

NOT MEASUREMENT
SENSITIVE

DOE-HDBK-1221-2024

DOE HANDBOOK

Suspect/Counterfeit Items Resource Handbook



U.S. Department of Energy Washington, D.C. 20585

This page intentionally left blank.

Foreword

This Department of Energy (DOE) Handbook assists the DOE enterprise in preventing suspect/counterfeit items (S/CI) from entering the supply chain. Specifically, it provides examples and information that may be used to prevent, detect, document, report, and control these types of items. Internal and external resources have been referenced for additional information.

The Handbook is available for use by all DOE elements and their contractors.

This Handbook does not establish new requirements, and any existing requirements are explicitly referenced from a DOE Order. DOE Order requirements prevail. This handbook provides guidance to implement DOE S/CI requirements and therefore uses the words “should” and “may.”

Beneficial comments (recommendations, additions, and deletions), as well as any pertinent data that may be of use in improving this document, should be emailed to counterfeit@hq.doe.gov or addressed to:

Office of ES&H Reporting and Analysis (EHSS-23)

Office of Environment, Health, Safety and Security (EHSS)

U.S. Department of Energy 1000 Independence Avenue, SW Washington, DC 20585

Acknowledgments

This Handbook was developed with significant contributions of Chris Beaman (EHSS), Lisa Enstrom (ANL), Tammie Graham (LLNL), Gabrielle Holcomb (EHSS), Kristy Kistner (ORISE), Nathan Morley (NNSA), John Verderber (WRPS), Lucas White (HMIS), and Bill Wingfield (LANL).

Table of Contents

1	Introduction.....	1
2	Terminology.....	2
3	Suspect/Counterfeit Item (S/CI) Risks.....	10
4	S/CI General Process	15
5	Indicators for S/CI Hardware Items (Fasteners)	30
6	Electronics.....	37
7	Suspect/Counterfeit Software	52
8	Indicators of Suspect Components.....	59
9	Counterfeiting of NRTL Certifications and Symbols	67
10	Suspect/Counterfeit & Fraudulent Documentation and Certification	68
11	References.....	73
	Appendix A – Suspect/Counterfeit and Defective Fastener Inspection.....	A-1
	Appendix B – Other Information Related to S/CI.....	A-2
	Appendix C – Resources	C-1

List of Tables

Table 1: Risk Mitigation Table	12
Table 2: Counterfeit Risk Based Approach Example Table	14
Table 3: Headmark Comparisons.....	31
Table 4: Electronics Evaluation Table- Level of Rigor	43
Table 5: Legacy Fastener List Codes that correspond to Figure 41	A-2
Table 6: High Strength Fastener Examples.....	A-2
Table 7: Non-Compatible Standard Example	A-2

Table of Figures

Figure 1: Model of an S/CI Program General Process Flow	15
Figure 2: FAR 52.246-26 Reporting Structure at DOE	20
Figure 3: Suspect/Counterfeit Item Example Reporting Chart	28
Figure 4: SAE Grade 5 bolts without a manufacturer mark	32
Figure 5: Double-stamped Bolt	32
Figure 6: General Fastener Quality	33
Figure 7: 8.8 grade bolt no manufacturer marking	33
Figure 8: Sample disposition process for a ratchet strap	34
Figure 9: “KS”-marked bolt from Legacy Headmark List	35
Figure 10: Blacktopped Example	38
Figure 11: Blacktopped Example-Indent Filled	39
Figure 12: Blacktopped Example –Side View – Overspray	39
Figure 13: Sanding Example	40
Figure 14: Marking on Indent	40
Figure 15: Genuine Atmel Device	41
Figure 16: Counterfeit Atmel Device	42
Figure 17: Example of Acceptable Indent	45
Figure 18: Example of Suspect Indent	45
Figure 19: Example Indications of Remarking	46
Figure 20: Example Texture Irregularity between top and bottom surface of the same device	47
Figure 21: Example Dimensional Inspection	48
Figure 22: Example Resistance to Solvent Failure	48
Figure 23: Example Scrape Test Failure	48
Figure 24: Example XRF Analysis	49
Figure 25: S/CI prevention model for Software	57
Figure 26: Example Tampering	60
Figure 29: General Appearance	60
Figure 27: Example Low Quality Print	61
Figure 28: Example Incorrect Manufacturer Label	61
Figure 30: Configuration	62
Figure 34: Shackle Missing Manufacturer Marking	63
Figure 35: Marking Alteration	63
Figure 31: Example Suspect Piping	64
Figure 32: Suspect WATTS Gas Ball Valve Label	64
Figure 33: Example Used When Ordered New	65
Figure 36: Suspect/Counterfeit NRTL Sticker (TIC, 2020)	67
Figure 37: Font Indication Example	69
Figure 38: Alteration Example	70
Figure 39: Dates and Numeration Example	71
Figure 40: Signature Example	72
Figure 41: Legacy Fastener List	A-1
Figure 42: Badge Reminder	A-3

1 Introduction

1.1 Purpose

This Handbook assists the Department of Energy (DOE) in preventing suspect/counterfeit (S/CI) items from entering the supply chain. Information and examples are provided to support preventing, detecting, documenting, reporting, and controlling these types of items.

1.2 Applicability

This Handbook is applicable to the DOE enterprise including the NNSA, which consists of elements within the DOE/NNSA and their contractors.

1.3 Scope

This handbook should be used in combination with current versions of DOE Order (O) 414.1 (current), *Quality Assurance*, and DOE Guide (G) 414.1-2, *Quality Assurance Program Guide*. It is also recommended that organizations leverage the use of current industry standards that address Counterfeit Prevention Programs and processes.

Internationally recognized consensus standards such as those from the Society of Automotive Engineers (SAE) and Independent Distributors of Electronics Association (IDEA) Standard 1010-B, *Acceptability of Electronic Components Distributed in the Open Market* are especially useful for aiding in S/CI prevention and detection. A comprehensive list of the SAE standards for Counterfeit prevention and detection is provided in the Appendix C, *Resources* of this handbook.

The current version of DOE G 414.1-2 is a valuable reference for the principles, requirements, and practices that establish and implement an effective quality assurance program or quality management system in accordance with DOE O 414.1. In addition, DOE G 414.1-2 provides information on S/CI program implementation that may be used in combination with the information in this handbook. Although a graded approach is used throughout the handbook to manage processes such as procurements, inspections, assessments, evaluations, etc. if an S/CI is discovered, it must be reported in accordance with current DOE requirements such as those stated in DOE O 414.1 (current).

2 Terminology

2.1 Acronyms

AGA	American Gas Association
ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
ASQC	American Society for Quality Control
ASTM	American Society of Testing Materials
CGA	Canadian Gas Association
CGD	Commercial Grade Dedication
CFR	Code of Federal Regulations
CFSI	Counterfeit, Fraudulent, and Suspect Items
CISA	Cybersecurity & Infrastructure Security Agency
CMTR	Certified Material Test Report
COA	Command Option Argument
C of C	Certificate of Conformance
CVSS	Common Vulnerability Scoring System
DOE	Department of Energy
DPA	Destructive Physical Analysis
D-U-N-S	Data Universal Numbering System
EFCOG	Energy Facility Contractor Group
EPRI	Electric Power Research Institute
ERAI	Electronic Resellers Association International
FM	Factory Mutual
FMEA	Failure Mode and Effect Analysis
FQA	Fastener Quality Act
FTIR	Fourier Transform Infrared Spectroscopy
G	Guide
GIDEP	Government-Industry Data Exchange Program
GL	Generic Letters
HTTPS	Hypertext Transfer Protocol Secure
IACC	International Anti-Counterfeiting Coalition
IAEA	International Atomic Energy Agency

IAQG	International Aerospace Quality Group
IDEA	Independent Distributors of Electronics Association
IC	Integrated Circuit
IFI	Industrial Fasteners Institute
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
NCR	Nonconformance Report
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
NPM	Node Package Manager
NQA	Nuclear Quality Assurance
NRC	Nuclear Regulatory Commission
NRTL	Nationally Recognized Testing Laboratory
O	Order
OASIS	Online Aerospace Supplier Information System
OCM	Original Component Manufacturer (electronic components)
OEM	Original Equipment Manufacturer
OIG	Office of Inspector General
OMB	Office of Management and Budget
ORPS	Occurrence Reporting and Processing System
OSHA	Occupational Safety and Health Administration
PSI	Pounds per Square Inch
QA	Quality Assurance
RC	Run Configuration
SAE	Society of Automotive Engineers
SAM	Scanning Acoustic Microscopy
SBOM	Software Bill of Materials
S/CI	Suspect/Counterfeit Item
SEM	Scanning Electron Microscope
SME	Subject Matter Expert
UL	Underwriters Laboratory
XRF	X-Ray Fluorescent

2.2 Definitions

Term	Definition	Reference
Aftermarket Manufacturer (electronics)	<p>A manufacturer that meets one or more of the following criteria:</p> <ol style="list-style-type: none"> 1. A manufacturer authorized by the original component manufacturer (OCM) to produce and sell replacement parts, usually due to an OCM decision to discontinue production of a part. 2. The manufacturer produces parts using semiconductor dice or wafers, manufactured by and traceable to an OCM, that have been stored until use. They are subsequently assembled, tested, and qualified using processes that meet technical specifications without violating the OCM's intellectual property rights (IPR), patents, or copyrights. 3. The manufacturer produces parts through emulation, reverse-engineering, or redesign, which match the OCM's specifications and satisfy customer needs without violating the OCM's IPR, patents, or copyrights. 	SAE AS5553D, <i>Counterfeit Electrical, Electronic and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation and Disposition,</i>
Authorized Distribution (electronics)	Transactions conducted by an OCM-Authorized Distributor distributing product within the terms of an OCM contractual agreement.	SAE AS5553D, <i>Counterfeit Electrical, Electronic and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation and Disposition,</i>
Blacktopping	A term used to describe the intentional covering of the original manufacturer part markings or masking the signs of rework and removal of original part markings.	IDEA-STD-1010-B, <i>Acceptability of Electronic Components Distributed in the Open Market</i>

Term	Definition	Reference
Certificate of Conformance (C of C)	A document signed or otherwise authenticated by an authorized individual certifying the degree to which items or services meet specified requirements.	ASME NQA-1-2008-2009, <i>Quality Assurance Requirements for Nuclear Facility Applications</i>
Certified Material Test Report (CMTR)	A written and signed document approved by a qualified party containing data and information that attests to the actual properties of an item and the actual results of all required tests.	DOE G 414.1-2B, <i>Quality Assurance Program Guide</i>
Checksum	Used to detect errors that may have been introduced during its transmission or storage. Checksums are often used to verify data integrity but are not relied upon to verify data authenticity.	
COA and RC	Command Option Argument (COA) which is downloaded through a Node Package Manager (NPM). Run Configuration (RC) is a configuration loader that is typically downloaded through NPM.	Sharma, A. (2021).
Consensus Standard (in reference to the Fastener Quality Act)	A Consensus standard is a document that describes fastener characteristics published by a consensus standards organization, or a Federal Agency, and does not include a proprietary standard.	PL 106-34, <i>Fastener Quality Amendments Act of 1999</i>
Consensus Standard Organization	Consensus standard organizations include: the American Society for Testing and Materials (ASTM), the American National Standards Institute (ANSI), the American Society of Mechanical Engineers (ASME), the Society of Automotive Engineers (SAE), the International Organization for Standardization (ISO), and any other organization identified as a United States consensus standards organization or a foreign and international consensus standards organization in the Federal Register (reference 61 Fed. Reg. 50582–83).	PL 106-34, <i>Fastener Quality Amendments Act of 1999</i>
Critical Nonconformance	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.	FAR 52.246-26, <i>Reporting Nonconforming Items</i>

Term	Definition	Reference
Data Universal Numbering System (D-U-N-S)	A D-U-N-S number is a unique nine-digit identifier assigned by Dun & Bradstreet which is used to identify and track businesses who enter in bids for Federal Government contracting. Although it is not required to perform work for the U.S. Federal Government, many other Federal Governments and companies do require it.	Dun & Bradstreet ¹
Decapsulation	The process of removing a cap, lid, or encapsulating material from a packaged integrated circuit by mechanical, thermal, or chemical means exposing the integrated circuit for further analysis, inspection, or electrical examination of the die and the internal features.	SAE AS6174A – Counterfeit Material; Assuring Acquisition of Authentic and Conforming Material
Defective	Any item or material that does not meet the commercial standard or procurement requirements as defined in such sources as catalogues, proposals, procurement specifications, design specifications, testing requirements, or contracts may be considered <i>defective</i> .	DOE O 232.2A, Occurrence Reporting and Processing of Operations Information
Die	A small block of semiconducting material on which a given functional circuit is fabricated.	SAE AS6174A– Counterfeit Material; Assuring Acquisition of Authentic and Conforming Material
Electronic Packaging	A major discipline within the field of electronic engineering and includes a wide variety of technologies. It refers to enclosures and protective features built into the product itself and not to shipping containers. It applies to both end products and to components.	SAE AS6174A – Counterfeit Material; Assuring Acquisition of Authentic and Conforming Material
Engineering Evaluation	A technical review conducted by qualified engineering and other technical personnel using accepted methods to determine the actual or potential cause of a substantial safety hazard and the effect of an S/CI.	DOE G 414.1-2B Chg. 2 (Admin Chg.), Quality Assurance Program Guide

¹ Dun & Bradstreet: <https://www.dnb.com/duns/duns-number-and-government.html>

Term	Definition	Reference
Failure Modes and Effects Analysis	Failure Modes and Effects Analysis (FMEA) is a structured risk assessment process and tool used to improve product and process design by assessing, quantifying, and reducing the risks associated with failure.	New Definition
Fastener	A metallic screw, nut, bolt, or stud having internal or external threads and load-indicating washers or washers represented as meeting a consensus standard.	New Definition
Head marking	Markings that are physically applied onto a fastener and may be used to provide traceability to the manufacturer, material/grade, and heat or lot numbers of the fastener. Markings may be required by the referenced material specification, standards, federal legal requirements, or procurement and contractual requirements.	New Definition
High-Strength	A fastener with a minimum tensile strength of 120,000 pounds per square inch (psi) or fasteners considered equivalent to a SAE grade 5 would be considered <i>high- strength</i> .	FQA- Report Committee on Commerce, Science and Transportation S. 795 November 19, 1999, Senate Report 106-224
Independent Distributor (electronics)	A distributor that purchases parts with the intention to sell and redistribute them back into the market. Purchased parts may be obtained from OEMs or Contract Manufacturers (typically from excess inventories), or from other Distributors (Franchised, Authorized, or Independent). Resale of the purchased parts (redistribution) may be to OEMs, Contract Manufacturers, or other Distributors. Independent Distributors do not normally have contractual agreements or obligations with OCMs. See definition of “ Authorized Distribution .”	SAE AS6174A– Counterfeit Material; Assuring Acquisition of Authentic and Conforming Material
Item(s)	An all-inclusive term used in place of appurtenance, assembly, component, equipment, material, module, part, structure, product, software, subassembly, sub-system, system, unit, or support systems.	10 CFR 830, <i>Nuclear Safety Management</i>

Term	Definition	Reference
Major Nonconformance	A nonconformance, other than a critical nonconformance, 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.	FAR 52.246-26, Reporting Nonconforming Items
Manufacturer	A manufacturer is the person or source which fabricates an item for sale in commerce.	New Definition
Nonconformance	A deficiency in characteristic, documentation, or procedure that renders the quality of an item or activity unacceptable or indeterminate.	ASME NQA-1-2008
Open Market (electronics)	The trading market that buys or consigns OEM, Contract Manufacturer, and Aftermarket Manufacturer's excess inventories of new electronic parts and subsequently utilizes these inventories to fulfill supply needs of other OEMs and Contract Manufacturers, sometimes due to urgent or obsolete part demands. Open Market may include the purchase and sale of parts with unknown origin or where the complete chain of custody of such parts is unknown.	SAE AS6174 – Counterfeit Material; Assuring Acquisition of Authentic and Conforming Material, Dated 2012-05
Risk Mitigation	The process of reducing the likelihood or impact of a potential negative event.	New Definition

Term	Definition	Reference
Suspect/Counterfeit Item (S/CI)	<p><u>Counterfeit Items.</u> Items that are intentionally manufactured, refurbished, or altered to imitate original products without authorization in order to be passed off as genuine.</p> <p><u>Fraudulent Items.</u> Items that are intentionally misrepresented with intent to deceive, including items provided with incorrect identification or falsified and/or inaccurate certification. They may also include items sold by entities that have acquired the legal right to manufacture a specified quantity of an item but produce a larger quantity than authorized and sell the excess as legitimate inventory.</p> <p><u>Genuine or Authentic Item.</u> Items that are produced and certified without the intent to deceive.</p> <p><u>Suspect Items.</u> Items where there is an indication or suspicion that they may not be genuine.</p>	DOE O 414.1D, <i>Quality Assurance</i>
Suspect/Counterfeit Items Control Plan	Documents an organization's risk-based strategy for identification, mitigation, disposition, detection, avoidance, reporting, and trending of S/CIs.	New Definition
Textured (electronics)	Plastic Electronic Components are typically made with a mix of fine glass and plastic. The surface of the molded package is textured when it is removed from the mold.	SAE AS6174A – Counterfeit Material; Assuring Acquisition of Authentic and Conforming Material

3 Suspect/Counterfeit Item (S/CI) Risks

Risk management weighs the likelihood that an event will occur against the consequence or impact of the occurrence. Risk assessment and mitigation are often collaborative efforts among multiple organizations and roles.

