousness of the nonconformance determines DoD's response. If a nonconformance is critical or major, the contracting officer should ordinarily reject the supplies; if a nonconformance is minor, the contract administration office can determine whether to accept or reject.[84] 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
- 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.[85]

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

[83] *Id.*
[84] 48 C.F.R. § 407(c)(1), (d) (eff. June 4, 1996).
[85] *Id.* at 209-11.

does not have a department wide definition of the term "counterfeit" and a consistent means to identify instances of suspected counterfeit parts."[86]

5. 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.[87]

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.[88]

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."[89] E-waste was being disassembled by hand, washed in dirty rivers, and then dried on city sidewalks. Date codes on the parts were frequently changed to make them appear new, and other false

---

[86] 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.

[87] 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"].

[88] *Id.* at vi-vii.

[89] *Id.* at 5.

markings were also placed on the parts.[90] 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."[91] 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.[92]

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.[93] 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."[94] 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.[95] The committee's written report was published on May 21, 2012, shortly after the enactment of

---

[90] *Id.* at 6.

[91] *Id.* at 7, *citing* Senate Armed Services Committee Hearing at 17.

[92] Senate Armed Services Committee Report, at 7, *citing* Committee Staff interview with Vivek Kamath, at 11 (October 6, 2011).

[93] *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.

[94] U.S. Senate Committee on Armed Services, Press Release: *Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts*, at 2 (May 21, 2012).

[95] Senate Armed Services Committee Report, at 66.

the FY 2012 NDAA, and it contained detailed explanations of what Congress hoped to achieve through that legislation.[96]

6. 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.[97] 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.[98] 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[99] 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,"[100] and those definitions were required to include "previously used parts represented as new."[101] 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;[102] 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.[103] In addition, the Secretary was instructed to establish processes for ensuring that DoD personnel submit a report to GIDEP within 60

---

[96] *See id. at* 66-72.

[97] National Defense Authorization Act for Fiscal Year 2012, Public Law 112-81, 125 Stat. 1298 (December 31, 2011).

[98] 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).

[99] FY 2012 NDAA § 818(a).

[100] 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).

[101] FY 2012 NDAA § 818(b)(1).

[102] *Id.* at § 818(b)(2).

[103] *Id.* at § 818(b)(3).

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 counterfeit electronic parts or suspect counterfeit electronic parts.[104] 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.[105]

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.[106] Under these new regulations, covered contractors[107] 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.[108] 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.[109]

The revised regulations envisioned by Section 818 were also expected to contain provisions requiring the use of "trusted suppliers."[110] 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

---

[104] *Id.* at § 818(b)(4).
[105] *Id.* at § 818(b)(5).
[106] *Id.* at § 818(c).
[107] 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.
[108] *Id.* at § 818(c)(2)(a).
[109] *Id.* at § 818(c)(2)(b).
[110] 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.

suppliers who obtain such parts exclusively from the original manufacturers of the parts or their authorized dealers; and

(ii) obtain electronic parts that are not in production or currently available in stock from trusted suppliers.[111]

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.[112] 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.[113] 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.[114] The DoD would also have the right to review and audit the selection of additional trusted suppliers by its contractors and subcontractors.[115]

A third area to be addressed by the new DFARS regulations would impose GIDEP reporting requirements on contractors.[116] 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.[117] 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.[118]

---

[111] FY 2012 NDAA § 818(c)(3)(A).
[112] *Id.* at § 818(c)(3)(B).
[113] *Id.* at § 818(c)(3)(C).
[114] *Id.* at § 818(c)(3)(D).
[115] *Id.* at § 818(c)(3)(D)(iii).
[116] 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.
[117] FY 2012 NDAA § 818(c)(4).
[118] *Id.* at § 818(c)(5).

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 Act.[119] The new program was required to include several elements at the contractor level.[120] Section 818 stated that the program shall require covered contractors[121] 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.[122]

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.[123]

In addition, Section 818 called for creation of an inspection program by Secretary of Homeland Security,[124] 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

---

[119] *Id.* at § 818(e).

[120] 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.

[121] Note that the program requirements were only directed at contractors, not subcontractors. *See* FY 2012 NDAA § 818(e)(2)(A).

[122] *Id.* at § 818(e)(2)(A)(i)-(ix).

[123] *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).

[124] *See* FY 2012 NDAA § 818(d).

Department.[125] Finally, Congress amended 18 U.S. Code § 2320 to include provisions on trafficking in counterfeit military goods or services.[126]

7. 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.[127] 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.[128]

The ABA also expressed concerns 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 to 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.[129]

---

[125] *See id.* at § 818(g).
[126] *See id.* at § 818(h).
[127] 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.
[128] *Id.* at 14-15.
[129] *Id.* at 18.

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 costs of obtaining the supplies, and potentially render it difficult or impossible to obtain needed supplies on a timely basis.[130]

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."[131]

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."[132] 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."[133] 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."[134]

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:

---

[130] *Id.* at 19.
[131] *Id.* at 31.
[132] *Id.* at 24.
[133] *Id.* at 25.
[134] *Id.*

> 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.[135]

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?[136]

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."[137] It was noted that such costs were unallowable even when the contractor obtained the parts from the Government itself.[138]

8. 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.[139] On October 31, 2012, DLA announced that all suppliers that provide electronic microcircuits to DLA would be required to provide items marked with a

---

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

[136] 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.

[137] 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).

[138] 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.

[139] 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.

botanical DNA taggant.[140] An anonymous source indicated that the DNA marking program started as a research project with Applied DNA Sciences,[141] 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 manufacturer would have its own DNA mark, which should be applied in-house at the end of the manufacturing process.[142]

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.[143]

9. 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)

---

[140] 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.

[141] *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.

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

[143] *Id.*

the counterfeit parts were provided to the contractor as Government property; and (3) the contractor provided timely notice to the Government.[144] 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.[145]

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., 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).[146] 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)."[147]

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."[148] 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."[149]

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

---

[144] National Defense Authorization Act for Fiscal Year 2013, Public Law 112-239, § 833, 126 Stat. 1844-1845 (2013).

[145] National Defense Authorization Act for Fiscal Year 2016, Public Law 114-92, § 885, 129 Stat. 726, 948 (2015).

[146] National Defense Authorization Act for Fiscal Year 2015, Public Law 113-291, § 817(1)(A), 128 Stat. 3292, 3432 (2014).

[147] *Id.*, §817(1)(D).

[148] National Defense Authorization Act for Fiscal Year 2017, Public Law 114-328, § 815, 130 Stat. 2000, 2271-2272 (2016).

[149] *Id.*

the purchase of microelectronics products and services by the DoD.[150] 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.[151] 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-establishing microelectronics foundry services and the industrial capabilities associated with those services.[152]

B. 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.[153] The DFARS implements and supplements the provisions of the Federal Acquisition Regulation ("FAR") and is issued under the authorization of the Secretary of Defense.[154] 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.[155]

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.[156] They are not merely internal agency procedures or interpretative guidance.[157]

---

[150] National Defense Authorization Act for Fiscal Year 2020, Public Law 116-92, § 224, 133 Stat. 1266 (2019).

[151] *Id.*

[152] 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).

[153] FY 2012 NDAA § 818(c).

[154] 48 C.F.R. § 201.301(a)(1).

[155] *Id.*

[156] Davies Precision Machining, Inc. v. U.S., 35 Fed. Cl. 651, 657 (1996).

[157] *Id.*

The FAR contains specific requirements that agencies such as DoD must follow when issuing agency-specific acquisition regulations (e.g., the DFARS).[158] The views of nongovernmental parties and organizations, as well as other agencies, must be considered in formulating acquisition policies and procedures.[159] 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.[160] Public meetings may also be held when a decision is likely to benefit from significant additional views and discussions.[161] 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.[162] 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),[163] 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 that have an operational system to detect and avoid counterfeit parts and

[158] 48 C.F.R. § 1.301(b).
[159] 48 C.F.R. § 1.501-2(a).
[160] 48 C.F.R. § 1.501-2(b), (c). Normally, at least 60 days will be given for receipt of comments. *Id.*
[161] 48 C.F.R. § 1.503.
[162] 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/.
[163] FY 2012 NDAA § 818(c)(1). The FY 2012 NDAA was signed by President Obama on December 31, 2011.

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.