Performing an assessment for the risks of receiving S/CIs will also weigh consequence or impact against the likelihood of occurrence. This may include how critical the item is to environment, safety, health, security, mission success, and/or strategic value, etc. against the likelihood that the item will be received as S/CI. Information to aid in determining the likelihood of an item being received as S/CI may be obtained from internal DOE resources or external sources where S/CIs have been reported. Some items are more likely to be S/CI since they have been historically and continue to be targeted by counterfeiters. These include obsolete components, difficult to procure items, items where lead times are critical, items where multiple versions are available, items where there is a high volume but low price or vice versa, common commercial items, items of strategic value, etc.

After performing a risk analysis on items, risks may be identified as low, moderate, or high. “Low Risk” (green) are items that carry a lower associated risk/hazards to the organization whereas “Moderate” (yellow) and “High” (red) risk will carry higher associated risks to an organization. Organizations may rate some items as higher risk than what is used in the example chart depending on how items are used. Risk mitigations may be employed using a risk-based approach as provided in the example in Table 1, *Risk Mitigation Table*. It should also be noted that the example provided in Table 2, *Counterfeit Risk Based Approach Example Table* does not provide a comprehensive list of items that may be used or procured as any item that can be made can be counterfeited.

In order to address risk, tolerance, and mitigations, an S/CI Control Plan or similar process or procedure may be developed. The S/CI Control Plan documents the organization’s risk-based strategy for identification, mitigation, disposition, detection, avoidance, reporting, and trending of S/CIs.

S/CI Control Plans may address the following processes:

- Roles and Responsibilities;
- Risk Assessment;
- Risk Assessment Process;
- Graded Approach Process;
- Flow Down/Procurement Clauses;
- Personnel Training;
- Obsolescence Management;
- Nonconformance Program Coordination (include S/CI, Trend for potential issues, etc.);
- Control of External Sources/Suppliers;
- Traceability;
- Material and Parts Control;

- Verification of Purchased/Returned Items;
- Inspections and Tests;
- Investigations;
- Handling, Segregation, and Marking;
- Reporting;
- Monitoring and Trending Activities; and/or
- Internal/External Audits and Assessments.
- Commercial Grade Dedication

Functional areas (Roles) that may be involved S/CI processes include but are not limited to:

- Quality Assurance & Control (Inspection);
- Logistics/Shipping/Receiving (Inspection);
- Assessment Personnel;
- Program/Project Management;
- Procurement/Supplier Management;
- Facilities/Stock/Assembly/Maintenance Personnel;
- Engineering;
- Materials Management & Logistics;
- Environment, Safety & Health (ES&H); and
- Security.

Table 2, *Counterfeit Risk Based Approach Example Table* provides an example of a graded approach and risk assessment process. Items may be graded differently by organizations depending on how items will be used. For instance, containers or packaging materials used in a critical application may have a higher impact to operations which may move that item higher in the chart. Examples are variable and are highly dependent on the organizations specific risk profile such as how vulnerable an organization may be to certain risks (e.g., use of uncontrolled supply bases, purchase of obsolete components, purchase from oversea suppliers, etc.) and risk tolerance such as what amount of risk is acceptable or not acceptable.

When developing a chart similar to Table 2, the plan should capture how each risk grade level will be mitigated. Risk mitigation is the action taken to reduce threats and ensure resiliency. When mitigating risks, steps are taken to reduce adverse effects. It is important to remember that mitigating risk is not just about fixing vulnerabilities—it's also about reducing the impact of any potential threats. When developing a mitigation strategy, it is important to consider how an organization may react to an event or occurrence as well as how you can prevent negative events or occurrences in the future.

When mitigating risk, it is crucial to develop a strategy that closely relates to and matches the organization's profile. A proper mitigation strategy will define how risks are managed. There are five main risk mitigation strategies that are commonly used which include: risk acceptance, avoidance, reduction, transference, and sharing.

1. **Risk acceptance** does not reduce any of the effects of the risk. This strategy is common when the cost of the risk itself outweighs any benefits of mitigating the risk. An organization with a low risk profile and that typically doesn't want to spend a lot of money on avoiding risks might use the risk acceptance strategy. It is important to remember that having a reporting process for S/CIs but not employing processes to prevent or detect S/CIs would be considered "accepting a risk." It is important to note that in many cases S/CIs are still reportable if identified, even by happenstance.
2. **Risk avoidance** is the opposite of risk acceptance. It is the action that avoids any exposure to the risk whatsoever. It's important to note that risk avoidance is usually the most expensive of all risk mitigation options.
3. **Risk reduction** is the most common risk management strategy employed. This strategy reduces exposure by taking actions to prevent or detect the risk.
4. **Risk transference** is handing over risk to a willing third party. This is often completed by means of a contract.
5. **Risk sharing** occurs when responsibility for risks assumed by one organization can be shared with another. Although this method may not eliminate the risk. It may reduce the risk to an acceptable level. Organizations with different risk tolerance levels may be able to use risk sharing to align responsibility for different types of risk with commensurate risk tolerance levels, and to assign responsibility for specific types of risk to organizations with the appropriate expertise or resources to address them.

Reference Table 1, *Risk Mitigation Table* for an example of when each mitigation strategy might be used:

		Likelihood		
Impact		Low Likelihood	Moderate Likelihood	High Likelihood
	Low Impact	Accept	Reduce	Reduce
	Moderate Impact	Reduce	Reduce	Transfer, Share, Reduce
	High Impact	Transfer, Share, Reduce	Transfer, Share, Reduce	Transfer, Share, Reduce, Avoid

Table 1: Risk Mitigation Table

1. Risk is identified as *Low to Moderate Likelihood and Low Impact (Accept/Reduce Strategy)*:
 - a. Risk Mitigation Plan – Mitigations may be informal.
 - b. Procurement Contracts – Recommended use of Suspect/Counterfeit Items contracting clause.
 - c. Procurement Cards (P-Cards) – These items may be procured using this method. It is important to note that contracting clauses are not typically used.

- d. Inspection and Tests – Informal or formal processes may be used.
- 2. Risk is identified as *High Likelihood and Low Impact (Reduce Strategy)*:
 - a. Risk Mitigation Plan – Mitigations may be informal.
 - b. Procurement Contracts – Recommended use of Suspect/Counterfeit Items contracting clause.
 - c. P-Cards – These items may be procured on P-Cards but should be procured using caution. For instance, organizations should use reputable and well-established suppliers that have a history of supplying quality products and use industry-accepted consensus standards (e.g., ISO, SAE, ASME, ASTM, etc.)
 - d. Inspection and Tests – Informal or formal processes may be used.
- 3. Risk is identified as *Low to Moderate Likelihood and Moderate Impact (Accept/Reduce Strategy)*:
 - a. Risk Mitigation Plan – Recommend formalized processes and procedures that address minimum requirements for projects that are procuring items in this risk category such as Roles and Responsibilities, Graded Approach (Risk Categorization process), Procurement, Reporting, handling of S/CIs if found, and evaluation/disposition process.
 - b. Procurement Contracts – Use of Suspect/Counterfeit Items clauses.
 - c. P-Cards – These items may be procured on P-Cards but should be procured using caution. For instance, using reputable and well-established suppliers that have a history of supplying quality products and use industry-accepted consensus standards (e.g., ISO, SAE, ASME, ASTM, etc.) mitigates some of the risk of receiving S/CIs.
 - d. Inspection and Tests – more formalized processes may be used.
- 4. Risk is identified as *Moderate to High Likelihood and High Impact (Transfer, Share, Reduce, and Avoid Strategy)*:
 - a. Risk Mitigation Plan – Recommend formalized processes and procedures that address minimum requirements for projects that are procuring items in this risk category such as Roles and Responsibilities, Graded Approach (Risk Categorization process), Procurement, Reporting, handling of S/CIs if found, and evaluation/disposition process.
 - b. Procurement Contracts – Use of Suspect/Counterfeit Items clauses.
 - c. P-Cards – These items may be procured on P-Cards but should be procured using caution. Again, using reputable and well-established suppliers that have a history of supplying quality products and use industry-accepted consensus standards (e.g., ISO, SAE, ASME, ASTM, etc.) mitigates some of the risk of receiving S/CIs.
 - d. Inspection and Tests – more formalized processes should be used.

NOTE: Although informal processes may be used for inspections of low to moderate risk type of items or services, individuals should be familiar with how their local organization reports S/CIs when or if they are identified.

	Low Likelihood		Moderate Likelihood		High Likelihood	
	Furniture	Lawn and Garden supplies	Custom Order Products <i>non-critical applications</i>	Fabricated Items	Food e.g., fish, poultry, etc.	Housewares e.g., light fixtures, cups, plates, etc.
	Containers, Packaging and Packaging Materials	Appliances	General Use Fasteners	Hand-Tools	Sporting Goods e.g., golf, sports gear, etc.	General Office Supplies e.g., printer ink cartridges
Moderate Impact	Metallic Materials e.g., bar stock, plate, forged materials, etc.	Documentation	Transportation e.g., ratchet tie down	Welding Materials	Bearings	Electronic Components
	Books and Instruction Manuals	Non-metallic crude materials	Automotive Components and Accessories	Batteries	Fire Control Equipment	Instrumentation, Laboratory Equipment, and Measuring Tools i.e., critical applications.
High Impact	Power Distribution Equipment	Aircraft and Aircraft related components or accessories	Construction Equipment	Networking, Computing and Telecommunications e.g., mouse, keyboard, monitors, webcams, etc.	Hoist, Lifting, and Rigging Equipment	Personal Protective Equipment (PPE)- e.g., hardhats, fall safety, bullet proof vests, etc.
	Chemicals, Lubricants, and Adhesives	Electrical Equipment and Electrical Safety Equipment e.g., breakers, relays, inverters, bus transfers, generators, fuses	Weapons, Weapons Components, and Weapons Accessories	High-Strength Fasteners i.e., critical applications	Pressure Safety Equipment e.g., valves, pipe, pumps, compressors, and accessories	Obsolete or End of Life Items in critical applications

Table 2: Counterfeit Risk Based Approach Example Table

4 S/CI General Process

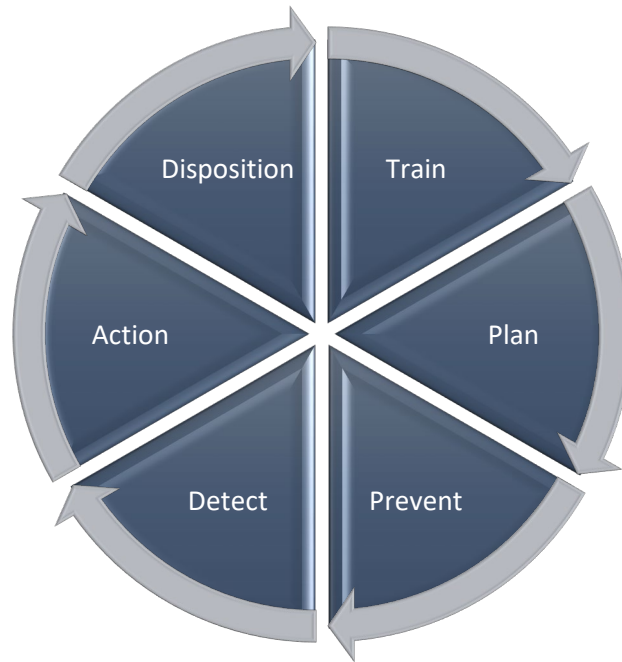


Figure 1: Model of an S/CI Program General Process Flow

Above is a model of an S/CI Program General Process Flow. The following sections describe an approach to how each process might be implemented. Note that every organization may have a different approach or methodology for implementation. This could include additional processes or steps.

4.1 Train Personnel on S/CI

Organizations should provide general training on S/CI to personnel who may come in contact with products, services, or software that may be S/CI. An online course is available in Learning Nucleus to all DOE Federal, contractor, and subcontractor employees as well as suppliers that support DOE: Suspect, Counterfeit, Defective, and Fraudulent Items Awareness (SCD-100DE) which is available at this link <https://learningnucleus.energy.gov/>. Registration is required to access Learning Nucleus. Information on registration can be obtained by emailing counterfeit@hq.doe.gov.

4.2 Planning

Up front planning can prevent S/CI, including S/CI software. Planning may include analysis of project or program needs including an in-depth planning stage. The Planning stage will typically use a defined graded approach and should consider the following:

- 1) What major procurements will be conducted during the project?
- 2) Will critical items be procured?
- 3) What steps, if any, should be included to reduce potential risks of suspect/counterfeit items?
- 4) Are there repeat purchases? How are these suppliers managed or given feedback if there are issues?

A key component of planning is to understand the risks and their controls. The integrity of systems and

information is a critical component of managing supply chain and cybersecurity risks.

4.3 Prevention

The responsibility for preventing S/CI from entering a DOE facility starts in areas such as project planning, design, and procurement. Actions may involve reviewing supplier quality assurance processes, training, and using screening resources such as the Government-Industry Data Exchange Program (GIDEP). The following sections discuss steps DOE personnel can follow to prevent S/CI. Note that procurement refers to the procurement of items, services, and special processes, all of which may have the potential to introduce S/CI into a system depending on the scope of work.

4.3.1 Prevention and Procurement

Prior to procurement, processes such as project planning or design processes should consider the bill of materials, how items will be used, criticality of items and their associated risks, tests that may be needed, and customer-defined specifications. It is vital at the procurement step that requirements are well understood and communicated to suppliers and that contracts properly document requirements. This is especially true when procuring items that will be used in a more critical capacity.

The procurement process generally starts with acquisition planning, which establishes the requirements for items including determining if any special procurement requirements exist. Many organizations will have a formalized procurement request process to standardize acquisition planning. This could include adding or choosing terms and conditions to be used in the contract. Individuals requesting procurements, should be familiar with local contract clauses. The enforcement of the terms and conditions by cognizant organization and procurement officials is necessary so that contractual requirements are not left out due to costs, schedule, and/or production pressures.

The following practices should be used during the procurement process to prevent S/CI. Purchasers should:

- Ensure that the suppliers have demonstrated their capability to deliver acceptable items in a timely manner;
- Ensure controls and verification activities are commensurate with the identified risks;
- Verify individuals performing S/CI prevention processes have received S/CI training;
- Verify requirements are included in the contract documents for any necessary technical and QA reviews of the supplier;
- Ensure quality specifications included in contracts are accurate, address the requirements, and provide sufficient information to the supplier; and
- Verify that approved QA and S/CI clauses are included in contracts.

A key element of the procurement process is the specification requirement, including technical and quality assurance requirements, and should be developed by the relevant Subject Matter Expert (SME). A graded approach may be applied based on the likelihood an item will be S/CI along with other factors such as specific application and the potential impact that failure of the item could have on the health and safety of the public, environment, and workers. The procurement package should describe specific quality controls

and verification methods, such as a QA audit and/or supplier source surveillance, receipt inspection, and post-installation inspection and test.

Determine during the procurement or procurement planning process if the organization will:

- 1) Evaluate the supplier's QA program using a graded approach;
- 2) Perform Inspection/Testing;
- 3) Perform Failure Modes and Effects Analysis (FMEA); or
- 4) Perform Commercial Grade Dedication (CGD) using in whole or in parts (depending on nuclear facility applicability) an established process such as the process stated in American Society of Mechanical Engineers (ASME) Nuclear Quality Assurance (NQA)-1. CGD is used for items that are deemed safety-significant or mission critical but where supplier evaluations may not be possible.

Unless the supplier's quality system for generating the documentation and maintaining part number configuration control was previously verified through performance-based evaluations, DOE and its contractors should be cautious about accepting items based solely on supplier-generated documentation or part-number verification.

4.3.2 Prevention and Supplier Quality Assurance

Evaluate the supplier QA program to verify the supplier or distributor has the capability to comply with purchase order requirements. Assessments should include some of the following S/CI prevention questions:

- 1) How are S/CIs prevented or detected at the supplier's facility? Does the supplier have documented processes or procedures?
- 2) How does the supplier perform testing, inspection, or verification of items to ensure they are genuine?
- 3) Is item traceability maintained (if applicable) at the facility? How is it maintained?
- 4) How are nonconforming items or materials and S/CIs segregated from conforming products?
- 5) Who is trained on S/CI prevention and detection? How are they trained?
- 6) How does the supplier manage customer-returned product? How do they ensure that it is not S/CI or nonconforming? How do they ensure these types of products do not re-enter the supply chain?
- 7) Would the supplier report S/CIs if identified? Where would they report them?
- 8) Does the supplier screen inventory for the presence of S/CI?
- 9) Does the supplier evaluate their sub-tier suppliers and distributors for S/CI prevention and detection controls?