1. 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 833 of the FY 2013 NDAA.[164] A proposed rule was published on May 16, 2013,[165] 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.[166] The proposed rule also included a new contract clause at DFARS 252.246.7007, entitled "Contractor Counterfeit Electronic Part Avoidance and Detection System.[167]

Following publication of the proposed rule, 50 respondents submitted public comments.[168] 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.[169] 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

---

[164] 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.

[165] 78 Fed. Reg. 28780 (May 16, 2013).
[166] *Id.* at 28780-28785.
[167] *Id.* at 28785.
[168] *See* 79 Fed. Reg. 28092 (May 6, 2014).
[169] *Id. See also*, Notice of Meeting, 78 Fed. Reg. 35262 (June 12, 2013).

buys itself,"[170] and it contended that "ADEC should be a requirement for a DOD-approved operational system to detect and avoid counterfeit parts."[171] Nokomis further proposed that "ADEC is critical to functionally meeting the proposed DFARS regulations."[172] 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."[173]

On May 6, 2014, a final rule was issued which made significant changes to the proposed rule.[174] 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."[175] 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.[176]

In its comments, DoD acknowledged that some respondents preferred the definition of counterfeit electronic part from SAE AS5553A.[177] However, DoD declined to adopt that definition due to the

---

[170] 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.

[171] *Id.* at 5.

[172] *Id.* at 7.

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

[174] 79 Fed. Reg. 26092 (May 6, 2014).

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

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

[177] 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.

"continually evolving nature of the definitions in industry standards and the inconsistencies among the definitions in the standards."[178]

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."[179] 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."[180]

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.[181] 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."[182] The new provisions required use of "suppliers that meet applicable counterfeit detection and avoidance system criteria."[183]

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."[184] 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.[185] 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 part are unallowable unless –

---

[178] *Id.* at 26093.

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

[180] *Id.*

[181] *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 form Accredited Sources*, available at https://www.intrinsix.com/hubfs/Premium_Content/trusted-asic-design/The_Guidebook_on_Trust.pdf.

[182] *Id.*

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

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

[185] 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).

(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.[186]

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.[187] 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.[188]

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")[189] and the corresponding contract clauses in Section 252.244-7007 (sometimes referred to herein as "Contract Clause 7007").[190] 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."[191] 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.[192] As requested by many respondents, the new regulations did not merely repeat the system criteria from Section 818 without elaboration, but

[186] 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.
[187] *Compare* 78 Fed. Reg. at 28783.
[188] 79 Fed. Reg. at 26101.
[189] *Id*. at 26106-26107 (codified at 48 C.F.R. § 246.870, eff. May 6, 2014).
[190] *Id*. at 26108 (codified at 48 C.F.R. § 252.244-7007, eff. May 6, 2014).
[191] 48 C.F.R. § 246.870-2(a) (eff. May 6, 2014).
[192] 48 C.F.R. § 252.246-7007(c) (eff. May 6, 2014).

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.[193] 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.[194]

2. 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.[195] DoD described the rule as taking a "risk-based approach to counterfeit management."[196] 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."[197]

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.[198] 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."[199] 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.'"[200]

---

[193] 79 Fed. Reg. at 26096.

[194] 48 C.F.R. § 252.246-7007(c)(9), (e) (eff. May 6, 2014).

[195] National Defense Authorization Act of 2015, Pub. L. No. 113-291, § 817, 128 Stat. 3432 (2014).

[196] 81 Fed. Reg. 50635, at 50640 (August 2, 2016).

[197] *Id.* at 50640. It noted that DoD uses the Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs.

[198] *Id*. at 50647 (codified at 48 C.F.R. § 202.101, eff. Aug. 2, 2016).

[199] *Id.*

[200] 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.

More importantly, the rule implemented a three-tier approach to selecting suppliers of electronic parts. The revised policy section[201] and the corresponding new contract clause at DFARS § 252.246-7008 (sometimes referred to herein as "Contract Clause 7008)[202] 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, (b) their authorized suppliers, or (c) suppliers that obtain such parts exclusively from the original manufacturers of their parts or their authorized suppliers.[203]

The second tier ("Tier Two) addresses situations where electronic parts were not in production by the original manufacturer or an authorized aftermarket manufacturer, and they were 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,"[204] 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.[205] Next, the contractor is required to assume responsibility for the authenticity of parts provided by the contractor-approved supplier.[206] Finally, the rule makes the selection of contractor-approved suppliers subject to review and audit by the contracting officer.[207]

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.[208] 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

---

[201] 48 C.F.R. § 246.870-2 (eff. Aug. 2, 2016).

[202] 48 C.F.R. § 252.246-7008 (eff. Aug. 2, 2016).

[203] 48 C.F.R. § 246.870-2(a)(i); 48 C.F.R. § 252.246-7008(b)(1).

[204] 48 C.F.R. § 246.870-2(a)(ii); 48 C.F.R. § 252.246-7008(b)(2).

[205] 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.

[206] 48 C.F.R. § 246.870-2(a)(ii)(B); 48 C.F.R. § 252.246-7008(b)(2)(ii).

[207] 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).

[208] 48 C.F.R. § 246.870-2(a)(ii)(C)(2); 48 C.F.R. § 252.246-7008(b)(3).

obtains an electronic part from a subcontractor (other than the original manufacturer) who refused to accept flow down of the sourcing provisions.[209] 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.[210]

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.[211] 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.[212] 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.[213]

3. 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."[214] 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.[215]

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.[216] 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.[217] The only instances in which the contractor is not required to

[209] 48 C.F.R. § 246.870-2(a)(ii)(C)(2)(i); 48 C.F.R. § 252.246-7008(b)(3)(i)(A).
[210] 48 C.F.R. § 246.870-2(a)(ii)(C)(2)(ii); 48 C.F.R. § 252.246-7008(b)(3)(i)(B).
[211] 48 C.F.R. § 252.246-7007 (eff. May 6, 2014).
[212] 81 Fed. Reg. 50635, at 50640 (codified at 48 C.F.R. § 252.246-7007(c)(5), eff. May 6, 2014).
[213] *Id.* at 50640 (codified at 48 C.F.R. § 252.246-7007(e), eff. May 6, 2014).
[214] 48 C.F.R. § 231.205-71 (eff. May 6, 2014).
[215] 48 C.F.R. § 231.205-71(b)(3) (eff. May 6, 2014).
[216] 81 Fed. Reg. 59510, at 59515 (codified at 48 C.F.R. § 231.205-71(b)(3)(i), eff. Aug. 30, 2016).
[217] *Id.* (codified at 48 C.F.R. § 231.205-71(b)(3)(ii), eff. Aug. 30, 2016).

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.[218]

4. 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.[219] 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 subparagraph (A), if obtaining the electronic parts in accordance with such clauses is not possible;

---

[218] *Id.*

[219] 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).

(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.

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.[220] Section 815 of the FY 2017 NDAA deleted the term "trusted suppliers" and inserted "suppliers meeting anticounterfeiting requirements" throughout Section 818(c)(3).[221] 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"). [222] No additional information about DFARS Case 2017-D023 has been located, and its status today remains unclear.

---

[220] National Defense Authorization Act for Fiscal Year 2017, Public Law 114-328, 130 Stat. 2000 (Dec. 23, 2016).

[221] *Id.* at § 815.

[222] The *Counterfeit Parts* blog authored by Henry Livingston contains the following notes:

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."[223] 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 suspect counterfeit electronic parts."[224] 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).[225]

5. 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.[226] 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.[227] After the FAR case was opened in 2013, a proposed rule was

---

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/.

[223] 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).

[224] FY 2012 NDAA § 818(c)(3)(C) (as amended Dec. 23, 2016).

[225] *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).

[226] FY 2012 NDAA § 818(c)(4), (5).

[227] 84 Fed. Reg. 64680 (November 22, 2019).

published on June 10, 2014,[228] and a public meeting was held on June 16, 2014.[229] However, a final rule did not issue until November 2019, with the amendments finally taking effect on December 23, 2019.[230]

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[231] and any items that the contracting officer determines to be critical items[232] for which the reporting requirements would be appropriate.[233] 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 as part of the service being provided.[234] The reporting requirements do not apply to acquisitions of commercial items, including commercially available off-the-shelf ("COTS") items.[235]

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.[236] That awareness could arise from inspection, testing, record review, or notification from another source, such as a seller, customer, or third party.[237] 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.[238] 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,

---

[228] 79 Fed. Reg. 33164 (June 10, 2014).

[229] 84 Fed. Reg. 64680, at 64682.

[230] 84 Fed. Reg. 64680.

[231] *See* 48 C.F.R. 52.246-11 Higher-Level Contract Quality Requirement.

[232] 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).

[233] *Id.* (codified at 48 C.F.R. § 46.317(a)(1), eff. Dec. 23, 2019).

[234] *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.

[235] *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.

[236] *Id.* at 64695 (codified at 48 C.F.R. § 52.246-26(b)(4), eff. Dec. 23, 2019).

[237] *Id.*

[238] *Id.* (codified at 48 C.F.R. § 52.246-26(c), eff. Dec. 23, 2019).

provided that the contractor or subcontractor made a reasonable effort to determine that the report was factual.[239]

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.[240] 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.[241] Finally, the contractor is required to retain counterfeit or suspect counterfeit items in its possession until it receives disposition instructions from the contracting officer.[242] 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.[243]

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.

6. 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

---

[239] *Id.* (codified at 48 C.F.R. § 52.246-26(f), eff. Dec. 23, 2019).
[240] *Id.* (codified at 48 C.F.R. § 52.246-26(b)(1), eff. Dec. 23, 2019).
[241] *Id.* (codified at 48 C.F.R. § 52.246-26(b)(2), eff. Dec. 23, 2019).
[242] 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).
[243] 84 Fed. Reg. 64680, at 64695 (codified at 48 C.F.R. § 52.246-26(g)(1)(iii), eff. Dec. 23, 2019).

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.[244] The examples included overarching quality management system standards such as ISO 9001, ANSI/ASQC E4, ASME NQA-1, SAE AS9100, SAE AS 9003, and ISO/TS 16949, as well as product or process specific standards such as SAE AS5553.[245]

7. 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 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.

C. 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."[246] 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.[247]

---

[244] 79 Fed. Reg. 70344 (Nov. 25, 2014).
[245] *Id.*, codified at 48 C.F.R. 46.202-4(b) (eff. Dec. 26, 2014).
[246] FY 2012 NDAA § 818(b)(2).
[247] *Id.*

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.[248] 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.[249] 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 chain.*"[250] 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."[251] 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."[252] 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

---

[248] *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).

[249] *Id.* at § 818(c)(2)(A).

[250] *Id.* at § 818(e)(2)(A) (emphasis added).

[251] 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.

[252] *Id.*

> counterfeit electronic parts by allowing those contractors to make risk-based decisions on how best to implement supply chain assurance measures.[253]

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.[254] 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."[255]

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.[256] However, aside from setting out the list of minimum considerations, neither the statute nor the regulations defines 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. 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.[257]

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.[258] It is also inconsistent with DoD Instruction 4140.67, which instructs DoD Component heads

---

[253] *Id.*
[254] *Id.* The comments state that "[t]his change confirms the final rule with DoDI 4140.67."
[255] 48 C.F.R. § 252.246-7008(c)(1)."
[256] 48 C.F.R. § 246.870-2(b); 48 C.F.R. § 252.246-7007(b), (c).
[257] 48 C.F.R. § 252.246-7007(c)(2) (emphasis added).
[258] 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.

to integrate DoD anti-counterfeiting policy into all relevant regulations and contract requirements.[259] 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."[260]

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."[261] 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.[262]

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.[263] 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.[264]

The U.S. Defense Logistics Agency ("DLA") Land and Maritime has adopted the SAE AS6171 set of standards for use by the DoD,[265] but it is still being called out only infrequently in DoD contracts. Test

---

[259] U.S. Department of Defense, Instruction No. 4140.67, *DoD Counterfeit Prevention Policy* (2013), at 9.

[260] *Id.* at 10.

[261] 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.

[262] *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.*

[263] Michael H. Azarian, *An Overview of Risk-Based EEE Counterfeit Part Detection Based on SAE AS6171*, *supra* note 236, at 1.

[264] *Id.* at 2.

[265] Defense Logistics Agency, *Adoption Notice*, SAE AS6171 (March 28, 2017), available at https://landandmaritimeapps.dla.mil/Downloads/MilSpec/Docs/SAE/saeas6171.pdf.

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,[266] but the ANSI National Accreditation Board, an accreditation body, lists only four labs that are accredited under SAE AS6171. [267]

D. DoD Issuances

The DoD issues a variety of documents that prescribe or implement policy on a specific subject, including directives, memoranda, instructions, and manuals.[268] 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.[269] DoD Manuals implement the policies contained in DoD Directives and Instructions and may be published in several volumes if they are lengthy.[270] Several DoD Issuances relate in some way to counterfeit prevention and mitigation.

1. 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.[271] For the first time, the Instruction explicitly recognized the need to prevent counterfeit materiel from entering the defense supply chain.[272] 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,

---

[266] Defense Logistics Agency, *List of Commercial Laboratories Suitable for Testing Military Devices*, available at https://landandmaritimeapps.dla.mil/offices/sourcing_and_qualification/labsuit.aspx.

[267] 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.

[268] *See Overview of Department of Defense Issuances*, available at https://www.esd.whs.mil/Portals/54/Documents/DD/iss_process/DoD_Issuances.pdf.

[269] *Id*.

[270] *Id*.

[271] 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/.

[272] Interview with Anonymous Source from DoD (notes in possession of authors).

installations, and utilities."[273] "Counterfeit materiel" includes all materiel "whose identity or characteristics have been deliberately misrepresented, falsified, or altered without legal right to do so."[274]

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,[275] 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."[276] 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.[277] 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.[278] 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[279]; 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 theft.[280] 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.[281]

2. 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.[282] The so-called "Kendall Memo" recognized that counterfeit items pose a "serious threat to the safety and operational effectiveness" of DoD

---

[273] DoD Instruction 4140.01 § G.2.
[274] *Id.*
[275] *Id.* at § 1.2(d).
[276] *Id.* at § 2.2.
[277] *Id.* at § 2.3(a), (b).
[278] *Id.* at § 2.5(b), (c).
[279] *Id.* at § 2.7(c).
[280] *Id.* at § 2.7(f).
[281] *Id.* at § 3.3.
[282] 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"].

systems.[283] 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.[284] 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.[285]

3. 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.[286] The purpose of DoD Instruction 4140.67 was to establish policy, provide direction, and assign responsibilities for prevention, detection, and remediation of counterfeit materiel in the DoD supply chain.[287] 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.[288]

Like the Kendall Memo, DoD Instruction 4140.67 allocates responsibility for counterfeit prevention and mitigation across the DoD.[289] 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

---

[283] 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.

[284] *Id.* at 1.

[285] *Id.* at 1-2.

[286] Department of Defense Instruction 4140.67, *DoD Counterfeit Prevention Policy*, § 1(d), at 1 (April 26, 2013) [hereinafter "DoD Instruction 4140.67"].

[287] *Id.* at § 1.

[288] *Id.* at § 3.

[289] 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.

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.[290] Specific responsibilities are further allocated to the Assistant Secretary of Defense for Sustainment and the Assistant Secretary of Defense for Acquisition.[291] The DoD Component Heads[292] 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.[293]

4. 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.[294] 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.[295] 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.[296]

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, .

---

[290] *Id.* at 7.

[291] *Id.* at 8.

[292] 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.

[293] *Id.* at 9-10.

[294] 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"].

[295] *Id.* at § 2(c).

[296] *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.

. ., by foreign intelligence, terrorists, or other hostile elements."[297] 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.[298]

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.
>
> (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.[299]

5. Other DoD Guidance

In 2018, the Department of the Navy issued SECNAV Instruction 4855.20A, its Counterfeit Materiel Prevention policy.[300] 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

---

[297] *Id.* at § 1(a).
[298] *Id.* at § 1(b).
[299] *Id.* at § 4.
[300] 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).

other required authorities.[301] SECNAV Instruction 4855.20A adopted the definition of "counterfeit materiel" used in DoD Instruction 4140.47.[302]

The Army Materiel Command also developed a Counterfeit Parts and Materials Prevention Program Guidebook in 2018.[303] 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). The regulation is currently being updated based on reviews of subject matter experts from across the Army, and is expected to be released in 2022. 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 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.[304]

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.

E. 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.

---

[301] SECNAV Instruction 4855.20A § 5.

[302] "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.

[303] 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.