To control entry of S/CIs through the procurement process, contractor QA programs should implement procedures for:

- Controlling procurement processes;
- Developing specification/requirements and receipt inspection plans;
- Approving QA and S/CI clauses;

- Reviewing technical and quality requirements;
- Reviewing contracts for legal interpretations of contract terms and conditions;
- Rating supplier past performance;
- Maintaining approved supplier lists;
- Performing source or receipt inspection (e.g., per pre-defined receipt inspection plan), surveillance, and performance-based audits;
- Validating product acceptability, including performing verifying, inspecting, and testing activities; and
- Using supplier quality information-sharing processes.

4.3.3 Prevention and Suppliers

Organizations should evaluate suppliers to prevent the introduction of S/CI. Evaluated suppliers may be called “*Approved Suppliers*” or added to an “*Approved Supplier List*.” Organizations may use other indicators than an *Approved Supplier List* to help those who are performing procurements to know which suppliers are acceptable to use. *Approved suppliers* should be used when procuring items where S/CI risks have been found to carry a high likelihood and impact to the organization.

Supplier approval may be achieved by:

- **Desk Assessment** – A desk assessment may be conducted through a survey, questionnaire, or remote review of the supplier’s information. This may be performing verification on a third-party certification that the supplier meets an internationally recognized consensus standard such as International Organization for Standardization (ISO), American Society of Mechanical Engineers (ASME), American Society for Testing Materials (ASTM), etc.
- **On-site Assessment** – An on-site assessment would typically include a performance-based audit, surveillance, or other assessment to a specified criteria such as an internationally recognized consensus standard. The assessment would be performed in-person at the supplier’s facility and would review processes and procedures along with their implementation.
- **Shared Assessments** – Organizations may decide to use assessments performed by other organizations internal or external to DOE, thereby reducing efforts, creating efficiencies, and saving government funds. This also reduces efforts by suppliers and manufacturers who support multiple assessments for similar organizational needs. Resources that may aid in gathering data for sharing assessment information include but are not limited to the DOE Consolidated Audit Program (DOECAP), Master Supplier List (MSL), GIDEP, Electronic Resellers Association International (ERAI), International Aerospace Quality Group (IAQG), Online Aerospace Supplier Information System (OASIS), ISO, and the Energy Facility Contractors Group (EFCOG).

4.3.4 Prevention and use of Contract Clauses

All contracts should contain some type of S/CI clause prohibiting the delivery of S/CIs. Clauses should include definitions of S/CI and any other applicable contractual requirements that may be unique or required for the procurement (e.g., Federal Acquisition Requirements, specifications, customer requirements, etc.). Local General Counsel or Contract Legal department should review clauses for any organization-specific requirements or terms that may be added.

The following example can be modified for an organization's use:

Notwithstanding any other provisions of this agreement, the Subcontractor warrants that all items provided to the Contractor should be genuine, new, and unused unless otherwise specified in writing by the Contractor. Subcontractor further warrants that all items used by the Subcontractor during the performance of work at the [name DOE location/site here], include all genuine, original, and new components, or are otherwise suitable for the intended purpose. The Subcontractor's warranty also extends to labels and/or trademarks or logos affixed, or designed to be affixed, to items supplied or delivered to the Contractor. Furthermore, the Subcontractor should indemnify the Contractor, its agents, and third parties for any monetary loss, injury, or property damage resulting directly or indirectly from material, components, or parts that are not genuine, original, and unused, or not otherwise suitable for the intended purpose. This includes, but is not limited to, materials that are defective, suspect, or counterfeit; materials that have been provided under false pretenses; and materials or items that are materially altered, damaged, deteriorated, degraded, or result in product failure.

In addition to the requirements above, the subcontractor must:

- 1) Purchase directly from product manufacturers or authorized manufacturer distributors whenever possible.*
- 2) Use counterfeit prevention and/or quality assurance procedures, which include an S/CI detection program.*
- 3) Immediately notify [name DOE location/site here] if subcontractor suspects or becomes aware of used or counterfeit goods having been furnished during the performance of work on this contract.*
- 4) Report suspected fraud, waste, or abuse by a DOE employee, Subcontractor, or grant recipient involving DOE programs to the Office of Inspector General by phone (800) 541-1625, or by email ighotline@hq.doe.gov. Additional information is available at: <http://energy.gov/ig/office-inspector-general>.*

Contractors may also include a statement that notifies subcontractors of the intent to hold items identified as S/CI and not ship them back.

Types of material, parts, and components known to have been misrepresented include (but are not limited to): fasteners; hoisting, rigging, and lifting equipment; personal protective equipment (PPE); cranes; hoists; valves; pipe and fittings; electrical equipment and devices; plate, bar, shapes, channel members, and other heat-treated materials and structural items; welding rod and electrodes; electronic components; chemicals, lubricants, and adhesives; power distribution equipment; construction equipment; bearings; fire control equipment; calibrated instrumentation and measuring tools; telecommunications and networking devices, and computer memory modules. In addition, because falsification of information or documentation may constitute criminal conduct, the Contractor may reject and retain such information or items, at no cost, and identify, segregate, and report such information or activities to cognizant Department of Energy officials.

Failure of a supplier to meet a quality clause like the one above should be reported by the contractor in accordance with the contractor's S/CI process which, at a minimum, should include notifications and

reporting as described in section 4.5, *Action: Notification and Reporting of S/CI* below.

Many S/CI items discovered by DOE/National Nuclear Security Administration (NNSA) were procured with credit cards. Under many procurement systems, the use of credit cards offers the potential for bypassing procurement controls. The use of a credit card in no way relieves the credit card holder from prohibitions, controls, or other required authorizations for the acquisition of goods and services. Care should be taken to assure appropriate application of procurement controls to mitigate the risk of S/CIs including use of reputable suppliers (i.e., assessed suppliers), flow-down of specification requirements, appropriate technical and quality requirements, and other procurement controls necessary to preclude entry of S/CIs into the DOE supply chain.

In addition to the clause language above, many DOE contractors are now required to address the requirements in FAR 52.246-26, *Reporting Nonconforming Items*. This requires that certain subcontracts flow down requirements for reporting critical and major nonconformances and S/CIs into GIDEP. Numerous exclusions to the insertion of this clause avoid burdening small businesses, so much of the burden for reporting is on the DOE Prime Contractor.

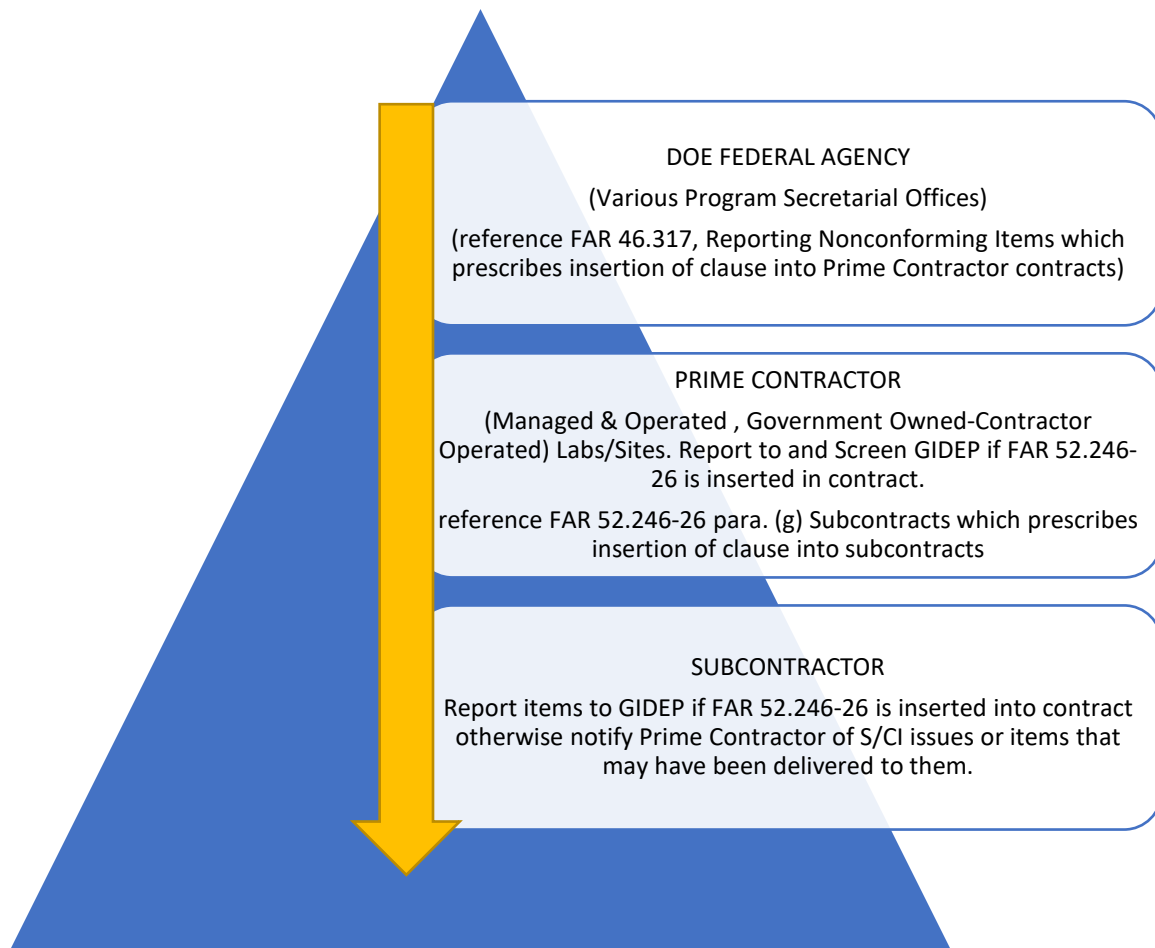


Figure 2: FAR 52.246-26 Reporting Structure at DOE

A general statement such as the following may be included in contracts to address GIDEP reporting:

Items discovered as Suspect/Counterfeit or Nonconforming may be reported to the Government-Industry Data Exchange Program (GIDEP) by [enter DOE site/location name here] in accordance with requirements stated in FAR 52.246-26, Reporting Nonconforming Items. It is important that contact information is up to date for the contractor/subcontractor site so that any communications regarding potential GIDEP submittals can be reviewed by the contractor/subcontractor company prior to submission and any responses may be appended to the report. If, for any reason, [DOE site] does not receive a response, we will submit the report 15 days from the original date on which we submitted the report to the contractor/subcontractor to review.

DOE Prime Contractors should be familiar with the FAR 52.246-26 requirements and collaborate closely with their DOE Federal Contracting Officers Representatives for questions on implementation, clause flow-down, and reporting into GIDEP.

4.3.5 Resolution on Disputes

Since organizations should not return items identified as S/CI or Fraudulent, contract clauses must clearly identify to suppliers that items will not be returned, and that the supplier may be liable for costs related to the item's replacement. This will aid in the recovery of funds for items purchased on contracts. If items are purchased on P-Card and cannot be returned to suppliers, an organization may be able to dispute the charges to recover lost funds on orders:

- 1) Involve the local P-Card office as early in the process as possible. If all reporting processes have been completed and there is not an open or pending investigation (i.e., the item has been released for disposition), the organization may be able to contact the merchant directly.
- 2) Typically, for the merchant to be able to process a reversal of charges, no more than 60-90 days may have passed since the item was billed to the card. However, this time period may have passed during the inspections and investigations of the item.
- 3) Prior to reporting, items are typically stated as *defective* or *nonconforming* rather than *S/CI*. The organization could provide proof of the defect or nonconformance such as labeling discrepancies or other information obtained during inspections.
- 4) If the merchant will not return funds because too much time has passed or the merchant does not believe there is sufficient information, work directly with the Procurement Card Office and credit card company to dispute the charges and obtain a refund.

Note that even after following all the above processes, the organization may still be unable to recover the funds.

4.4 Detection

After completion of the procurement process, it is likely that items will go through processes such as receipt and inspection. During these processes, items/services may be found to be nonconforming and may be further identified as suspect/counterfeit.

To eliminate the risk of S/CIs being reintroduced into the supply chain, items identified as being S/CI should ***not*** be returned to the supplier. If a suspect item is found to be acceptable (through engineering evaluation, verification testing, or the disposition process), the item may be installed or used.

It is vital that individuals who handle products or services are familiar with, and receive training on, potential indications of S/CI and how to report these types of items. Nonconformance reporting processes may be used to control items identified as S/CI to prevent the inadvertent installation or use and to complete additional requirements such as reporting into the Occurrence Reporting Processing System (ORPS). Nonconformance Reports (NCRs) should be reviewed by an S/CI subject matter expert (SME) or S/CI Coordinator in a timely manner to make a technical determination that the item is S/CI. At a minimum, an S/CI Coordinator should consider:

- Does the item meet the contract criteria?
- Were S/CI requirements flowed down to the supplier in the contract?
- Were there any past performance issues with the supplier (i.e., similar suspect or nonconforming issues)?
- Does the item have S/CI indications as noted in this handbook?
- Were costs impacted in a way that appears the supplier gained monetary funds from using substandard or low-quality materials?

S/CI processes and programs that fail to prevent an S/CI from being delivered to a DOE facility are key areas for focus to prevent such occurrences.

Other processes for managing S/CIs may be used outside of the nonconformance process, but if used, they should address the following:

- Records the critical information of the item identified (e.g., part number, description, supplier/manufacturer, and D-U-N-S as applicable);
- Marking, tagging, and segregating;
- Actions taken and by whom (e.g., who reported the item? who is capturing the information? who is dispositioning it?);
- Disposition and reporting conducted (e.g., was the item destroyed, used as is? where was the item reported? objective evidence that the item was released by the Office of Inspector General (OIG); and
- Trending and continuous improvement metrics.

4.4.1 Detection and Inspections

Acceptance is the process of ensuring that items meet requirements and specifications and that they will be usable for their intended purpose. Acceptance may include all or some of the following steps:

- Source Inspections: Acceptance inspections may take place at the supplier's or purchaser's facility. It could include dimensional inspections, surveillance of testing, and ensuring "on-site stores and inventories" are evaluated to detect the presence of S/CIs, including electronic components and integrated circuits.

- Testing: Acceptance may be achieved by performing specialized testing that is conducted in-house or by a third-party laboratory.
- Receipt Inspections: Organization may use a defined graded approach to inspect items. Low-risk procurements (e.g., textbooks, batteries, phone chargers, etc.) may not have formal acceptance criteria but these items may still undergo a basic or more informal inspection for S/CI characteristics (e.g., labeling, packaging, missing or incorrect owner's manual, color variations, etc.). Whoever is performing inspections should be familiar with how to report S/CIs, even if identified in low-risk items.

Item/part number verification and review of certification documentation (e.g., Certified Material Test Reports-CMTRs, Certificate of Conformance-C of C) alone are *not* sufficient to verify the quality of a purchased item. Item specifications and QA criteria should be specified and verified. Consideration should be given to the following:

- History of S/CI concerns with the item and/or supplier;
- Intended safety function of the item;
- Attributes required to perform the function;
- Processes that encompass/embrace these attributes;
- Supplier past performance information;
- Source inspection, surveillance, assessments, or QA audit results;
- Receipt inspection and acceptance testing results;
- Special test and examination methods (e.g., chemical analysis, hardness, and tensile testing); and
- Post-installation testing.

Sampling:

Large lots of received items may be sampled using criteria such as American National Standards Institute (ANSI)/American Society for Quality Control (ASQC) Z1.4, *Sampling Procedures and Tables for Inspection by Attributes*. If S/CIs are discovered during inspection or sampling, the nonconforming lot should be controlled and dispositioned in accordance with local procedures. Note that if one component of an item (e.g., a ratchet strap bolt) is suspect/counterfeit, the entire item (e.g., the ratchet strap in its entirety) should be considered S/CI.

Personnel Performing Inspections:

Personnel trained to recognize S/CI should inspect items.

Documentation:

If a product is an S/CI, it should be documented in accordance with applicable procedures during the inspection process.

Verification testing may be conducted on a sampling basis, either at the purchaser's facility or a qualified independent test laboratory.

Commercial Grade Items in Safety Systems:

When the design specifies the use of commercial-grade items in safety systems, ensure that the item will perform the intended function and will meet design requirements applicable to the replaced item and its application. The purchaser's acceptance process should provide sufficient confidence that the items meet specified requirements and should include inspections, tests, or analysis by the purchaser, or third-party dedicating entity, supplemented after delivery as necessary by one of the following:

- Commercial grade surveys;
- Product inspections or witnesses at hold points at the manufacturer's facility;
- Analysis of historical records for acceptable performance; or
- Receipt of acceptable documentation, as applicable to the item.