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

1. 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.[305] In addition, it creates civil causes of action for trademark infringement, false advertising, dilution, and other claims.[306]

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.[307]

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 for trademark infringement. Use of a counterfeit mark subjects the user of the infringing mark to treble damages,[308] and it also gives the trademark owner the right to elect an award of statutory damages instead of actual damages and profits.[309]

---

[305] 15 U.S.C. § 1051.
[306] 15 U.S.C. §§ 1114, 1125.
[307] 15 U.S.C. §§ 1114(1).
[308] 15 U.S.C. § 1117(b).
[309] 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

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."[310] To be "substantially indistinguishable, two marks must be nearly identical . . . with only minor differences which would not be apparent to an unwary observer."[311] 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.[312] "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."[313]

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.*,[314] the Ninth Circuit Court of Appeals held that a broker was liable for trademark infringement for distributing Intel math coprocessors which had been relabeled from slower chips to faster and more expensive math coprocessors.[315] 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."[316] 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.

---

(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.

[310] 15 U.S.C. §§ 1127; Tiffany and Co. v. Costco Wholesale Corp., 971 F.3d 74, 95 (2d Cir. 2020).

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

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

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

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

[315] *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.

[316] *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).

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.[317] 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."[318] It further stressed that full disclosure about the condition of a product is required in order to avoid liability for trademark infringement.[319] 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.[320]

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.[321]

Other courts have reached similar conclusions. See, e.g., *Beltronics USA, Inc. v. Midwest Inventory Distribution LLC*,[322] 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

---

[317] *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).

[318] *Id*.

[319] *Id.*, *citing* Champion Spark Plug Co. v. Sanders, 331 U.S. 125 (1947).

[320] *Id. at* 619-20 (citations omitted).

[321] *Id.* at 620.

[322] 562 F.3d 1067, 1072 (10th Cir. 2009). The Tenth Circuit cited a long line of opinions from other circuits reaching similar conclusions.

mark.[323] 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.[324]

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.[325] The Lanham Act does authorize a court to enter an award of attorney fees to a prevailing party in an exceptional case.[326] An exceptional case is one in which the infringing party acts in a malicious, fraudulent, deliberate, or willful manner,[327] 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 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.[328]

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,

---

[323] Beltronics USA, Inc. v. Midwest Inventory Distribution, LLC, 522 F. Supp. 2d 1318, 1327 (D. Kan. 2007), *aff'd,* 562 F.3d 1067.

[324] *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."

[325] 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.

[326] 15 U.S.C. § 1117(a).

[327] 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).

[328] *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."

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.[329] 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."[330] 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.[331] 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.

Lanham Act Section 43(a) provides multiple causes of action to the owners of both registered and unregistered marks:[332]

> 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,

---

[329] 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.

[330] 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.

[331] 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.

[332] 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.

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. [333]

Section 43(a) thus creates two distinct causes of action: false association and false advertising.[334]

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.[335] 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.

2. 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 such goods.[336] 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.[337]

---

[333] 15 U.S.C. §1125(a) (referred to as "Lanham Act § 43(a)").

[334] *See* Lexmark Intern., Inc. v. Static Control Components, Inc., 572 U.S. 118, 122 (2014).

[335] *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.

[336] 18 U.S.C. § 2320(a)(1).

[337] Stop Counterfeiting in Manufactured Goods Act, H.R. 32, 109th Cong. (2006).

Section 818 of the FY 2012 NDAA subsequently made it a crime, with enhanced penalties, to traffic in counterfeit military goods and services.[338]

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).[339]

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.[340]

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 –

[338] FY 2012 NDAA § 818(h).
[339] 18 U.S.C. § 2320(a) (emphasis added).
[340] 18 U.S.C. § 2320(f)(4). The term "counterfeit mark" is defined in 18 U.S.C. § 2320(f)(1).

(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;

(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.[341]

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.[342]

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:

---

[341] 18 U.S.C. § 2320(f)(1).
[342] *Id.*

(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.[343]

Incidents involving serious bodily injury or death carry even heavier penalties.[344]

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.[345]

3. 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,

[343] 18 U.S.C. § 2320(b)(1).
[344] 18 U.S.C. § 2320(b)(2).
[345] 18 U.S.C. §§ 2320(c), 2323.

> 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.[346]

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 purpose of executing, or attempting to execute, the scheme (or specified fraudulent acts).[347] However, to be part of the execution of the fraud, the use of the mails need not be an essential element of the scheme.[348] Instead, it is sufficient for the mailing to be "incident to an essential part of the scheme,"[349] or "a step in [the] plot."[350]

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.[351]

---

[346] 18 U.S.C. § 1341 (as amended, Jan. 7, 2008).

[347] 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).

[348] *Id.* at 710, *citing* Pereira v. U.S., 347 U.S. 1, 8 (1954).

[349] *Id.* at 710-11, *citing* Pereira v. U.S., 347 U.S. at 8.

[350] *Id*. at 711, *citing* Badders v. U.S., 240 U.S. 391, 394 (1916).

[351] 18 U.S.C. §1343(as amended Jan. 7, 2008).

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.[352] Use of emails is a type of communication that may give rise to wire fraud.[353] Similarly, use of cellular telephones may constitute wire fraud.[354]

Trafficking in counterfeit goods or services, mail fraud, and wire fraud all constitute racketeering activity under 18 U.S.C. § 1961.[355] 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.[356] A pattern of racketeering activity requires at least two acts of racketeering activity.[357] A violation of the act can result in fines, imprisonment, and forfeiture of the proceeds of the racketeering activity and associated enterprise.[358] Civil remedies are also available[359]; however, it appears they are seldom successful.[360]

F. 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:

---

[352] 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").

[353] *See, e.g.,* U.S. v. Hussain, 972 F.3d 1138 (9th Cir. 2020).

[354] U.S. v. Nunez, 78 Fed. Appx. 989 (5th Cir. 2003).

[355] 18 U.S.C. § 1961(1).

[356] 18 U.S.C. § 1962.

[357] 18 U.S.C. § 1961(5).

[358] *See* 18 U.S.C. § 1863.

[359] 18 U.S.C. § 1864.

[360] *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").

- 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.[361] The indictment alleged that Wren and McCloskey, though 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.[362]

- 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.[363] Yang agreed to plead guilty to conspiring to traffic in counterfeit goods and counterfeit military goods, and on April 17, 2014, he was sentenced to 21 months in prison.[364] 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.[365]

- 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.[366] 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

---

[361] 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.

[362] 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.

[363] U.S. v. Hao Yang, Case 1:13-cr-00305-JFM, Indictment (D. Maryland June 12, 2013).

[364] 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.

[365] *Id.*

[366] 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.

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.[367]

- 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.[368] 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.[369] 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.[370]
- 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.[371]
- 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.[372]

---

[367] *Id*.

[368] U.S. v. Peter Picone, Case No. 3:13-CR-128 AWT, Indictment (D. Conn. June 25, 2013).

[369] 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.

[370] *Id*.

[371] 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.

[372] 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.

- 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."[373] Vasquez was charged with wire fraud, 20 counts of trafficking in counterfeit goods, and one count of trafficking in counterfeit military goods.[374] He was sentenced to 46 months in prison and ordered to pay $144,000 in restitution. The press release announcing his sentencing further 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.[375]

G. 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.[376] A few of the standards relevant to counterfeit avoidance and prevention are discussed below.

1. IDEA

The Independent Distributors of Electronics Association ("IDEA") is an association of independent distributors that promotes quality initiatives in the supply chain.[377] It focuses on disseminating information to its members and other independent distributors with the goal of "stamping out counterfeit

---

[373] 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.

[374] *Id*.

[375] 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.

[376] 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.