Additional guidance for verifying the acceptability of commercial grade items in safety applications may be found in ASME NQA-1 and Electric Power Research Institute (EPRI) NP-5652, *Guideline for the Acceptance of Commercial Grade Items in Nuclear Safety-Related Applications*.

4.4.2 Detection and Engineering Involvement

An important objective of engineering involvement is to prevent or mitigate potential risks to the public and worker safety attributable to S/CIs. Engineering should be involved in support of procurement, product inspection and acceptance testing, maintenance, and the nonconformance dispositioning process. The extent of engineering involvement should be commensurate with the risk and intended application of the item (i.e., graded approach).

Engineering functions may include but are not limited to:

- Participating in S/CI training;
- Developing technical and procurement specifications to preclude the introduction of S/CIs;
- Determining critical characteristics of purchased items that should be specified in the purchase order and selecting those characteristics to be verified during receipt inspection or prior to use;
- Determining verification activities such as inspections tests and methods of acceptance. The extent of verification may be based on risk (impact/likelihood of counterfeit), supplier past performance, sample size, dollar value, and other organizational factors.
- Evaluating acceptance test results and dispositioning S/CIs;
- Reviewing technical changes to, and deviations from, procurement documents;
- Developing methods for maintenance and inspection personnel to use;
- Participating in supplier qualification processes, audits, surveillances, and source inspections; and
- Maintaining, modifying, or justifying the replacement of equipment involving design changes. Guidelines on engineering evaluation to justify equipment replacement are provided in EPRI NP-6406, *Guidelines for the Technical Evaluation of Replacement Items in Nuclear Power Plants*.

4.4.3 Detection and Evaluations

If S/CIs are detected prior to being installed, S/CIs should be withheld from installation or use pending the evaluation. It is possible that during routine maintenance or during other inspection processes that an item that is already in use or installed is identified as S/CI. The next sections discuss the evaluation processes for items that are installed including safety and non-safety related systems.

4.4.3.1 *Evaluation: Installed Items Determined to be S/CI*

Evaluations should be conducted to determine whether a system can be operated in its present configuration without modification or replacement of the S/CI, or whether the system should be locked out, tagged out, and/or removed from service. Typically, these evaluations are conducted by engineers or SMEs of these systems. Evaluation results should be documented and specify any conditional use of the system and any compensatory actions that will ensure the least possible threat to public and worker safety. Results should be communicated to the field office in accordance with local procedures.

Contractors should ensure that S/CIs are dispositioned either to remain in place (if an engineering evaluation justifies it) or are scheduled to be removed. If an S/CI is to be replaced at a later date, this date should be specified in the documented engineering evaluation and added to maintenance schedules. Installed S/CIs that can be removed from their current applications should be marked/tagged and controlled to preclude their reuse.

If an engineering evaluation determines that an S/CI does not pose a potential safety risk and if the item can remain in place, then it should be distinctly identified or controlled by suitable means in accordance with:

- Local procedures;
- Affected design media updated to reflect the field condition, in order to prevent issuance of an additional nonconformance report; and
- Performance of a duplicate engineering evaluation.

NOTE: In areas where operating temperatures are 500° F and above or are subject to cyclic loading where fatigue failure is likely to occur, Grades 8 and 8.2 suspect/counterfeit fasteners should not be allowed to remain in place and should be replaced prior to further use of the equipment. There may be specific instances where engineering evaluation may determine it is necessary to leave items in-place for a defined period of time. Additional information on fastener and other material properties and inspection and testing criteria is provided in applicable American Society of Testing Materials (ASTM) and Society of Automotive Engineers (SAE) standards.

4.4.3.2 *Evaluation: Safety Systems*

DOE O 414.1 (current) requires that contractor's quality assurance program or quality management system to be developed and implemented for all work commensurate with facility/activity hazards and mission impact. Contractors should establish and maintain current lists of safety systems and those facilities/activities affecting the DOE or DOE/NNSA mission. Such lists provide a basis for establishing priorities, conducting inspections, and identifying and dispositioning S/CIs discovered in use. S/CIs discovered after installation or use should be documented under local processes, appropriately

dispositioned, and reported into ORPS. Additional reporting may also be required into GIDEP. Reporting is discussed further in the *Notification and Reporting of S/Cis* section.

If S/CI are discovered in a safety system or mission-critical facility, qualified technical personnel should immediately conduct an engineering evaluation using recognized methods and local procedures to determine:

- Where and how the S/CI is used in a safety system or mission-critical facility, its potentially adverse effect on safety, and its proposed disposition;
- Whether the system should be removed from service immediately, locked out, and tagged out until the S/CI has been replaced with an acceptable item;
- Whether the system can be used, with limitations on operation, until the item can be replaced; and
- How to mitigate potential hazards to workers during S/CI removal.

If an engineering evaluation determines that an S/CI does not pose a potential safety hazard, the item may remain in place, provided it is properly identified or controlled by other suitable means, according to local procedures. When it is removed, the item should be identified, marked, and controlled to prevent its reuse in an application where it may not be suitable. Sampling inspection and special inspection techniques, (e.g., portable testing equipment) may be used to locate and evaluate S/CIs installed in safety systems and mission-critical facilities.

4.4.3.3 *Evaluation: Non-Safety Systems*

S/CI discovered in non-safety systems should prompt inspection of comparable items in safety systems, such as an extent of condition review. S/CI discovered in non-safety system applications should be technically evaluated to determine if it could create personnel safety hazards and be treated in accordance with the contractors approved S/CI process. Items discovered in non-safety systems may take a less formal approach to evaluate, but actions should still be taken to aid in recurrent issues.

4.5 Action: Notification and Reporting of S/CI

Items identified as S/CI should be documented, reported, and controlled (e.g., marked, tagged, and/or segregated) in accordance with the requirements specified in DOE O 414.1 (current) and FAR 52.246-26. Please refer to the requirement for the most up-to-date information on meeting established timelines that may be stated below or other information.

The following reporting steps may be used, although some organizations may find that steps may be done concurrently, in a different order, or may include additional steps to meet organizational level requirements:

- 1) Suspect/Counterfeit Item is identified by organization.

NOTE 1: Before proceeding to the next steps, sites should use their internal procedures for addressing S/CI. Local organizational processes typically involve a designated S/CI coordinator who manages the process and the various reporting steps.

NOTE 2: This step should also include any reporting between the DOE contractor and DOE

Contracting Officer (Federal), which is required to be conducted within 60-days according to FAR 52.246-26.

- 2) Report item to the Office of Inspector General (email counterfeit@hq.doe.gov for S/CI reports) Go to the OIG Hotline form² anonymous reporting.

NOTE 2: The OIG may not respond within the 60-day GIDEP reporting time period required by FAR 52.246-26. Items should be considered “under investigation” per the exclusion listed in this FAR until a release is given to the reporting organization by the OIG or cognizant official. For questions, please contact counterfeit@hq.doe.gov prior to reporting to GIDEP in step 3 as noted below.

- 3) Determine other required reporting paths as noted below. Note that Step 3 can be done concurrently or in any order the reporting organization chooses:
 - 3a. Does S/CI meet criteria in DOE O 232.2A, Occurrence Reporting and Processing of Operations Information? If yes, report to ORPS and continue to next question. If no, continue to next question.
 - 3b. Does S/CI meet criteria in DOE O 210.2A, DOE Corporate Operating Experience Program? If yes, report to DOE OPEXShare and continue to next question. If no, continue to next question.
 - 3c. Does S/CI meet the criteria in Federal Acquisition Requirement (FAR) 52.246-26, Reporting Nonconforming Items? If yes, report to GIDEP. If no, continue to step 4.
- 4) End process.

² OIG Hotline Form is at <https://www.energy.gov/ig/office-inspector-general>.

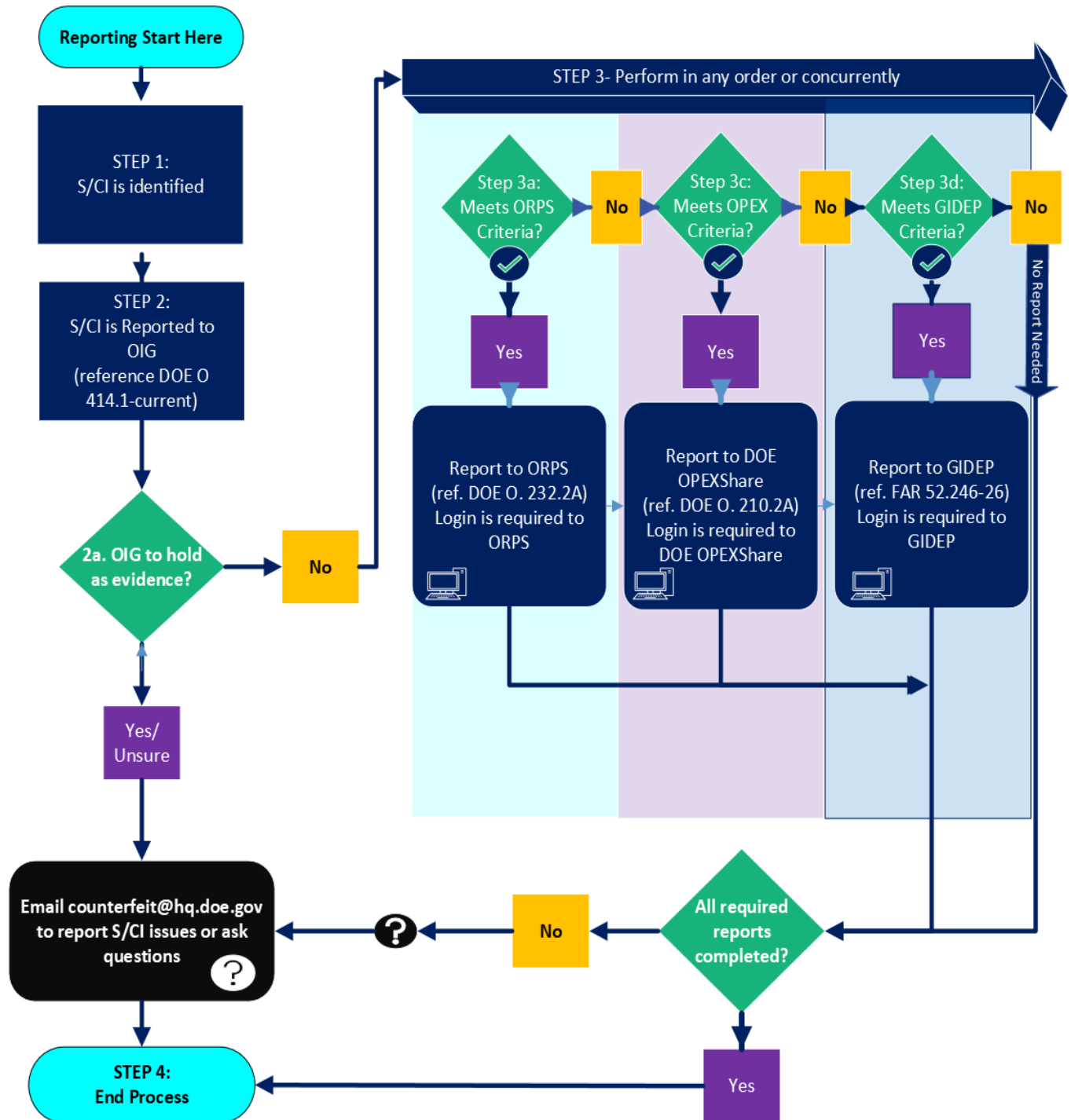


Figure 3: Suspect/Counterfeit Item Example Reporting Chart

4.6 Disposition of S/CI

Known S/CIs should be removed as soon as possible when an engineering evaluation has determined that the S/CI could create a safety hazard. S/CIs may be destroyed, provided that the:

- Item cannot be traced to a supplier, manufacturer, or distributor;
- Item is not required as material evidence by the local OIG for litigation; and/or
- Local OIG has authorized disposition of the item by the reporting organization; or
- Item has been in the reporting organization's possession for more than 10 years; no investigation or litigation has been needed on the item in that time period, and the item is not needed for training purposes (e.g., the item may be disposed of due to statute of limitations).

NOTE: Items that will be used for training purposes must clearly indicate through marking or tagging that the item will be used "FOR TRAINING ONLY" or that it is a "TRAINING PROP." Smaller items may be bagged and tagged. Items should be stored in a way to preclude use.

If authorized by the OIG, destruction of the S/CI should be performed in a manner that permanently and irrevocably alters the S/CI so that it cannot be used. Examples of alteration include melting, shredding, or destroying the threads on fasteners; crushing circuit breaker casings; or embedding fasteners in concrete or other media, rendering them useless. A Certificate of Destruction should be obtained from the disposal source or used to trace destruction of items. Certificates of Destruction forms should contain the following information:

- 1) Traceability to the item or documentation used for disposition (e.g., nonconformance report number);
- 2) Item part number, model number, or other identification number;
- 3) Method of destruction;
- 4) Source of destruction (internal or external source being used and contract number if applicable); and
- 5) Date destruction was completed.

Burying S/CIs may be acceptable if they do not contain hazardous material or material prohibited by Federal, State, or local regulations (for example cadmium-plated fasteners; chromium, welding materials; etc.).

Consideration should be given to surplus safety systems, components, structures, and mission-critical facilities that have been confirmed counterfeit. All systems, structures or components with known S/CI should have an associated NCR, which should remain open until those surplus SSCs or systems essential to mission execution facilities are sold, returned to use, or scrapped.

For more other information related to S/CI and Resources see [Appendix C](#).

5 Indicators for S/CI Hardware Items (Fasteners)

There are diverse types of fasteners used throughout DOE, both in critical and non-critical applications. Typically, critical application fasteners must be “High-Strength” or rated with a minimum tensile strength of 120,000 pounds per square inch (psi). These are fasteners considered equivalent to a SAE grade 5 or above. High-strength fasteners are also required to meet requirements from internationally recognized consensus standards such as American Society for Testing Materials (ASTM), ASME, ISO, and Society of Automotive Engineers (SAE), etc. When fasteners do not meet these standards, they may be more likely to fail and there have been documented cases of failures which have resulted in millions of dollars of damage and losses in life. Therefore, it is critical that DOE and its contractors have a rigorous S/CI process for identifying sub-standard fasteners.

It is also imperative that organizations understand U.S. laws such as the Fastener Quality Act (FQA). The FQA, Public Law (PL) 101-592, was signed by President George H. W. Bush on November 16, 1990. The Act protects public safety by: (1) requiring that certain fasteners, sold in commerce, conform to the specifications to which they are represented to be manufactured; (2) providing for accreditation of laboratories engaged in fastener testing; and (3) requiring inspection, testing, and certification in accordance with standardized methods.

On March 7, 1996, President William J. Clinton signed the National Technology Transfer and Advancement Act of 1995, PL 104-113, which amended the FQA to further clarify and define the requirements of the original Act. Further amendments were announced on August 14, 1998 (reference PL 105-234), which exempted certain fasteners approved by the Federal Aviation Administration (FAA) from FQA coverage. Additional acts were released on June 8, 1999, which amended the FQA further (reference PL 106-34 and FQA Amendments Act of 1999). The amendments added clarification to “consensus standards” used for fasteners.

Fasteners should be considered suspect/counterfeit or defective when they do not conform to nationally recognized consensus standards. This may include the failure to meet specific criteria such as marking (e.g., manufacturer identification), mechanical testing, or chemical composition requirements.

Fasteners that do not include a manufacturer mark but include a grade (e.g., are high strength) may be considered “suspect” and require further evaluation to determine if the:

- (1) Consensus standard requires marking such as grade marking and a manufacturer marking;
- (2) Item meets the standard requirements; or
- (3) Item is defective, counterfeit, or fraudulent because it does not meet the consensus standard requirements (e.g., marking, mechanical, chemical requirements).

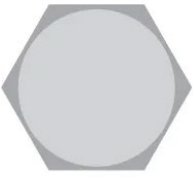

Fasteners without any headmark are not high-strength and do not fall under FQA requirements. It is still important to verify procurement contract requirements and specifications to see if the bolt was specified to be a certain grade. See example below:	Fasteners that have a “grade” mark, are not part of an assembly, and are considered high strength (above 120,000 psi) fall under FQA requirements. If missing a manufacturer marking as noted below, the fastener is not in compliance with this requirement and should be reported as S/CI. If part of an assembly, additional verification should be completed such as inspection or test to determine authenticity.
 <p>No grade marking and no manufacturer marking</p>	 <p>SAE Grade 5 Marking without a manufacturer marking</p>

Table 3: Headmark Comparisons

5.1 FQA Clarifications

Does a manufacturer-produced fastener meet the Fastener Quality Act requirements?