[377] Faiza Khan Interview Summary (Appendix 19), at 1.

components."[378] IDEA provides Responsible Procurement Solutions™, a process for procurement of electronic components, inspection, and disposition of suspect counterfeits.[379] 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."[380]

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.[381] 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 Management System Standard for Independent Distributors of Electronics Association Members).[382] A new purchasing standard directed to buyers is also under development.[383]

The original IDEA-STD-1010 was released in October 2006, and the current version, IDEA-STD-1010-B was released in April 2011.[384] Ms. Khan indicated that the next revision, IDEA-STD-1010-C, is currently under development and should be available near the end of 2021.[385] IDEA-STD-1010-B relates to visual inspection and distinguishes between counterfeit and substandard parts.[386] 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."[387] "Substandard," on the other hand, means a "device that does not meet the manufacturer's stated specifications for form, fit, or function."[388]

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.[389] Testing facilities must be qualified, including ISO Certification at a minimum and consideration of issues

---

[378] *Id.* at 1.
[379] *See* https://www.idofea.org/about.html.
[380] Faiza Khan Interview Summary, at 1.
[381] *Id.* at 1.
[382] *Id.* at 1; *see also* https://www.idofea.org/idea-products/quality-standards.html.
[383] Faiza Khan Interview Summary, at 1.
[384] Independent Distributors of Electronics Association, IDEA-STD-1010-B: *Acceptability of Electronic Components Distributed in the Open Market* (hereinafter IDEA-STD-1010-B) (2011).
[385] Faiza Khan Interview Summary, at 1.
[386] *Id.* at 2.
[387] 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.
[388] IDEA-STD-1010-B § 5.9.
[389] *Id.* at § 6.

such as available equipment, business practices, and personnel.[390] 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).[391] 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.[392] 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 nonconforming product conditions.[393] Finally, the standard provides detailed inspection checklists and a lengthy list of other relevant standard generating bodies and associations.[394]

IDEA-QMS-9090, the Quality Management Standard, is intended for use by IDEA members, although other independent distributors may also use it as guidance.[395] 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."[396] 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.[397]

2. 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."[398] One of SAE's core competencies is voluntary consensus standards development.[399] 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

---

[390] *Id.* at § 8.
[391] *Id.* at § 10.
[392] *Id.* at § 11.
[393] *Id.* at § 12.
[394] *Id.* at §§ 14, 16.
[395] *See* Faiza Khan Interview Summary, at 2.
[396] Independent Distributors of Electronics Association, IDEA-STD-9090: *Quality Management System Standard for Independent Distributors of Electronics Association Members* § 10.1 (2018).
[397] *Id.* at § 10.2.
[398] SAE International, *About Us*, available at https://www.sae.org/about.
[399] *Id.*

address aspects of preventing, detecting, responding to, and counteracting the threat of counterfeit electronic components.[400] 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.[401]

a. 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 that procure, integrate, or repair EEE parts or assemblies.[402] 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."[403]

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."[404] 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.[405]

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."[406] These processes include training of personnel and purchasing parts from

---

[400] 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.

[401] SAE Aerospace, Committee Charter, SAE G-21 Counterfeit Materiel Committee (October 2010), available at https://www.sae.org/servlets/works/committeeHome.do?comtID=TEAG21.

[402] SAE International, AS5553C: *Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition* (hereinafter "SAE AS5553C"), at 3 (2019).

[403] *Id.* at 1.

[404] *Id.* at § 2.2.2.

[405] *Id.*

[406] *Id.* at § 3.1.

authorized sources whenever possible.[407] 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.[408] Flow downs, traceability, and reporting are also required.[409] AS5553 was adopted by the DoD on August 31, 2009.

b. 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 AS6171A, was released in April 2018.[410] 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."[411] 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."[412]

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."[413] 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.[414] A "suspect counterfeit part" is a part "for which there is objective, credible evidence indicating that the part is likely a Counterfeit Part."[415]

---

[407] *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 authorize sources, when those parts are still in production or available in stock. *Id.* at 7.

[408] *Id.* at § 3.1.3.

[409] *Id.* at §§ 3.1.4, 3.1.7, 3.1.8.

[410] SAE International, AS6171: *Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts*, Rev. A, at 1 (2018) [hereinafter "SAE AS6171A"].

[411] *Id.* at 1.

[412] *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.

[413] *Id.* at § 2.2.4.

[414] *Id.* at § 2.2.4.

[415] *Id.* at § 2.2.1.

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.[416] 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.[417] 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.[418]

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.[419]

- 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.[420]
- AS6171/4: Techniques for Suspect/Counterfeit EEE Parts Detection by Delid/Decapsulation 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.[421]

---

[416] *Id.* at § 1.1.
[417] *Id.* at § 3.1.
[418] *Id.* at § 3.
[419] *Id.* at § 4.
[420] *Id.*
[421] *Id.*

- AS6171/5: Techniques for Suspect/Counterfeit EEE Parts Detection by Radiological Test Methods. Internal and external inspection intended to detect deliberate misrepresentation or damage.[422]
- 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.[423]
- 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.[424]
- AS6171/8: Techniques for Suspect/Counterfeit EEE Parts Detection by Raman Spectroscopy Test Methods. Used for identification of materials.[425]
- AS6171/9: Techniques for Suspect/Counterfeit EEE Parts Detection by Fourier Transform Infrared Spectroscopy (FTIR) Test Methods. Another test used for identification of materials.[426]
- 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.[427]
- 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.[428]

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

---

[422] *Id.*
[423] *Id.*
[424] *Id.*
[425] *Id.*
[426] *Id.*
[427] *Id.*
[428] *Id.*

c. SAE AS6081

SAE AS6081 ("Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors") was issued in November 2012,[429] 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.[430] 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,[431] including practices relating to supplier management, procurement, inspection, testing, and evaluation.[432]

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."[433] A "fraudulent part" is "[a]ny suspect part misrepresented to the Customer as meeting the Customer's requirements."[434] 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.[435]

AS6081 requires covered distributors[436] 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.[437] Those processes include an assessment of potential

---

[429] SAE International, AS6081, *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors* (Nov. 2012) [hereinafter "SAE AS6081"].

[430] *Id.* at 1.

[431] 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.

[432] *Id.* at 1, 3.

[433] *Id.* at § 3.3.

[434] *Id.* at § 3.2.

[435] *Id.* at § 3.1.

[436] 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.

[437] *Id.* at § 4.2. Requirements must also be flowed down to the distributor's suppliers, contractors, and subcontractors.

suppliers to determine the risk of receiving fraudulent or counterfeit parts and creation of a list of approved suppliers.[438] 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.[439] The distributor must retain records documenting supply chain traceability wherever possible.[440]

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.[441] 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.[442] 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 with the opportunity to verify the findings.[443] 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.[444]

---

[438] *Id.* at § 4.2.2.

[439] *Id.*

[440] *Id.* at § 4.2.4.

[441] *Id.* at § 4.2.6.4.

[442] *Id.*

[443] *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.

[444] *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.

d. 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 or counterfeit parts will enter the supply chain.[445] 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,[446] 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.[447] 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."[448]

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.[449] 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.[450] 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.[451] Emphasis is placed on traceability back to the 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.[452] 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.[453]

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.[454] Returns

---

[445] 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.

[446] SAE AS6496 at § 1.2.

[447] *Id.* at § 2.3.

[448] *Id.* at § 2.3 (emphasis in original).

[449] *Id.* at § 3.2.

[450] *Id.*

[451] *Id.* at § 3.4.2.

[452] *Id.* at §§ 3.5, 3.5.1. The term "military parts" is not defined by the standard.

[453] *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.

[454] *Id.* at § 3.6.1.

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.[455] 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.[456] Suspect, fraudulent, and counterfeit parts must be quarantined and cannot be reintroduced to the supply chain.[457] Counterfeit parts must be reported to appropriate organizations, including customers, GIDEP, and law enforcement authorities.[458]

3. 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.[459] CCAP-101 is a certification program for the detection and avoidance of counterfeit electronic components supplied by independent distributors.[460] 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."[461] 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 markings have been altered. All components that cannot be authenticated through test & inspection shall be treated as counterfeit."[462]

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]."[463] 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

---

[455] *Id*.
[456] *Id*.
[457] *Id*.
[458] *Id*. at § 3.10.
[459] Components Technology Institute, Inc., CCAP-101, *Counterfeit Parts Avoidance Program, Certification For* (Rev. E-1, July 11, 2013).
[460] *Id*. at 1.
[461] *Id*. Note the definition is so broad that it even encompasses components which infringe upon the patent rights of another.
[462] *Id*. at 3.
[463] *Id*. at 4.

required to avoid delivery of counterfeits.[464] 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.[465] Required testing includes microscopic inspection and visual inspection, as well as additional specified tests for particular types of components.[466] The independent distributor is also required to have a formal procedure for selecting, approving, and monitoring its suppliers.[467]

4. 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.[468] 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."[469] 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.[470] In addition, manufacturers are required to develop and implement a counterfeit parts control plan, including a list of authorized distributors and a list of approved suppliers.[471] The standard also addresses returns and restocking items into inventory.[472]

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

---

[464] *Id*.