- 1) Use resources including but not limited to the U.S. Patent and Trademark Office (USPTO) [Fastener Quality Act reference site](#)³ and Department of Defense Specialty Metals Certification [website](#)⁴ to identify the manufacturer from their insignia (if the item is marked).
- 2) Validate that the manufacturer is a registered fastener manufacturer by checking with the USPTO, by verifying current fastener insignia list⁵. If they are not registered, then they must have a valid and current quality management system from a consensus standard organization (e.g., ISO 9001) – see #4 below for FQA exclusions.
- 3) Validate the fastener meets the grade requirements listed on the fastener such as marking, mechanical, and chemical (e.g., ASTM, ASME, ISO, SAE, etc.).
- 4) Some fasteners fall under the FQA exclusions which means they would not automatically be considered “fraudulent” or “suspect” if found to lack registration with the USPTO or meeting other FQA requirements. However, they may be considered suspect/counterfeit or defective if further evaluation such as chemical or mechanical testing concludes the item is substandard, or if the fastener is included on the “Legacy Fastener Headmark List” (see [Appendix A](#)). NOTE: the fasteners in Appendix A should be considered suspect/counterfeit and no further testing is required.



³Fastener Quality Act Reference Site: <https://www.uspto.gov/trademarks/laws/fastener-quality-act-fqa/fastener-quality-act-fqa>.

⁴ DoD Specialty Metals Certification website: https://www.indfast.org/info/specialty_metal_certifications.asp.


⁵ USPTO FQA Registry website: https://www.uspto.gov/sites/default/files/documents/FQA_Registry.pdf.

The NIST website⁶ contains additional frequently asked questions with regards to the Fastener Quality Act.

5.2 Suspect/Counterfeit Fastener Indicators

Indication	Example
<p>Marking:</p> <ul style="list-style-type: none"> Fastener is missing a manufacturer or grade mark (unless certified to a specification not requiring marking). Missing key information or markings on packaging. Head markings are marred, missing, or appear to have been altered. 	 <p><i>Figure 4: SAE Grade 5 bolts without a manufacturer mark</i></p>
<p>Marking:</p> <ul style="list-style-type: none"> Headmarks with raised marks and depressed marks on same fastener (not normal manufacturing process). Stamping contains metric and standard measurements or double stamping. <p>NOTE: Some manufacturers to identify and trace a fastener to a specific lot, as part of their process, may use a vibro-etch pen to note that lot number on the bolt head. This is acceptable as part of the manufacturing process.</p>	 <p><i>Figure 5: Double-stamped Bolt</i></p> <p>Additional Description: Bolt has been double stamped with two radial lines which indicate 18-8 stainless steel and B-8. These fasteners should be considered suspect/counterfeit and defective and should not be used. Although 18-8 and B8 are chemically equivalent, they differ in tensile strength.</p>

⁶ <https://www.nist.gov/standardsgov/compliance-faq-fastener-quality-act-fqa>

Indication	Example
<p>General Fastener Quality:</p> <ul style="list-style-type: none"> • Evidence of machining marks. • Poor thread form, evidence of wear, or threads are not of uniform color or finish. • Coating/plating is incorrect or inadequate quality. 	 <p>Figure 6: General Fastener Quality (Sokoloff, 2006)</p>

5.3 Identification Examples

5.3.1 Case Study #1

An 8.8 metric fastener without a manufacturer marking is identified on a ratchet strap. The fastener would be considered “suspect” until further analysis or testing could be conducted to prove that the item is defective or counterfeit. Testing on items such as bolts for ratchet straps may not be cost effective or feasible.

In the example for the ratchet strap, if ISO 898-1, *Mechanical Properties of Fasteners Made of Carbon Steel and Alloy Steel Part 1* was specified this would require the 8.8 fastener to have a manufacturer marking and the fastener would be at a minimum be considered nonconforming to that marking requirement. This can be determined visually and without testing. Further chemical and mechanical testing may be conducted to determine if the fastener material was misrepresented did not meet the requirements of the standard and the material was not capable of meeting its intended use. Fasteners in assemblies (e.g., ratchet straps) are *excluded* under the Fastener Quality Act (FQA) from automatic determination as counterfeit and/ or fraudulent such as in the example of the ratchet strap, but items should still be evaluated to determine if they are adequate/safe for the intended use (i.e., using a graded approach and as determined by local processes or procedures).



Figure 7: 8.8 grade bolt no manufacturer marking

5.3.1.1 Case Study #1 Disposition & Reporting Example:

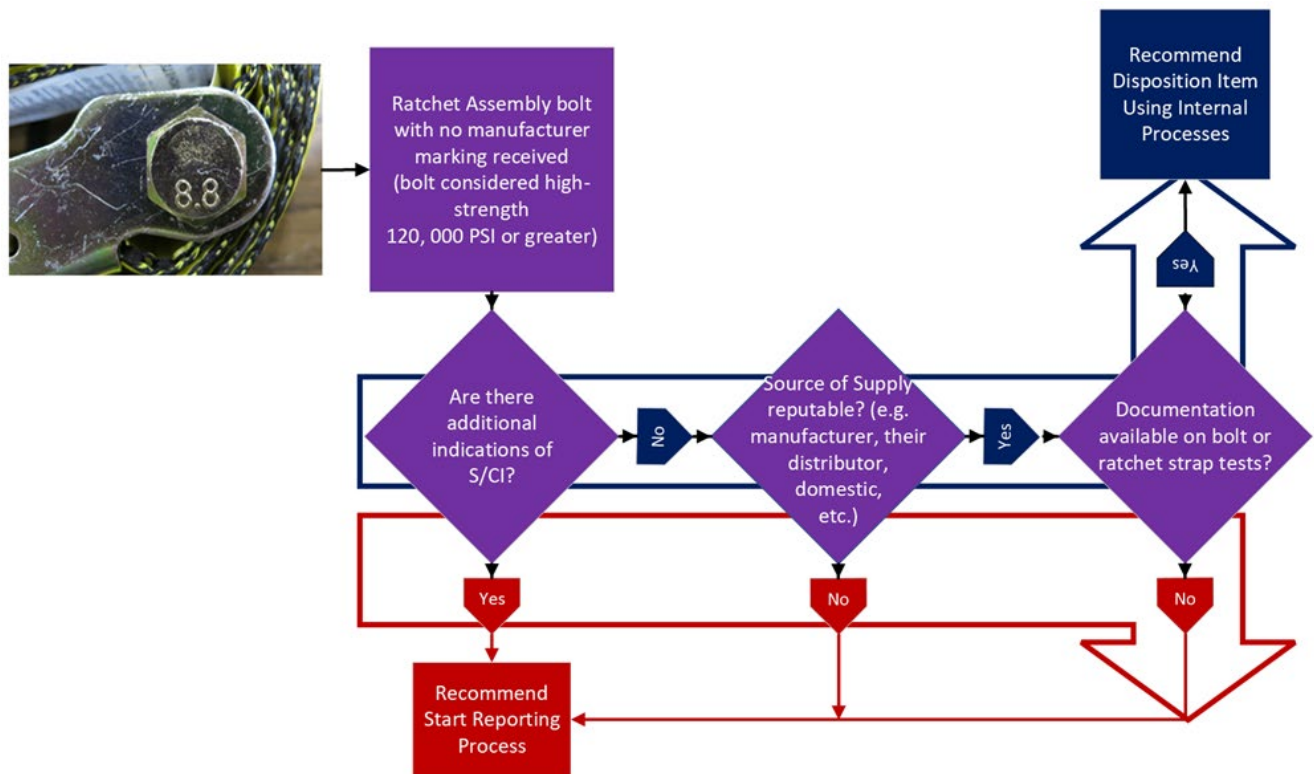


Figure 8: Sample disposition process for a ratchet strap

Start Reporting Process:

Fasteners that are determined to be S/CI are required to be reported. This may include local S/CI reporting processes. The S/CI Coordinator or individual responsible for reporting external to the organization may follow these additional reporting steps:

- 1) In case study #1, this item was found to be nonconforming and *suspect* due to the missing manufacturer marking. However, because the item is part of an assembly, further analysis should be conducted to confirm whether or not the item is substandard, counterfeit, or defective. Unless further analysis is conducted (e.g., testing, documentation is obtained that indicate substandard material), the item is not required to be reported to the DOE OIG. If the item was not part of an assembly, then report it to the DOE Office of Inspector General (OIG) in accordance with DOE O 414.1 (current), *Quality Assurance*.
- 2) Report to the Occurrence Reporting and Processing System (ORPS) in accordance with DOE O 232.2A (current), *Occurrence Reporting and Processing of Information*. Suspect/Counterfeit and Defective Items that meet the criteria of this order may be reportable to ORPS⁷. In the example of case study #1, if the ratchet strap was found in use, this is reportable to the ORPS system. If the ratchet strap was found in receipt inspection, then it would not be reportable to ORPS.

⁷ <https://www.energy.gov/ehss/occurrence-reporting-and-processing-system> to learn more about the ORPS database.

- 3) Report Operating Experience in accordance with DOE O 210.2 (current), *DOE Corporate Operating Experience Program*. Suspect/Counterfeit and Defective Items operating experience such as best practices, lessons learned, or other information that may be valuable to the broader DOE enterprise may be reported using the DOE OPEXShare website⁸. Information regarding the ratchet strap and processes used to identify, remove, or any lessons gained may be shared with the broader DOE community.
- 4) Report to the Government-Industry Data Exchange Program (GIDEP)⁹ in accordance with Federal Acquisition Regulation (FAR) 52.246-26, Reporting Nonconforming Items. If this FAR is included in a contract (e.g., contractor to DOE or subcontractor), it would be a requirement to report S/Cis and certain nonconformances (major and critical). The ratchet strap may be considered reportable depending on how the item is used (e.g., item failure could adversely affect the environment, safety, or health of the public or workers).

5.3.2 Case Study #2

Surveillances and inspections of inventories and legacy equipment may aid in identifying suspect/counterfeit fasteners. In one such case, a DOE site was inspecting a legacy lift when they noticed that the lift had “KS”-marked SAE grade 5 bolts. These bolts are included on the Legacy Headmark List ([Appendix A](#)). If these bolts were produced prior to 1999, they could be substandard and should be removed from service. Testing may be conducted to determine safety/adequacy if items will continue to be used. Items produced after 1999 may also be tested to verify quality. Some manufacturers have improved the quality of their products since they were placed on the Legacy Headmark List. However, legacy materials that may be in stock or on older assembled components may have questionable quality. Since it may not be possible to determine when the bolts were produced, to be on the side of caution, the organization should replace the bolts.



Figure 9: “KS”-marked bolt from Legacy Headmark List

This item is considered “suspect/counterfeit” per the Legacy Headmark List in [Appendix A](#).

⁸ opexshare.doe.gov to learn more about OPEXShare.

⁹ <https://www.gidep.org/> to learn more about GIDEP.

5.3.2.1 Case Study #2 Reporting:

Fasteners that are S/CI should be reported using the organizations S/CI reporting process. The S/CI Coordinator or individual responsible for reporting external to the organization may follow these additional reporting steps:

- 1) Report to the DOE OIG in accordance with DOE O 414.1 (current). This item was found to be *suspect/counterfeit* due to the manufacturer marking being on the Legacy Headmark List (reference [Appendix A](#)). If procurement / supplier information can be obtained or is known, this item *should be* reported to the DOE OIG.

Additional Legacy Fastener Reporting Example: A legacy bolt was found in the back of closet. No one knows when, where, or how it was procured or brought onto the DOE site, but it is suspect/counterfeit. This would *not* be reportable to the OIG since there is no information to investigate.

- 2) Report to ORPS in accordance with DOE O 232.2A (current). Suspect/Counterfeit and Defective Items that meet the criteria of this order *may be* reportable to ORPS¹⁰. In the example of case study #2, the bolts were found on a legacy lift in which the item was in use and performed a function that could affect safety (i.e., lifting personnel or materials). This would be reportable to ORPS.
- 3) Report Operating Experience in accordance with DOE O 210.2 (current). Information regarding the bolts and processes used to identify, remove, or any lessons gained may be shared with the broader DOE community.
- 4) The bolts should be considered for reporting to GIDEP in accordance with FAR 52.246-26 since the item may adversely affect worker safety if it were to fail.

5.3.3 Case Study #3

A standard stainless-steel bolt sheared during a torquing operation causing concern that the bolt may be suspect/counterfeit. After verifying all the mechanical and chemical attributes of the bolt it was determined that the attributes were all in the ranges specified and there were not any other indications (other than the bolt shearing unexpectedly) that would cause suspicion that the item might be suspect/counterfeit. After further review it was found that the torquing operation was not conducted to manufacturers specifications which caused the bolt to shear. In this case the cause of the defect was of a controllable nature, therefore the item is *not* considered suspect or counterfeit. It is still a best practice to always review items for the potential of suspect or counterfeit when there is an unexpected failure, especially in systems where the item may be more critical.

5.3.3.1 Case Study #3 Reporting:

Fasteners that are S/CI should be reported using the organizations S/CI reporting process. The S/CI Coordinator or individual responsible for reporting external to the organization may follow these additional reporting steps:

- 1) In case study #3, this would *not* be reportable to the DOE OIG.

¹⁰ <https://www.energy.gov/ehss/occurrence-reporting-and-processing-system> to learn more about the ORPS database.

- 2) Report to the Occurrence Reporting and Processing System (ORPS) in accordance with DOE O 232.2A (current). Suspect/Counterfeit and Defective Items that meet the criteria of this order may be reportable to ORPS¹¹. In the example of case study #3, this *may be* reportable to ORPS depending on the particular details surrounding the bolt shearing (e.g., did anyone get injured, was there a possibility of someone being injured, how was the overall end product going to be used and if the bolts sheared in use would this have injured anyone).
- 3) Report Operating Experience in accordance with DOE O 210.2 (current). In this case, information *may be* shared with the broader DOE community.
- 4) The bolts would not be reportable to GIDEP in accordance with FAR 52.246-26 since the shearing was caused by an installation error and the manufacturer's instructions were not followed.

6 Electronics

Counterfeit electronics pose a serious threat to industry and government supply chains. Counterfeiters have attacked every commodity of electronics from simple components such as capacitors, to complex integrated circuits, such as microprocessors, and complete assembled units such as computer network routers. Inexpensive commercial devices, as well as high-cost military components, have been counterfeited.

Counterfeit electronic parts may be divided into five major categories, which can be broken down into 4Rs and 1C or 4R1C as shown below:

- 1) Recovered;
- 2) Refurbished;
- 3) Repackaged;
- 4) Rejected; and
- 5) Cloned.

Electronics that have indications of S/CI should be reported using the organizations S/CI reporting process.

6.1 Recovered

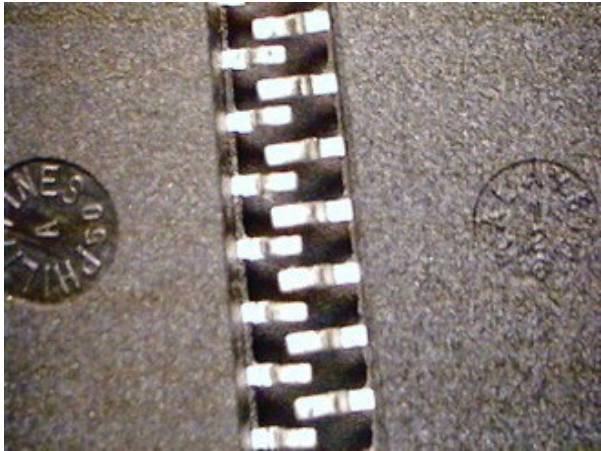
The first "R" is *recovered* electronics. In recent years, recovered electronics are the most common type of suspect/counterfeit electronic items. The first major wave of counterfeit parts was recovered parts from salvaged electronics waste. This type of counterfeit device has the appearance of the correct device, often with the wrong die¹² internally and a remarked package. The counterfeiter's process includes:



¹¹ <https://www.energy.gov/ehss/occurrence-reporting-and-processing-system> to learn more about the ORPS database.

¹² A small block of semiconducting material on which a given functional circuit is fabricated.

- Component removal;
- Sanding and/or blacktopping (recoating);
- Remarking;
- Detailed cleanup of solder; and
- Packaged to make it look new.