[465] *Id.* at 5-6. ISO 9001 is an international quality management standard. *See* https://www.iso.org/standard/62085.html.

[466] *Id.* at 7-19.

[467] *Id.* at 7.

[468] JEDEC Solid State Technology Association, JESD243, *Counterfeit Electronic Parts: Non-Proliferation for Manufacturers* (March 2016) [hereinafter "JESD243"].

[469] JESD243, at 1.

[470] *Id.* at § 4.1.

[471] *Id.* at § 4.2.

[472] *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).

counterfeit, fraudulent, and recycled electronic components in avionics.[473] 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."[474] The companion standard covers management of electronic components from non-franchised sources.[475]

H. Recommendations and Conclusions

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

1. 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.[476] Congress specifically indicated that those definitions "shall include previously used parts represented as new."[477] 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:

- 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

---

[473] 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).

[474] *Id.* at § 3.1.5.

[475] International Electrotechnical Commission, IEC 62688-2:2019, *Process management for avionics – Counterfeit prevention – Part 2: Managing electronic components from non-franchised sources* (2019-09).

[476] FY 2012 NDAA § 818(b)(1).

[477] *Id.*

unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.[478]

- 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."[479]
- 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."[480]
- 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."[481]
- 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."[482]
- 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.[483]
- SAE AS6171A: A "counterfeit part" is:

---

[478] 48 C.F.R. § 202.101.
[479] DoD Instruction 4140.01 § G.2, at 19.
[480] DoD Instruction 4140.67, Glossary, at 12.
[481] SECNAV Instruction 4855.20A, Enclosure 2 (Definitions) (2018).
[482] IDEA-STD-1010-B § 5.9.
[483] 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).

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
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.[484]

- 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."[485]
- 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."[486]
- 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."[487]
- 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."[488]
- 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."[489]

---

[484] SAE AS6171A § 2.2.4.
[485] SAE AS6174A § 2.3.5.
[486] SAE AS6496 § 2.3; SAE AS6081 § 3.3.
[487] Components Technology Institute, Inc., CCAP-101, *Counterfeit Components Avoidance Program, Certification For* (Rev. E-1, 2013), at 3.
[488] JEDEC Solid State Technology Association, JESD243, Counterfeit Electronic Parts: Non-Proliferation for Manufacturers § 3 (2016).
[489] 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.

- Lanham Act: A "counterfeit" is a "spurious mark which is identical with, or substantially indistinguishable from, a registered mark."[490]
- 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;
>
> (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.[491]

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

[490] 15 U.S.C. § 1127.
[491] 18 U.S.C. § 2320(f)(1).

"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,"[492] and SAE AS6174A includes a similar definition of "fraudulent materiel."[493] Again, there is no requirement that the misrepresentation be knowing or deliberate. Fraud has been defined as "a knowing misrepresentation or knowing concealment of a material fact made to induce another to act to his or her detriment."[494] 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.[495] 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."[496] The problem with the inclusion of the word "fraud" as part of the definition of "counterfeit" part or materiel is that it raises the specter 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."

---

[492] SAE AS6496 § 2.3; SAE AS6081 § 3.2.

[493] 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.

[494] Bryan A. Garner, ed., BLACK'S LAW DICTIONARY (11th ed. 2019).

[495] *Id.*

[496] SAE AS6171A § 2.2.2.

A better approach may be for the DFARS and standards definitions to leave out any reference of 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 counterfeit part; certainly, within an organization, there should not be more than one definition in use.[497] 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.

2. 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,

[497] 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.

in 2018.[498] The Army Materiel Command developed a Counterfeit Parts and Materials Prevention Program Guidebook in 2018,[499] although it only provides recommendations and is not binding on Army Materiel Command personnel. The regulation is currently being updated based on reviews of subject matter experts from across the Army, and is expected to be released in 2022. 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 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.

3. 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*

---

[498] 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).

[499] 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.

their authorized suppliers.[500] 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.[501] 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?[502]

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 the OCM or an authorized distributor. Mr. Gray also pointed out that many authorized distributors are, in fact, small businesses.[503]

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.[504] 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.[505] Even in those instances when a part does go out of production, Mr. Olney observed that the government can still purchase

---

[500] 48 C.F.R. § 246.870-2(a)(1)(i); 48 C.F.R. § 252.246-7008(b)(1) (emphasis added).
[501] Robin Gray Interview Summary (Appendix 19), at 3.
[502] *Id.* at 3.
[503] *Id.* at 3.
[504] Andrew Olney Interview Summary (Appendix 19), at 2.
[505] *Id.* at 3.

parts from a company such as Rochester Electronics (an authorized distributor and licensed manufacturer) and authorized resellers that distribute legacy products.[506]

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."[507] 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.[508]

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].[509]

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."

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.

4. 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

---

[506] *Id.* at 3. *See also* Dan Deisz Interview Summary (Appendix 19), re Rochester Electronics' role in the supply chain.

[507] Dr. Brian Cohen Interview Summary (Appendix 19), at 4.

[508] *Id.* at 4.

[509] FY 2012 NDAA § 818(c)(3)(A)(i), as amended by FY 2017 NDAA § 815 (eff. Dec. 23, 2016).

appropriate policies and procedures in place to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts.[510] 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.[511]

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 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

[510] FY 2012 NDAA § 818(c)(3)(C), as amended by FY 2017 NDAA § 815 (eff. Dec. 23, 2016).
[511] 48 C.F.R. § 246.870-2(a)(ii).

suppliers. That appears to be inconsistent with the mandate in Section 818(c), as amended, and may result in a less demanding qualification process.

5. 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.[512] 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.[513] 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.[514]

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
>
> (C) Make documentation of inspection, testing, and authentication of such electronic parts available to the Government upon request.[515]

---

[512] 48 C.F.R. § 252.246-7007(b).

[513] 48 C.F.R. § 252.246-7007(c)(9).

[514] 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.

[515] 48 C.F.R. § 252.246-7008(b)(3)(i).

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.[516]

Conversely, Robert Bodemuller, a Supply Chain Quality Principle Engineer in 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.[517] 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.[518]

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.

6. 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

---

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

[517] Robert Bodemuller Interview Summary (Appendix 19), at 3.

[518] *Id.* However, Mr. Bodemuller noted that Lockheed does not believe it has an obligation to audit at the lower tiers of the supply chain.

that address a minimum of 12 issues.[519] 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 their 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.

7. 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 officer determines to be critical items.[520] 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

[519] 48 C.F.R. § 246.870-2(b); 48 C.F.R. § 252.246-7007(b), (c).
[520] 48 C.F.R. § 46.317(a).

the simplified acquisition threshold.[521] However, the reporting requirements do not apply to acquisitions of commercial items, including commercially available off-the-shelf ("COTS") items.[522]

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.[523] 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.[524] 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.[525] 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 authorities," and contractors should be provided with guidance about the identity of those authorities and how they can be contacted.

---

[521] *Id.*
[522] 48 C.F.R. § 46.317(b).
[523] FY 2012 NDAA § 818(c)(4).
[524] 48 C.F.R. § 52.246-26.
[525] *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.

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.[526] 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.[527] 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.[528]

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."

---

[526] Richard Smith Interview Summary (Appendix 19), at 2.

[527] 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.

[528] 48 C.F.R. § 52.246-26(f).

Designating suspect counterfeit parts as "nonconforming" makes it impossible for others to search the 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.[529] 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.[530]

8. 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.

---

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

[530] 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.

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 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,[531] 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 fall 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.

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

[531] *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.

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 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.[532]

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.

IX. Adoption of Machine Vision Technologies to Evaluate the Authenticity and Security of Microelectronic Parts

For purposes of this section of the report, the term "Image Analysis" refers to methods for automated image acquisition and/or processing using computer algorithms. Image Analysis 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;

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

- 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);
- 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.).

Image Analysis 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.[533] 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.

Image Analysis 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.

A. 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.

1. 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

[533] 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.

establish and maintain an acceptable counterfeit electronic part detection and avoidance system.[534] 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.[535]

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.[536]

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.[537]

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.

2. 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?*

---

[534] 48 C.F.R. § 246.870-2(b)(1).
[535] 48 C.F.R. § 246.870-2(b)(2).
[536] 48 C.F.R. § 252.246-7007(b)(2).
[537] 48 C.F.R. §§ 252.246-7008(b)(3)(i), (c)(2).

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.

3. Can Image Analysis Satisfy the Requirements for Visual Inspection?

It is readily apparent that Image Analysis can never satisfy the requirements for certain individual types of testing indicated by the relevant standards, such as solvent testing, X-ray fluorescence, acoustic microscopy, and Raman spectroscopy. However, a more detailed analysis is required to determine whether Image Analysis 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.[538] A trained inspector is required to conduct a physical examination of the devices.[539] 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.[540] 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.[541]

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 non-uniform color, exposed base material, repaired or bent leads, missing leads, and corrosion.[542] 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

---

[538] 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).

[539] *Id.* at § 3.1.

[540] *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.

[541] *Id.*

[542] *Id.* at 7.

texture discrepancies.[543] Differences in the corner radius, color discrepancies, and texture discrepancies between the top, bottom and sides of the part must be documented.[544] 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.[545] 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."[546]

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*."[547] 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.[548]

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.[549] 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.[550] CCAP-101 also requires a detailed visual inspection of the package, component markings, and lead condition.[551]

Image Analysis 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.[552] 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

---

[543] *Id.* at 12, 17.
[544] *Id.* at 17.
[545] *Id.* at 30.
[546] *Id.* at 7.
[547] SAE AS6081 at 19 (emphasis added).
[548] *Id.* at 20.
[549] IDEA-STD-1010-B at 32-37.
[550] *Id.* at 45-50.
[551] CCAP-101 at 11-12.
[552] *See* Section V(A) (Evaluation of Existing Machine Vision and AI Technologies), *supra*, for a description of the functionality of these systems.

inspection and imaging of microelectronic parts for compliance with the standards would require extensive programming and training of Image Analysis algorithms and redesign of part handling mechanical systems.

In principle, Image Analysis 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. Image Analysis would not satisfy the documentation review portion of general EVI, and in order for Image Analysis 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, Image Analysis-based inspection in place of inspection by the unaided eye. Furthermore, if parts were to be inspected while still in their packaging, the Image Analysis technology would have to be capable of imaging the parts through the packaging while still maintaining accuracy.

4. 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.[553] Tests and inspections are to be performed in accordance with "*accepted Government- and industry-recognized techniques*."[554] 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.[555]

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;

---

[553] 48 C.F.R. § 252.246-7007(c)(2).
[554] *Id.* (emphasis added).
[555] *Id.* at § 252.246-7007(c)(4).

(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.*[556]

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."[557] 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 sources."[558] 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.[559] 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, Image Analysis systems may be able to assist with the traceability requirements of Contract Clauses 7007 and 7008. Image Analysis 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.[560] In addition to external visual inspections, those tests may include X-ray

---

[556] 48 C.F.R. § 252.246-7008(c)(1), (2) (emphasis added).

[557] SAE AS5553 at 6.

[558] *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).

[559] *Id.*

[560] SAE AS6171C at 29.

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. 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.[561] 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.[562] 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."[563]

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.

---

[561] 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

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

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

B. 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.

1. 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 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.[564] 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.[565] 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.

---

[564] 48 C.F.R. §§ 252.246-7007, 252.246-7008.
[565] *See* 81 Fed. Reg. at 50646.

2. 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.[566]

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.[567]

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.[568]

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

---

[566] Robin Gray Interview Summary (Appendix 19), at 4.
[567] Andrew Olney Interview Summary (Appendix 19), at 3.
[568] Dr. Brian Cohen Interview Summary (Appendix 19), at 4.

low cost and cannot require that anything extra be added to the part."[569] 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.[570]

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 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.[571]

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."[572] 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.

C. 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

[569] Kevin Sink Interview Summary (Appendix 19), at 5.
[570] *Id.*
[571] Interview with Anonymous Source (notes in possession of authors).
[572] Robert Bodemuller Interview Summary (Appendix 19), at 4-5.

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.[573] 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.[574] The patent application must also satisfy certain disclosure requirements known as enablement, written description, and claim definiteness in order for a patent to issue.[575] Today, U.S. patents are enforceable for 20 years from the date the patent application was filed;[576] 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.[577] 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.[578] 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").[579]

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

---

[573] 35 U.S.C. § 271(a).
[574] 35 U.S.C. §§ 101, 103.
[575] 35 U.S.C. 112(a), (b).
[576] 35 U.S.C. § 154(a)(2).
[577] 35 U.S.C. § 202(c)(4).
[578] Broadcom Corp. v. Qualcomm Inc., 501 F.3d 297, 314 (3d Cir. 2007).
[579] *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).

adopted the Cooperative Classification System,[580] 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.

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.

1. 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

[580] Previously, the USPTO used the United States Patent Classification System.

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	Recognizing objects characterized 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.

2. 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.[581] 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.

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

# Indicates abandoned applications -- Abandoned applications have no patent protection. These can serve as prior art when applying for a patent.

a. 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.

i. "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.

I. Structural Features

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

Patent **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.

Patent **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.

Patent **US8908920Systems 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.

Patent **US8989500Method for Extracting Random Signatures from a Material Element and Method For Generating a Decomposition Base to Implement the Extraction Method**

Signoptic TechnologiesExpiration: 8/11/2027

Identifies non-moving elements within part of an object, generates a signature based on the vector of those random elements.

Patent **US9443298Digital 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.

Patent **US9582714Digital 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.

Patent **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.

Patent **US9672678Method 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.

Patent **US9972224Fibers 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.

Patent **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.

Patent **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.

Patent **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.

Patent **US20180053312Authentication-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.

Patent **US20200065577System 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.

Patent **WO2020028288Systems 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.

ii. 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.

Patent **US7256398Security 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.

Patent **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.

Patent **US8341759Detecting 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.

Patent **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.

Patent **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.

Patent **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.

Patent **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.

Patent **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.

Patent **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.

Patent **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.

Patent **US20170160320Methods 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.

iii. Measurement

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

Patent **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.

Patent **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.

I. Object Texture

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

Patent **US8325987Amorphous 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.

Patent **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.

Patent **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.

Patent **US20190286102System 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).

II. Defect Detection

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

Patent **US8472677Method 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.

Patent **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.

Patent **US9721337Detecting 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.

Patent **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.

b. 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.

i. 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.

Patent **US9885745* Apparatus and method for integrated circuit forensics**

US Secretary of NavyExpiration: 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.

Patent **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.

Patent **US20170032285Authenticating 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.

Patent **US20190189236Artificial 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.

Patent **US20190219525Method 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.

Patent **US20190279329Systems 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.

ii. 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.

Patent **US8798313Counterfeit 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.

Patent **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.

Patent **US10089478 Authentication method and system**
CoPilot Ventures Fund III LLC Expires: 9/4/2023

Normalizes observable characteristics corresponding to a unique pattern.

iii. Process by Physical Manipulation

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

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

*U.S. Air Force 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.

Patent **US9798910Mobile 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.

Patent **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.

Patent **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.

c. 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.

i. 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.

Patent **US8472677Method 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.

Patent **US8848905Deterrence 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.

Patent **US9031329Photo 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.

Patent **US9053364Product, 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.

Patent **US9646373System 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.

Patent **US9767459Detection 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.

Patent **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.

Patent **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.

Patent **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.

Patent **US20170160320Methods 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.

Patent **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.

Patent **US20190279377Determination 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.

ii. 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.

Patent **US6944331Locating 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 reference 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.

Patent **US8712163Pill 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.

Patent **US9384390Sensing 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.

Patent **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.

Patent **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.

Patent **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.

Patent **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.

d. Related technologies

i. 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.