These parts can be caught early by a careful visual inspection using industry methods described in the Independent Distributors of Electronics Association (IDEA) Standard 1010-B, *Acceptability of Electronic Components Distributed in the Open Market* and SAE standard AS6171/2A, *Techniques for Suspect/Counterfeit EEE Parts Detection by External Visual Inspection, Remarking and Resurfacing, and Surface Texture Analysis Using SEM Test Methods*. On the occasions that they are not visually detected, decapsulation or basic tests such as a curve trace will identify the counterfeit units. If these devices reach the application board, they may fail outright and cause serious delays to manufacturing schedules. If the device makes it to the field, it can pose a significant risk due to unreliability and premature failure. Recovered Parts Examples (Blacktopping):

Description	Figure
Indent that has been filled in with the “blacktopping” material.	 <p data-bbox="932 1373 1260 1402"><i>Figure 10: Blacktopped Example</i></p>

<p>Close-up of indent that has been filled in with the “blacktopping” material.</p>	 <p><i>Figure 11: Blacktopped Example-Indent Filled</i></p>
<p>Shows blacktopping on the edge of the parts. See how the top of the part is shiny and the bottom has a duller finish. These parts are made in a mold. These molds are not designed to put a beautiful shiny finish on the top so they can sell their good looks. The texture should not change halfway on a section of the part. This picture is a notable example of an original vs. a fake finish.</p>	 <p><i>Figure 12: Blacktopped Example –Side View – Overspray</i></p>


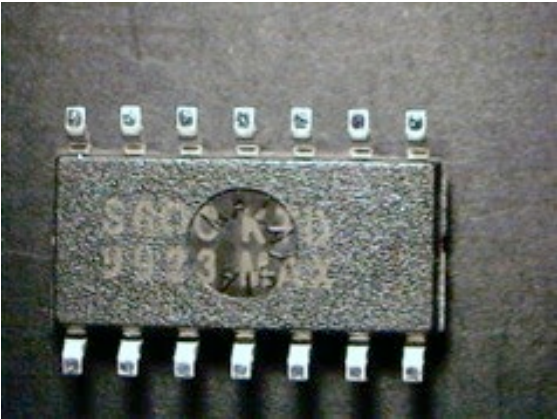
6.2 Refurbished

The second “R” is *refurbished* electronics. These electronic devices are often the correct item and may even still have the original marking on the package. These refurbished units are at an elevated risk of failure since they are often subjected to excessive heat during removal from previously used circuit or wiring boards and may have been introduced to harsh chemicals during the refurbishment process. Excessive heat can weaken the die. Counterfeiters have become experts in reworking a package and the solder on the leads. They can make the device look new and unused.

Even the best visual inspection techniques can have a challenging time identifying these refurbished parts with certainty. Typical signs that a part may be S/CI include solder that looks too new, the absence of test contacts on leads, questionable scratches, and solder inconsistency. Decapsulation provides no assistance in the detection of units that have the correct die internally. After careful visual inspection, an additional test that provides value with plastic parts is Scanning Acoustic Microscopy (SAM). SAM can look inside the package to look for severe internal package damage. Electrical testing is also effective since device

failure rates provide an indication of handling issues. Entire lots should be rejected if the high failure rates indicate systemic issues, which may indicate long term reliability concerns with all the units. Refurbished parts would have similar packaging indications as recovered parts.

6.2.1 Refurbished Electronics Examples:

Description	Figure
<p>Sanding is noticeable in the upper left-hand corner of the item.</p> <p>(reference: Counterfeit electronic component detection – AERI)</p>	 <p><i>Figure 13: Sanding Example</i></p>
<p>This part is marked on top of the indent, which is not acceptable per manufacturing specifications.</p> <p>(reference: Counterfeit electronic component detection – AERI)</p>	 <p><i>Figure 14: Marking on Indent</i></p>

6.3 Repackaged

The third “R” is *repackaged*, which often involves die salvaging. This is another common method available to counterfeiters and is a process that removes a compatible die from a used package for subsequent use in a newly manufactured package. The package was chemically decapsulated, the die was removed, and then the die was built into new package. The result is a newly packaged device with the correct die internally. All the packaging and marking are new, so it does not appear to be suspicious. However, there is great danger in using the parts since the chemical decapsulation process damages the die and diminishes its reliability. An internal visual inspection of the die will not typically identify the recovered die. An extensive Scanning Electron Microscope (SEM) Destructive Physical Analysis could

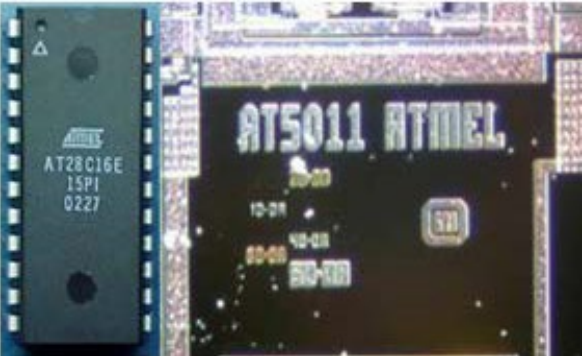
detect the recovered die, but SEM analysis is not typically part of counterfeit device inspection. The best method of detection is a robust electrical test at design temperature and vibration conditions. Parts are not normally screened under actual design conditions. Chips assembled in this way result in high failure rates due to inferior quality and reliability of the recovered die.

Also closely related to recovered die are units that are newly manufactured from acquired dies. The new die can be purchased from reputable sources or illegally obtained from integrated circuit (IC) manufacturer's rejects. A leftover failed die can be effectively used by the counterfeiters since the finished unit will look correct in every way. Once again, the only effective method to identify these units is a robust electrical test since visual identification techniques are ineffective on newly packaged units.

Counterfeiters are becoming experts in device substitution. In this way, they are working as component engineers trying to determine the device that will work as the best substitute for the requested device. Using device substitution techniques, they are able to replace one transistor with a similar function. It is an easy task to identify a similar device and remake the component, since die markings on such components are not common. The substitution may have significant issues since the replacement part may have insufficient parameters for handlings (voltages, amperages, etc.) and may not be able to withstand the designed requirements. The counterfeiter's methods also extend to simple components such as capacitors, resistors, and diodes. These simple device types often have minimal or no marking present on the packages.

6.3.1 Repackaged Example

In the example, the comparison of a S/CI and genuine Atmel device on external visual inspection indicate a variation in indent locations. This should suggest that further evaluation of the device is necessary. Upon further evaluation of the internals of die after decapsulation, there are inconsistencies in manufacturer markings with the genuine being marked "ATMEL" and S/CI being marked "CSI."

Description	Figure
Genuine Atmel Device is marked "Atmel" on interior of die.	 <p data-bbox="850 1640 1182 1667"><i>Figure 15: Genuine Atmel Device</i></p>

Suspect/Counterfeit is missing pin 1 locator indent and indents are inconsistent to comparison genuine example. Marked “CSI” instead of “Atmel” on interior of die.



Figure 16: Counterfeit Atmel Device

6.4 Rejected

The fourth “R” is *rejected* by manufacturers. Usually, these are tightly controlled, but rejected items continues to be an issue. These rejected items occasionally show up in the secondary components supply chains. Most manufacturers have tightened their procedures to ensure that rejected items are not reused; however, it is difficult to have complete assurance that a failed device is destroyed. Some of the units can be diverted or smuggled out and eventually sold as new. These rejected units are often nearly functional, and with the true manufacturer marking they look like real, fully functional units. The risks are also significant for eventual re-use of rejected wafers, or re-use of the remaining rejected die left over after assembly. Robust electrical testing may be one of the only effective methods to identify manufacturing rejects that could be sold as good units.

6.5 Clones

“C” stands for *clones*. SAE Aerospace Standard AS6171 *Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts* defines a cloned part as: *A reproduction of a part produced by an unauthorized manufacturer without approval or design authority that replicates the authorized manufacturer’s part.*

Counterfeiters that use the “cloning method” are eliminating a substantial portion of the development costs of the part, which is why this method is becoming more popular. Cloning can be done in two ways: by reverse engineering or by obtaining design information and/or technical data inappropriately (such as by unauthorized knowledge transfer from a person with access to the part design). An alert on cloned parts issued by ERAI identified the following indicators:

- Inconsistent font and grammar on all labels which had appeared to be tampered with.
- Inconsistent part markings when compared to a known good device.

- Inconsistent pin-one indicator cavities which varied in depth.
- Solvent tests did not present signs to indicate the parts were not authentic.
- A scrape test concluded no resurfacing material was present.
- Radiological inspection revealed the lead frame, die size and placement and bond wire gauge and routing were inconsistent from the known good device.
- XRF analysis found the leads contained Sn and Cu which did not match the factory label denoting RoHS compliancy code “e4” and varied from those found in the known good devices.
- Decapsulation revealed the die layout was consistent between the samples but differed “significantly” from the known good devices.
- SEM did not uncover any signs to indicate the components were not authentic.
- The parts passed visual inspection.

Clones may be identified by performing destructive physical analysis. It is often during these tests that discrepancies and differences from the original manufacturer may be identified.

6.6 General Test Methods for Electronics

How is testing conducted for 4R1C as discussed above? Inspection methods can be based on a graded approach or could use a multi-stage process dependent on findings from the previous stage. For example, an organization may begin by inspecting the item’s packaging then move to visual inspection of the parts. In addition to this, organizations may use sampling plans to accommodate large quantity purchases. Below are some common test methods listed in order of graded approach from least to most intensive.



Table 4: Electronics Evaluation Table- Level of Rigor

6.6.1 Visual Inspection

A visual inspection is a non-destructive test used to verify attributes of component, such as condition, part marking, lead conditions, dimension, and surface quality. The inspection should start with the exterior box, Electro-Static Discharge (ESD), or other manufacturer-provided packaging. Additional indications to note during visual inspection of packaging include:

- 1) Part orientation in package. Are all items oriented the same direction?
- 2) Pin orientation. Do all parts in a reel or tape appear to have pin one oriented in the same direction and do they all appear to be of the same design and type (e.g., consistent)?
- 3) Parts packaged in accordance with manufacturers specifications. Are the items packaged correctly in accordance with manufacturer's instructions or specifications (e.g., humidity, impact, or other necessary controls to prevent damage during shipment or storage)?

6.6.1.1 General Packaging Indicators

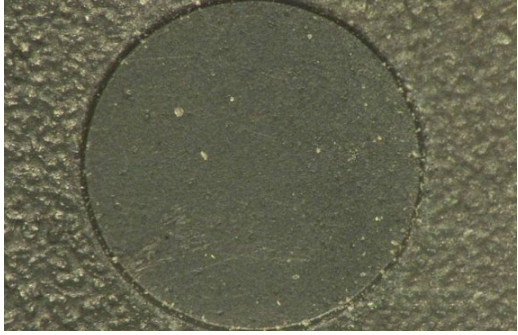
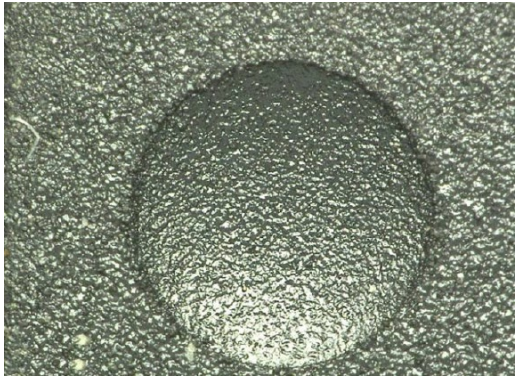
All reputable electronics manufactures have quality standards that reduce the likelihood of major imperfections. The part numbers are to be in a certain location on the part, and they are not to be crooked, misspelled, or out of alignment. The logos are also monitored very closely and should not vary from part to part. In addition, the markings are to withstand tough environments and still be legible. Visual inspection of the exterior of the item (often referred to as the package) can be conducted with or without a microscope. Typically, this type of inspection will require some sort of comparison such as the manufacturer datasheet to provide specifications (e.g., package type, dimensions, markings, or other relevant data).

Some indications to note when inspecting the general appearance of items include:

- Part markings;
- Color of the part marking;
- Color of the surface; and
- Scratches or chip outs on the surfaces.

6.6.1.2 Indents

Indents should be inspected to verify that they are per manufacturer specification. Indents are never partially made during the manufacturing process and they should be consistent and uniform in depth throughout the circle.

<p>Example of a uniform and acceptable indent that is smooth in appearance (Harold "Woody" Hewett, Electro-Comp Services, Inc., 2010)</p>	 <p><i>Figure 17: Example of Acceptable Indent</i></p>
<p>Indent is grainy in appearance, which indicates alteration of the part.</p> <p>(Harold "Woody" Hewett, Electro-Comp Services, Inc., 2010)</p>	 <p><i>Figure 18: Example of Suspect Indent</i></p>

6.6.1.3 Markings

Remarking is becoming increasingly difficult to detect. Methods are being used by counterfeiters that will completely remove ink markings and leave no remnant or shadow of the original marking (i.e., ghost markings). The new markings which are applied over the top, look completely normal and may pass visual inspections. Counterfeiters are even using surface sandblasting and laser ablation to remove laser marking which was previously being removed by sanding. Chemically impervious blacktopping materials that have similar material composition to the original plastic package are also in use. These blacktop materials are not easily dissolved by military specifications marking permanency tests or even acetone tests. Blacktop removal now requires more aggressive chemical removal methods such as Dynasolve.

Not all blacktopping is a sign of counterfeit components. Some companies blacktop or coat their chips on a board after fabrication. This effort precludes individual component replacement or repair. Thus, the device should be returned to the vendor for repair services.

Additional questions on marking indications include:

- Are part markings consistent with manufacturer's requirements and do they appear to be good quality (e.g., verify placement, alignment, marking consistency, etc.)?

- Are the date codes and lot codes consistent with when and where the part was originally manufactured?
- Is the item still produced or is it obsolete? Sometimes items are produced well after the date the manufacturer stopped production and no other manufacturers have picked up the production. Reference Product Change Notifications (PCNs) to determine if an item has changed manufacturing locations, when it was first starting to be produced, and when it was last produced. PCNs may also aid in noting marking or die changes. PCNs are often available from the manufacturer on their website or by request.

Note that the “C” in the top line is different than the “C” in the bottom line and that the “3” is slightly higher than the other markings in the same line. These indications are consistent with remarking.

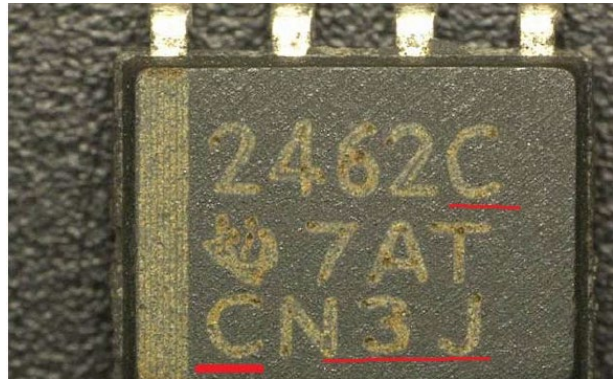
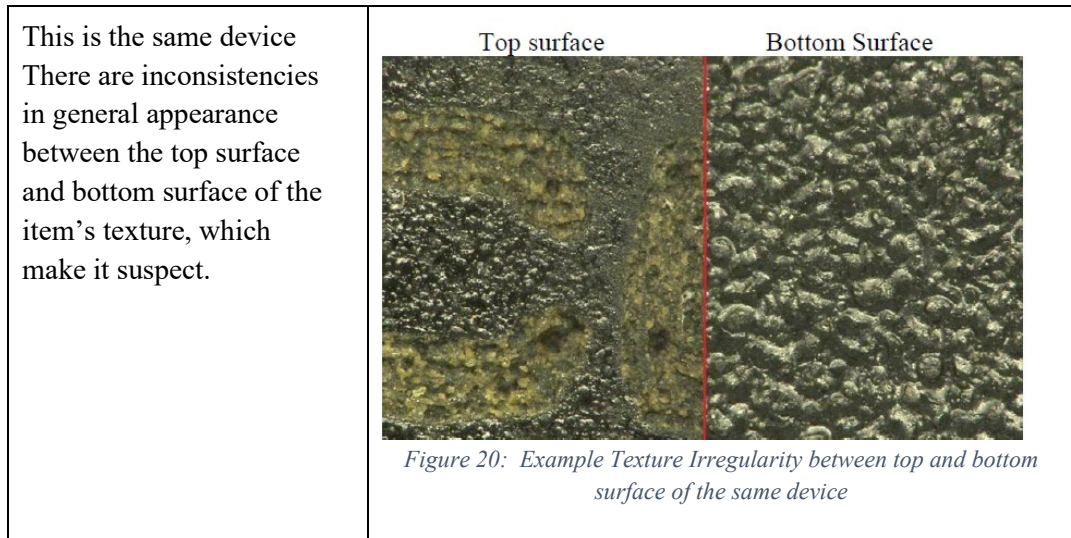


Figure 19: Example Indications of Remarking

6.6.1.4 Surface and Texture Appearance

Plastic electronic components are typically made with a mix of fine glass and plastic. The surface of the molded package is textured when it is removed from the mold. Although difficult to see in pictures, a microscopic view shows that the differences between a typical fake and the surface of an authentic part can best be described as having a sharper and duller look. The glass in the mixture makes for sharp peaks and valleys, whereas, when painted with the blacktopping material the peaks and valleys are smoothed over and filled in, as if there were a coat of paint on sandpaper. The surface should have a molded appearance rather than a surface that has been changed by chemical or sanding to remove initial markings. Inspect the texture (grain) of the surface of the part where applicable. Are the top and bottom textures the same?



6.6.1.5 Contact Surfaces

Inspect contact surfaces such as leads, balls, and contacts for the following:

- Are the leads bent or bowed?
- Are there any insertion marks?
- Are the leads, balls, or contacts too shiny?
- Is the plating smooth and even? Are there any voids in the plating?
- In the case of a Ball Grid Array, are the balls flattened or distorted?
- Is there any foreign substance visible on the surfaces or the leads?
- Do items have the correct number of leads, balls, pads, etc.?

6.6.2 Dimensional Inspection

Dimensional inspection may be used to compare the physical attributes and dimensions of the part to the specifications and requirements in manufacturer datasheets. A micrometer or other instrument with the appropriate level and accuracy should be used. When measuring a part, it is especially important to measure part thickness as it may be a key indicator that the part has been remarked.

Note in the image that the part thickness is undersized which is a key indicator that the part may have had a portion of the top layer of the original markings removed by sanding and then has been remarked. (Harold "Woody" Hewett, Electro-Comp Services, Inc., 2010)

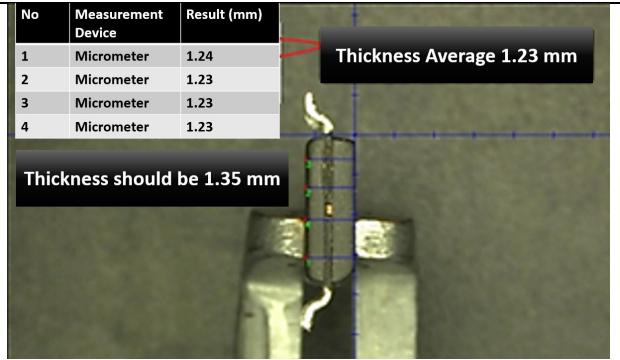


Figure 21: Example Dimensional Inspection

6.6.3 Resistance to Solvents and Scrape Testing

There are several ways to verify a device's resistance to solvents which include the use of chemicals (such as acetone or Dynasolve) or using a scrape test method. The purpose of these tests is to determine if a part has been blacktopped or has a false coating material which has been used for remarking.

Acetone was used to remove blacktopping, which after removal sanding is clearly visible. (Harold "Woody" Hewett, Electro-Comp Services, Inc., 2010)



Figure 22: Example Resistance to Solvent Failure

When the scrape test is performed on a part that has been remarked, there is flaking visible on the surface where the part was scraped. (Harold "Woody" Hewett, Electro-Comp Services, Inc., 2010)

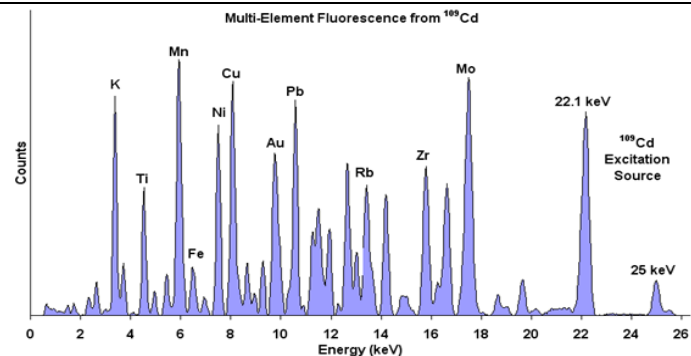


Figure 23: Example Scrape Test Failure

6.6.4 X-Ray Fluorescence Testing (XRF) Analysis

X-ray fluorescence is a non-destructive testing method used to analyze the chemical composition of an item. XRF analyzers determine the chemistry of a sample by measuring the fluorescent (or secondary) X-ray emitted from a sample when it is excited by a primary X-ray source. Each of the elements present in a sample produces a set of characteristic fluorescent X-rays (“a fingerprint”) that is unique for that specific element, which is why XRF spectroscopy is an excellent technology for qualitative and quantitative analysis of material composition.

Example of XRF where multiple elements are identified in the sample.



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

Figure 24: Example XRF Analysis

XRF Resources: AS6081, *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors*; AS6171, *Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts*; and ASTM-B658-98, *Standard Test Method for Measurement of Coating Thickness by X-Ray Spectrometry*.

6.6.5 X-Ray Inspection

X-Ray is a non-destructive testing method used to aid in identifying defects internal to the device. There are various methods of X-Ray that may be employed such as computed laminography and computed tomography. X-ray can detect voids, cracks, and differences in die construction.

X-Ray Inspection Resources: SAE AS6171/5, *Techniques for Suspect/Counterfeit EEE Parts Detection by Radiological Test Methods*.

6.6.6 SAM and C-SAM Inspection

Scanning Acoustic Microscopy (SAM) and Confocal Scanning Acoustic Microscopy (C-SAM) are non-destructive analysis methods to detect defects inside of an electronic device. These methods use ultrasonics to detect material changes; therefore, SAM and C-SAM may detect more finite defects (such as cracks and delaminations), and it may be more sensitive to voids that may be present in the material.

SAM and C-SAM Resources: AS6171/6, *Techniques for Suspect/Counterfeit EEE Parts Detection by Acoustic Microscopy (AM) Test Methods*. J-STD-020, *Standard Moisture/Reflow Sensitivity Classification for Non-hermetic Surface Mount Devices (SMDs)*; J-STD-033, *Joint IPC/JEDEC Standard for Handling, Packing, Shipping, and Use of Moisture/Reflow Sensitive Surface-Mount Devices*; and J-

STD-035, Joint IPC/JEDEC Standard for Acoustic Microscopy for Non-Hermetic Encapsulated Electronic Devices.

6.6.7 Destructive Physical Analysis (DPA)

Destructive Physical Analysis (DPA) is the process of performing decapsulation¹³ disassembling, testing, and inspecting electronic components to assess quality and reliability. Part of this testing may include other tests such as:

- Ball Shear Strength;
- Die Shear Strength;
- Digital Microscopy;
- Visual Inspection;
- Glassivation Layer Inspection;
- Cross-Sectioning;
- Particle Impact Noise Detection;
- Scanning Electron Microscopy (SEM);
- SEM Metallization Inspection;
- Solder reflow/ Moisture Sensitivity Testing;
- Glassivation Thickness;
- Metallization Thickness;
- Hermeticity Testing;
- SEM, XRF, and FTIR elemental analysis;
- Scanning Acoustic Microscopy (C Mode); and

In the case of a hermetically sealed device, removal of the lid or “delidding” may be conducted using more of a mechanical process and will not require the use of a chemical agent. These types of items typically have a ceramic packaging that cannot be dissolved by acids or other erosive solvents; therefore, the top must be mechanically removed to expose the internal die.

Internal inspection permits the visual inspection for foreign material, corrosion, mechanical damage, or other workmanship and processing issues. In addition to this, items may be compared to known good items or a “gold standard” in order to identify potential die discrepancies.

DPA Resources: SSQ-25000, *Destructive Physical Analysis Testing Specification for the Space Station Program* and AS6171/4, *Techniques for Suspect/Counterfeit EEE Parts Detection by Delid/Decapsulation Physical Analysis Test Methods*.

¹³ The process of removing a cap, lid, or encapsulating material from a packaged integrated circuit by mechanical, thermal, or chemical means exposing the integrated circuit for further analysis, inspection, or electrical examination of the die and the internal features.

6.6.8 Electrical Test Methods and Inspection

Electrical testing may be conducted on individual items or Printed Circuit Boards (PCBs) to verify that components are functional, meet electrical specifications, or will fulfill specified reliability requirements.

Electrical Test Resource: AS6171/7, *Techniques for Suspect/Counterfeit EEE Parts Detection by Electrical Test Methods*.

6.6.9 Environmental Test Methods and Inspection

Environmental testing may be used to determine if a device will perform under extreme conditions for a defined period of time. Environmental testing can also be used to identify S/CIs and may include the following test methods and inspections:

- Accelerated aging testing such as Burn-In, High-Temperature Operating Life and Low-Temperature Operation.
 - Used to accelerate failure mechanisms and determine reliability.
- Cyclical Moisture Resistance.
 - Evaluates high-heat and humidity conditions.
- Highly Accelerated Stress Test.
 - Combines high temperature, high relative humidity, and high atmospheric pressure to evaluate accelerated resistance to humidity.
- Preconditioning Testing.
 - Measures the resistance of non-hermetic surface mount devices to worst-case moisture absorption followed by the soldering process and rework.
- Steam Aging.
 - Replicates shelf life by artificially aging components and circuit boards.
- Thermal Cycling.
 - Determines the ability to withstand exposure to alternating extremes of high and low temperatures.
- Thermal Shock Testing.
 - Accelerates failure modes due to rapidly changing temperatures.

7 Suspect/Counterfeit Software

Why is software quality and the prevention of substandard and counterfeit software so important?

Electronics, electrical products, and many of the modern conveniences that we rely on each day require software to control them. If the software does not work properly, this could result in frustration at a minimum or a catastrophic accident. Recent events such as the case of Elaine Herzberg, a pedestrian fatality with a self-driving Uber vehicle in Tempe Arizona in December 2018, prove that there is still a gap in discussion of liability, vulnerability, and quality that needs to occur around software controls.

The impact of adulterated and counterfeit software was examined in 2018 by The Software Alliance (BSA). It found that 37 percent of software installed on personal computers is unlicensed or counterfeit. Organizations now face a one-in-three chance of encountering malware when they obtain or install an unlicensed software package or buy a computer with unlicensed software on it. Because of the link between counterfeit software and IT security issues from malware, this poses a danger for consumers and businesses alike, especially when software is used in critical applications. (BSA, 2018)

Once they detect malware, consumers and enterprises may need to invest considerable time and money to identify the corrupted software, repair their systems, recover lost data, and deal with identity theft. Each malware attack can cost a company \$2.4 million on average and can take 243 days to detect and 50 days to resolve. To the extent that the infection leads to company downtime, or lost business data, it can also seriously affect the company's brand and reputation. The cost for dealing with malware that is associated with unlicensed software is growing too. It can now cost a company more than \$10,000 per infected computer, and cost companies worldwide nearly \$359 billion a year. (BSA, 2018)

In a 2022 report from Verizon, it was found that a data breach in the supply chain can lead to wide ranging consequences. Supply chain was responsible for 62% of System Intrusion Incidents in 2021. A supply chain breach occurs when someone infiltrates the system through an outside partner or providers with access to systems and data. This has dramatically changed the attack surface of the typical enterprise in the past few years, with more suppliers and service providers touching sensitive data than ever before. Solar Winds, which is discussed in Section 7.3 below, is an example of a supply chain breach that impacted DOE and many other Federal agencies. (Verizon, 2022)

DOE sites may also be impacted through the purchase of commercial enterprise resource software or products that may have been exaggerated or misrepresented as having specific features, capabilities, or functionality that they really do not.

7.1 CASE STUDY: Lufkin VS IBM

Lufkin Industries, a publicly traded company based in Lufkin, Texas, manufactures machinery and equipment used in various segments of the energy industry. In 2009, Lufkin decided to upgrade its business-operations computer-software system. Over a period of several months, Lufkin engaged in numerous meetings with International Business Machines (IBM) Corporation in which they exchanged information about Lufkin's needs and IBM's capabilities. Lufkin needed an "off-the-shelf" system that could quickly replace its old system for a price lower than the cost of upgrading that system. Based on

Lufkin's operational needs, IBM recommended its "Express Solution for SAP," which uses software developed by SAP¹⁴, a separate German corporation.

During these extended discussions, IBM made numerous representations about its Express Solution that turned out to be false. IBM represented that the Express Solution was a preconfigured system that could be implemented for Lufkin within 4 to 6 months and meet 80% of Lufkin's requirements without any enhancements. Even though IBM knew that its Express Solution would require extensive customization before it could meet most of Lufkin's needs, IBM continued to represent the Express Solution as a "fit" for Lufkin. The intent was to land the sale and then figure out how to provide what Lufkin needed. Lufkin purchased the products and found that it did not meet their needs. When Lufkin filed suit, the jury found IBM liable on all claims. The jury awarded damages for fraudulent inducement and common law fraud but awarded zero damages for breach of contract. (International Business Machines Corporation, Petitioner v. Lufkin Industries, LLC, Respondent, 2018)

The Lufkin case study demonstrates the impact that a substandard software can have to a business and costs to a project. The impact of safety or critical application software as shown in the next case study can be much more detrimental.

7.2 CASE STUDY: Cisco Networking Devices

An IT company asked a cybersecurity firm to analyze some of its equipment only to discover that some of its core Cisco networking devices were counterfeit. In the case of this analysis, the counterfeits were made for profit and did not include any malware, but the items did have access to exploit backdoors into the company to steal data and spread malware. The impact of a malicious counterfeit can be massive because this gives the attacker full control of that system. This is just one form of a supply-chain induced attack. (Newman, 2020)

To avoid the procurement of counterfeit products, Cisco encourages customers to procure items directly from them or their authorized distributors by going [here](#)¹⁵. Cisco also has an Identifying Counterfeit and Pirated Products [here](#)¹⁶.

There have been numerous instances of the Department of Justice bringing charges against Cisco counterfeit schemes including where items were sold to the U.S. government. Recently, a large case has been brought forward concerning fraudulent networking products which initiated an Operating Experience Level 3 (OE-3), *Suspect/Counterfeit and Fraudulent Networking Products*, to raise awareness of this issue across the DOE Enterprise. This OE-3 can be found here:

<https://stage.energy.gov/ehss/articles/operating-experience-level-3-2022-01-suspectcounterfeit-and-fraudulent-networking>.

¹⁴ Systeme, Anwendungen und Produkte in der Datenverarbeitung (SAP GmbH) is a German Software Company

¹⁵ Cisco Distributor Locator website: <https://www.ciscochannelconnect.com/DistiLocator>

¹⁶ Cisco Counterfeit and Brand Protection Webpage: <https://www.cisco.com/c/en/us/about/legal/brand-protection/identify-counterfeit-products.html>

7.3 CASE STUDY: Solar Winds

SolarWinds is a major software company based in Tulsa, OK, which provides system management tools for network and infrastructure monitoring, as well as other technical services to hundreds of thousands of organizations around the world. Among the company's products is a IT performance monitoring system called Orion.

The SolarWinds hack is the commonly used term to refer to the supply chain breach that involved the SolarWinds Orion system starting in 2019. In this hack, suspected nation-state hackers identified as Nobelium by Microsoft – and often simply referred to as the SolarWinds Hackers by other researchers – gained access to the networks, systems, and data of thousands of SolarWinds customers.

The hackers used a method known as a supply chain attack to insert malicious code into the Orion system. A supply chain attack works by targeting a third party with access to an organization's systems rather than trying to hack the networks directly.

More than 30,000 public and private organizations use the Orion system to manage IT resources, including local, state, and federal agencies. As a result, the hack compromised the data, networks, and systems of thousands when SolarWinds delivered an update to the Orion software that contained this backdoor malware. Through this code, hackers accessed SolarWinds's customer information technology systems, which they could then use to install even more malware to spy on other companies and organizations.

The purpose of this attack is still largely speculated and unknown, but this hack has been a catalyst for rapid and broad change in the cybersecurity and software industries. (Saheed Oladimeji, 2022)

7.4 Software Maintenance and Reuse

The unauthorized removal of systems and network maintenance tools from the supply chain may introduce supply chain risks, such as unauthorized modification, replacement with counterfeit, or malware insertion while the tool is outside of the enterprise's control. (National Institute of Standards and Technology, 2022)

Organizations should verify that code is maintainable. One way to ensure that code is maintainable is to ensure it is compliant with the current organizational software policies. Issues may arise if the code is no longer maintained or supported by the organization.

Software quality plays a significant role in how easily software can be reused. There are obstacles of software quality that impact reuse such as:

- Security – Ensure code is secure. If using pre-existing code, the codebase could potentially be vulnerable to security attacks. If the code does not have a history of being thoroughly tested, it may contain security vulnerabilities that hackers could exploit once your product is launched.
- Reliability – Confirm reliable code by ensuring availability, fault tolerance, and recoverability. When reusing code from a third party, some degree of control is lost since your organization did not build the code in-house. If using a third party's open-source code, then anyone can use and modify the components that were reused at any time, which could change your organization's ability to reuse the code in the future.
- Performance Efficiencies – Ensure code efficiency by improving response times and monitoring processor, memory, and utilization.
- Proprietary – Understand the owner of the code. If the code is proprietary and is not available to

the public, then the owner of the code can change the terms of the license. This can affect how an organization may be allowed to use to use code and software.

- Methodology – Understand the standards and methodology used to develop code. If the code is undocumented or poorly written (e.g., did not follow any coding standards), then it may be more vulnerable.
- Operating environment – Understand the operating environment. The code may be specific to a particular platform or environment that your organization must be capable of supporting.

Special Processes Example:

The enterprise should, whenever possible and practical, use asset location technologies to track systems and components transported between entities across the supply chain, between protected areas, or in storage awaiting implementation, testing, maintenance, or disposal. Methods include Radio Frequency Identification, digital signatures, or blockchains. These technologies help protect against: Diverting the system or component for counterfeit replacement.