I. 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

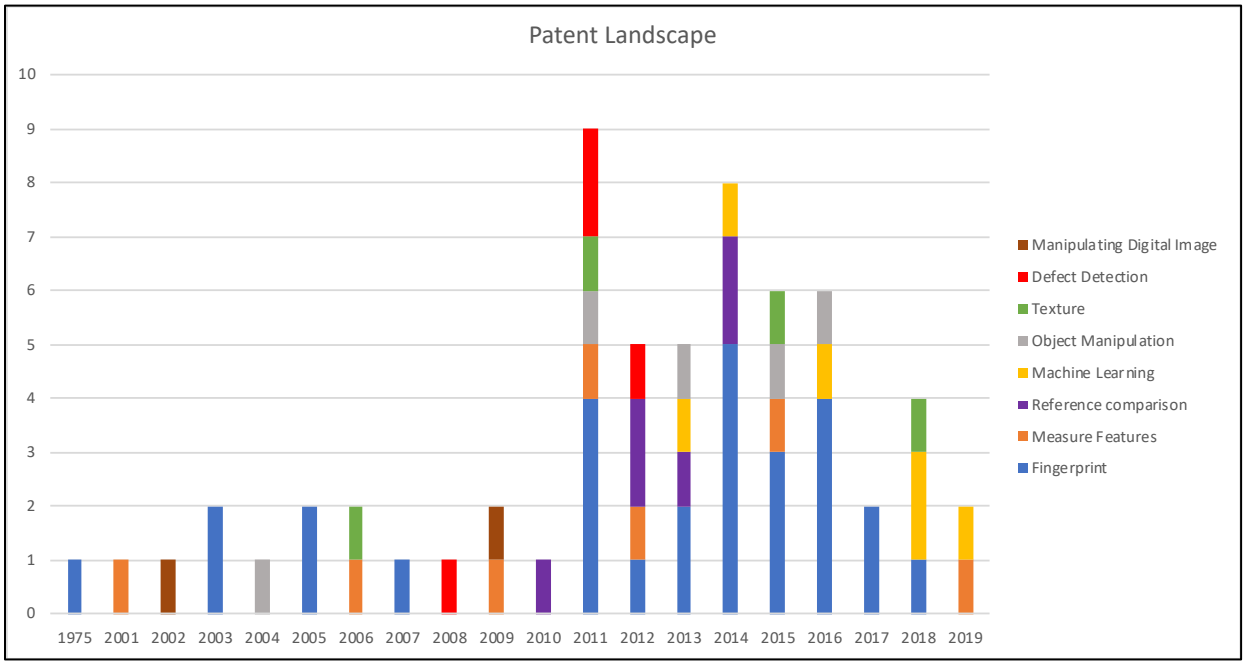


Figure 18. Patent Landscape

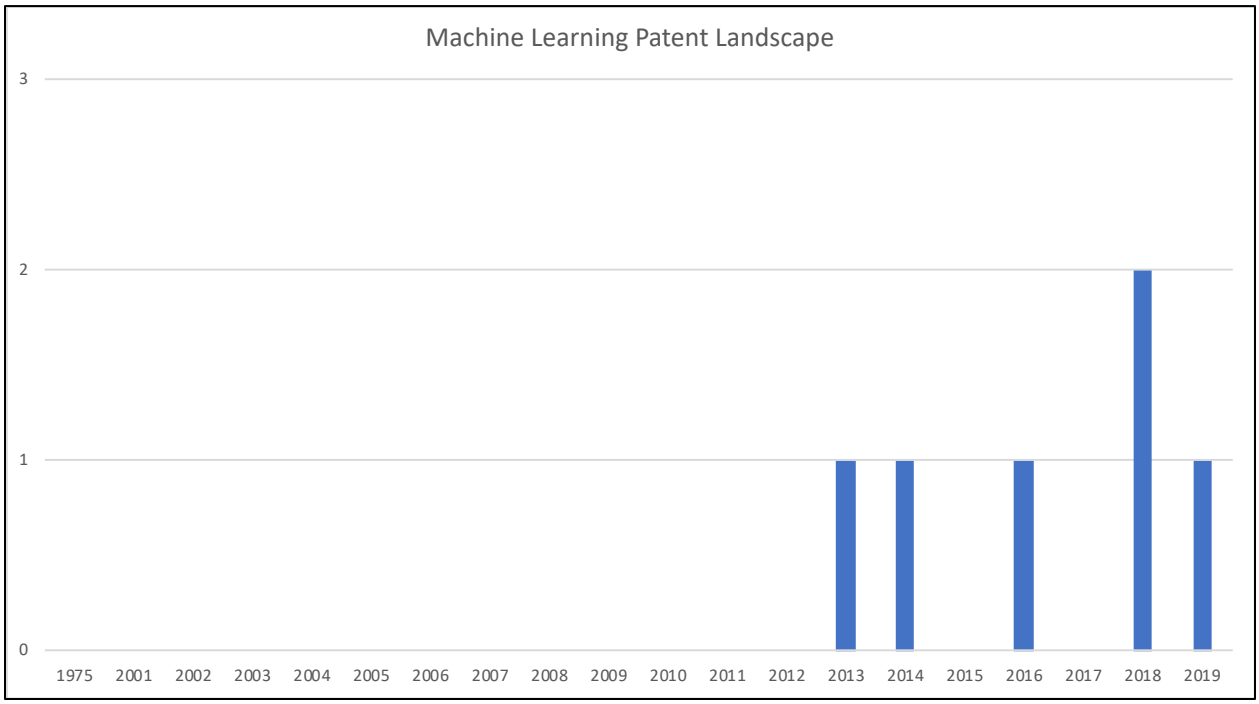


Figure 19. Machine Learning Patents by Year

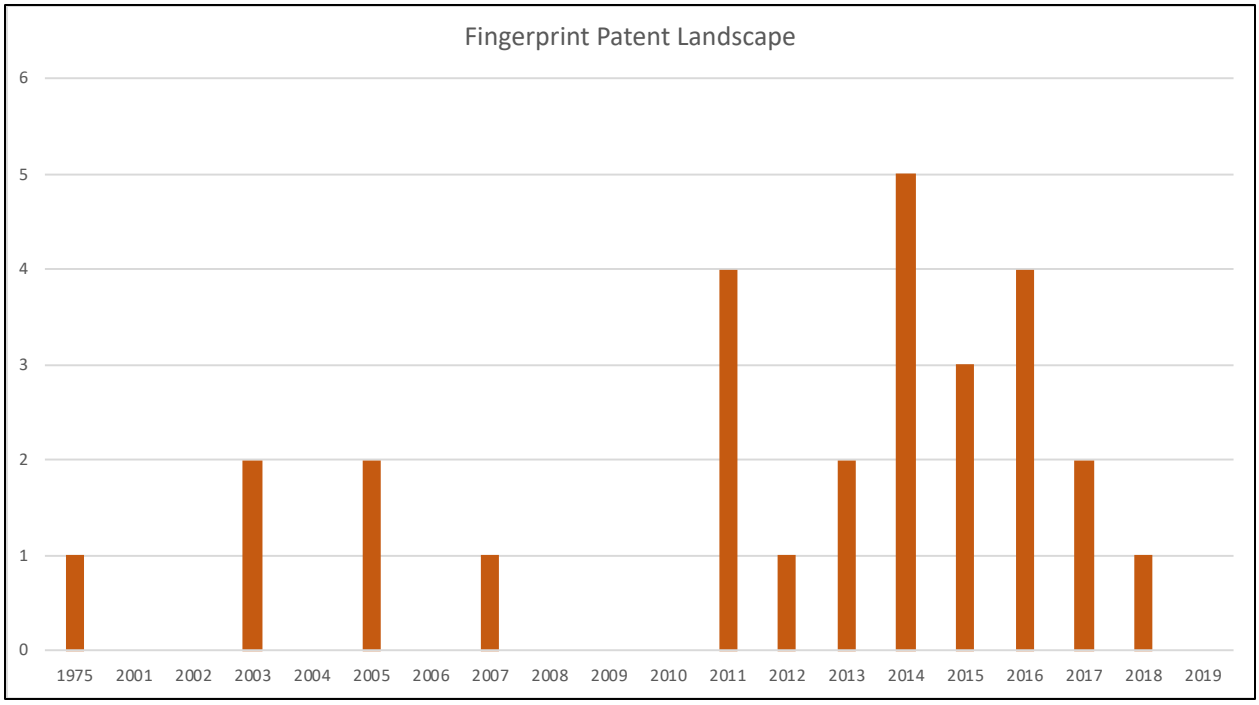


Figure 20. "Fingerprint" Patents by Year

D. 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.[582,583,584] 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.[585,586,587]

---

[582] Ujjwal Gwin, et al., *Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain,* 102 PROCEEDINGS OF THE IEEE 1207 (2014).

[583] 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.

[584] 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.

[585] 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

[586] Damir Akhoundov, *2019 ERAI Reported Parts Statistics,* ERAI Blog, available at https://www.erai.com/erai_blog/3167/2019_erai_reported_parts_statistics.

[587] 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.

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.[588] 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.

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 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.

E. 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,

[588] *See* Senate Armed Services Committee Report, published May 21, 2012.

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.