7.5 Avoiding Counterfeit Downloads

The following are best practices to help software engineers avoid malicious sites:

- Identify trusted software publishers. Organizations may have an approved supplier list that includes trusted software and sites that may be used. For software downloaded directly from a software publisher (e.g., a commercial vendor or open-source community site), limiting what sites are allowed to only known and trusted publishers can help avoid the use of malicious software. Establish appropriate software supply chain risk management processes to regularly evaluate these software providers.
- Identify trusted download sites. For software libraries, plug-ins, and components, centralized download sites or app stores are common. Only allowing downloads from official app stores (e.g., the Chrome web store or Apple’s App Store) or major software repositories (e.g., Microsoft NuGet, npm, PyPi, or Maven Central) can prevent the installation of counterfeit software. These sites have policies and procedures to prevent malware from being published and to identify and remove malware that sneaks through. However, many tools allow for downloading software from arbitrary sites, some of which may be malicious.
- Only download software when connected to a trusted network, either directly or via a Virtual Private Network. A policy where software should only be downloaded when on a corporate network is best as even home Internet connections can be subverted. DNS hijacking can be more easily accomplished via untrusted wireless networks like those in hotels and coffee shops.
- Only visit download sites using https¹⁷ and only if their certificate is valid. Note that adversaries can obtain their own certificates and use https on typosquatting¹⁸ sites, so this is not a defense against this attack. However, DNS hijacking may send users to sites with invalid certificates.
- Double check that the site name is correct. Make sure to look at the entire URL¹⁹, as adversaries can change just the domain (i.e., doe.com or doe.us instead of doe.gov).
- When searching for a download site, be careful about clicking on advertisements as they could be “malvertisements” bought by an adversary. Using a search result that is not an ad, and verifying the site and its URL are as expected after clicking the result, is recommended.

¹⁷ Hypertext Transfer Protocol Secure

¹⁸ Registration of a common misspelling of another organization's domain as their own

¹⁹ Uniform Resource Locator

Even when on a legitimate site, ensuring the software being downloaded is genuine is important because adversaries will attempt to trick users. This can affect plug-ins and extensions to browsers_(Cimpanu, 2020)_or integrated development environments (Krill, 2023). The following best practices are suggested:

- Double check that the software name is correct to protect against typosquatting. Where possible, looking at the number of downloads of this software and similarly named software may help identify counterfeit packages. The legitimate software will have more downloads.
- Where available, check out recent reviews of the software. Often, other users will warn that a software is malicious or suspect.
- Consider a policy to require the use of software that has a substantial history and significant usage. In other words, allow other software engineers to try out newer software and vet it before using it in US government projects.

7.6 Avoiding Download Interception & Subversion

With the global use of https for secure browsing, the interception and modification of genuine software is much harder. The best practices noted previously such as downloading software from trusted networks and using https sites with valid certificates will help address potential attack vectors.

One additional best practice is to verify software after download. Many software publishers include a checksum of the software that can be used to verify that the software was downloaded correctly. An attempt to alter the download would be detected – unless the adversary also updated this checksum. A more secure verification approach is to verify a digitally signed hash of the software. That signature can be verified, and the hash matched to one of the downloaded software. The most popular build tools (e.g., Gradle, Maven, and NuGet) provide mechanisms to verify signatures for open-source libraries. Some organizations also provide an internally hosted repository (e.g., Sonatype Nexus Repository) that verifies signatures, which means that software engineers can use this repository instead of checking signatures themselves.

Software subversion is one of the most difficult S/CI software scenarios to avoid. In this scenario, typified by the SolarWinds Orion attack discussed above, genuine software downloaded from a legitimate site may be malicious because an adversary inserted malware at the source. Such an attack can occur with software applications and with software libraries (e.g., the coa²⁰ and rc²¹ JavaScript packages). (Aguirre, 2021)

An adversary may present itself via a compromised computer being used by an employee unaware of the infiltration. However, there are some best practices that can be employed such as:

- Identifying trusted software publishers. One useful avenue for commercial software publishers is to request self-attestation that the publisher is following the NIST²² Secure Software Development Framework, as required for Federal agencies by OMB Memo M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*.
- Monitoring software products for security issues and vulnerabilities.

Once software has been downloaded, it still needs to be protected. This is particularly relevant to software that is downloaded and made available for a broader community. Organizations may have internal repositories for third-party libraries or directories containing commonly used software applications. The following are best practices for protecting such repositories:

²⁰ Command Option Argument (COA)

²¹ Run Configuration (RC)

²² National Institute of Standards and Technology (NIST)

- Restrict who can upload or change software in the repository. Some organizations also require that these privileged users use multi-factor authentication and/or a special privileged account to modify such software or administer the repository.
- Verify software after download, as discussed previously.

In addition, steps should be taken to protect any software built by the organization to make sure that an adversary does not subvert it. However, such guidance is outside the scope of this document. Interested readers may wish to review the NIST Secure Software Development Framework (see tools and resources below), which contains many references to additional information regarding software assurance.

7.7 S/CI Prevention Strategy for Software

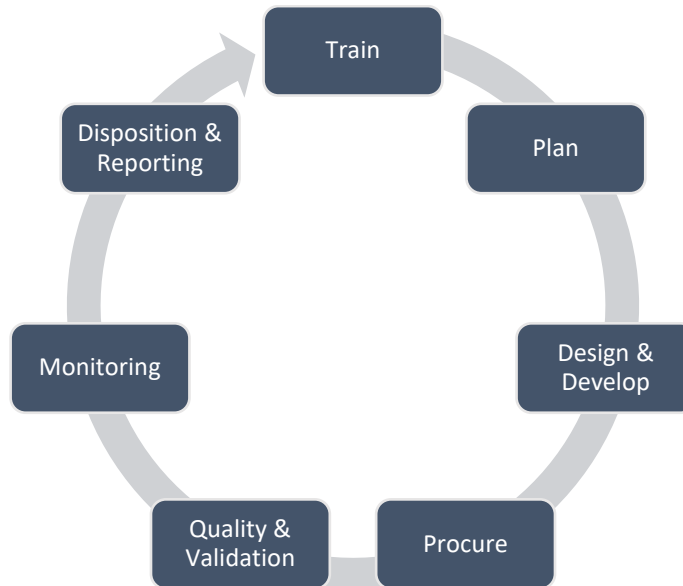


Figure 25: S/CI prevention model for Software

S/CI prevention strategies may use a graded or risk-based approach as discussed in previous sections.

Plan:

Up front planning prevents S/CI, including S/CI software. Planning may start at the project planning stage, uses a defined graded approach, and should consider the following:

1. What major procurements will be conducted during the project?
2. Do any of the major or critical items include ICT/OT or software?
3. What steps, if any, should be included to reduce potential risk of suspect/counterfeit, pirated, or other maliciously tainted ICT, OT, or software?

A key component of planning is to understand potential risks and their controls. The integrity of systems and information is critical component of managing supply chain risks and cybersecurity risks. The insertion of malicious code into a counterfeit product are two primary examples of risks that affect the supply chain and cybersecurity.

Design and Develop:

During the design and development of software, software engineers should consider S/CI as part of the selection and downloading of tools, plug-ins, third-party libraries and components, and any other software used by the project. Before starting development, consider establishing processes for mitigating S/CI risks with software. Such processes should consider defending against the following scenarios:

- Counterfeit software is provided via a site that looks like the genuine website but is not. A common practice for adversaries is to name a site such that it could be mistaken for a legitimate site (i.e., typosquatting). Another option is to hijack a Domain Name System (DNS) such that a user is directed to a site controlled by the adversary rather than the genuine site.
- Counterfeit software with a name that is similar to the genuine software's name is uploaded to an app store, marketplace, code repository or other legitimate site. Typosquatting is common here as well.
- Genuine software is intercepted during download and replaced with counterfeit software.
- Genuine software is subverted at the source with malicious code inserted into it.
- Genuine software may be subverted after installation with malicious code inserted into it.

Quality and Validation:

Restricting the team to only using software from trusted software publishers, identifying practices for ensuring the software downloaded is the correct software, and establishing procedures for monitoring and responding to published vulnerabilities in this software is recommended. Specific best practices are provided below.

Verify the quality of software at intervals during phases such as procurement, receipt, inspection, and installation, as appropriate. Prior to offering software, items, or service for acceptance by the purchaser, the supplier will often verify that the item or service being furnished complies with the procurement requirements. It is also especially important that requirements are specified correctly in procurement documents so that during the quality and validation step at receipt, items will meet intended needs. Often, the requirements and frequency of verification are determined by the procurement documents, applicable specification, code and standard, uniqueness, complexity, application of the software/ item, quantity and frequency of the procurement, and previous quality-related performance of the supplier.

It is important to carefully consider the graded approach to quality and validation of software, and to document the process. For example, documentation might include the necessary steps to perform quality checks and validation of critical items or software.

Monitoring:

Monitor software products for security issues and vulnerabilities. For software libraries²³, a best practice is to use a Software Composition Analysis tool that automatically scans for known vulnerabilities. For other software types, monitoring for vulnerabilities may require regularly checking for new versions to see if they are security-relevant, subscribing to appropriate mailing lists, and monitoring security websites such as Ars Technica, BleepingComputer, and Cybersecurity & Infrastructure Security Agency (CISA) Alerts.

Request a Software Bill of Materials (SBOM) for all software products and monitor them for known vulnerabilities. A SBOM is a listing of all software libraries and components in a software product, so it can be used to identify software that uses a vulnerable library. Creating a repository of SBOMs can be particularly useful to identify software with critical vulnerabilities, such as recently occurred with the log4shell vulnerability. (Berger, 2021)

The log4shell vulnerability, contained in the Log4j 2 library, allowed attackers to exploit a known vulnerability using text messages which could control a computer remotely. The Apache Software Foundation, which publishes the Log4j 2 library, gave the vulnerability a Common Vulnerability Scoring System (CVSS) score of 10 out of 10. The highest-level severity score (i.e., 10), was assigned because of the vulnerability's potential for widespread exploitation, and the ease with which malicious attackers can exploit it. While mitigation evolves and the damage unfolds, the fundamentals of the Log4j vulnerability will not change.

In addition, steps should be taken to protect any software built by the organization to make sure that an adversary does not subvert it. However, such guidance is outside the scope of this document. Interested readers may wish to review the NIST Secure Software Development Framework (reference [Appendix C](#)), which contains many references to additional information regarding software assurance.


Software identified as S/CI should be reported using the organizations S/CI reporting processes. Additional resources and tools for S/CI prevention in software are included in [Appendix C](#).

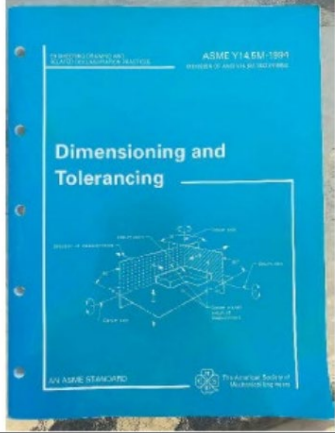
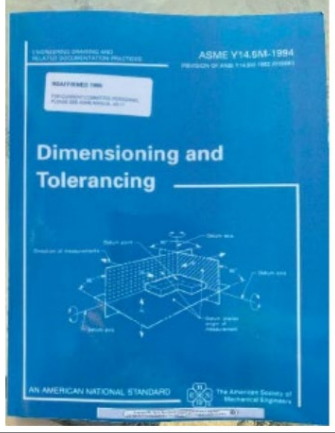
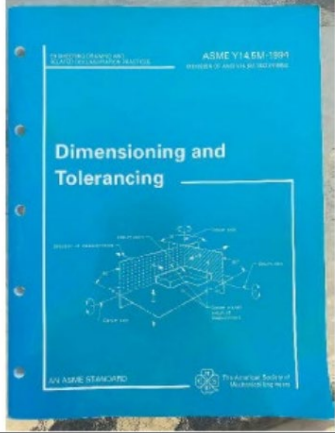
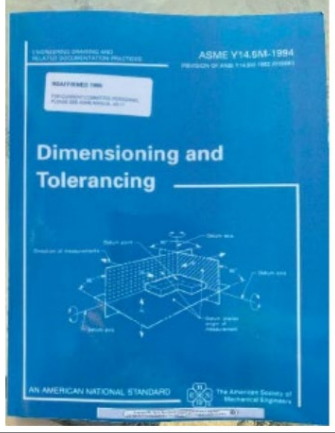
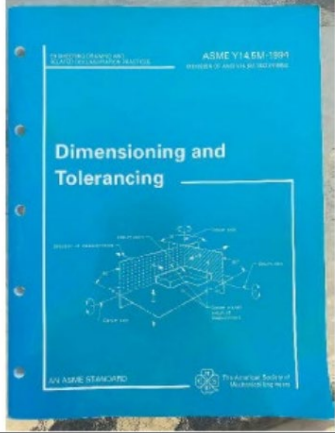
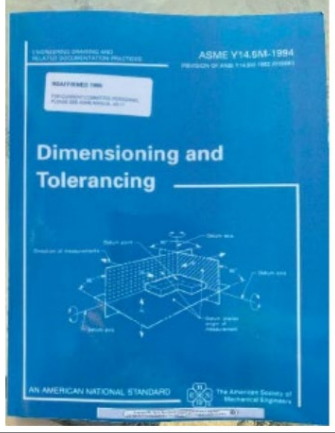
8 Indicators of Suspect Components

8.1 General Suspect/Counterfeit Indicators

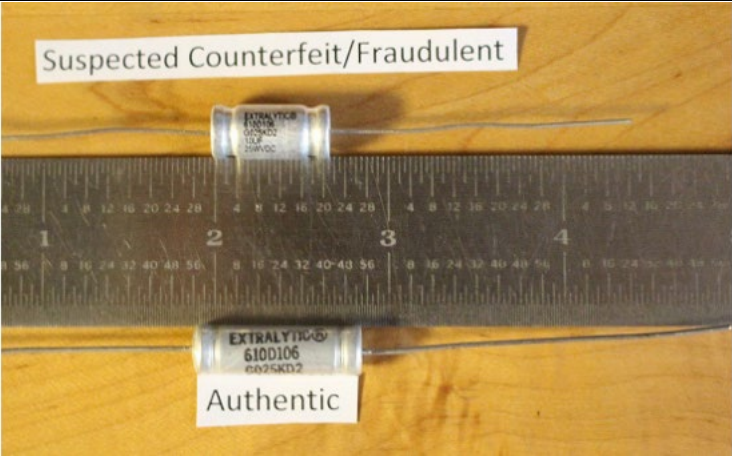
The list includes general and prescriptive indicators of suspect/counterfeit items and components. Items that are identified to have general indications of S/CI should be reported using the organizations S/CI reporting process.

²³ A software library is a suite of data and programming code that is used in software development. Software libraries help developers save time by creating standardized, consistent, and quality code that can be used across multiple projects.

General Indications- Packaging	Examples
<ul style="list-style-type: none"> • Unusual or inadequate (i.e., shipped in plain package with no manufacturer barcode). • Used or damaged parts in new packaging. • Foreign newspapers used as packaging. • Not in a manufacturers box or container. • Package lacks details or lacks critical information. • Package has evidence of tampering. • Package has evidence of being altered or replaced. • Item is packaged for sale in another country and not for sale in the U.S. • Item is not packaged appropriately for the type of item to prevent damage during shipping. 	 <p data-bbox="1019 583 1333 611"><i>Figure 26: Example Tampering</i></p> <p data-bbox="932 646 1393 835">Items may have been visibly tampered with, which may be evident if tamper seals have been broken. Always check tamper-proof seals to verify they are intact.</p>

General Indications- General Appearance	Examples				
<ul style="list-style-type: none"> • Color is different than usual. • Materials used are different than usual. • Item is worn or discolored. • Item appears previously used when ordered as “New.” • There are marks on the item that appear as though it has been opened, tampered with, or repaired. • Missing manufacturer’s standard markings and logos. 	<table border="1" data-bbox="613 989 1401 1440"> <thead> <tr> <th data-bbox="613 989 987 1010">Authentic</th><th data-bbox="987 989 1401 1010">Suspect/Counterfeit</th></tr> </thead> <tbody> <tr> <td data-bbox="613 1010 987 1440">  </td><td data-bbox="987 1010 1401 1440">  </td></tr> </tbody> </table> <p data-bbox="850 1455 1166 1482"><i>Figure 27: General Appearance</i></p> <p data-bbox="597 1503 1409 1730">On the Suspect/Counterfeit book pictured above, the shade of blue of the book was different than the original and authentic version. Numerous other indications were also noted after inspecting the book such as blurred text and image on the front cover, misspellings, and different print on the back cover and binding edge. Reference Data Collection Sheet (DCS) 2446.</p>	Authentic	Suspect/Counterfeit		
Authentic	Suspect/Counterfeit				
					


General Indications- Print and Labels	Examples
<ul style="list-style-type: none"> • Low quality print. • Differences in labels or printing on similar or same lot of items. • Missing or incorrect manufacturers logo. • Inconsistency or conflicting information on tags, labels, docs. • Missing stickers or information on labels nameplates. • Wrong type of print (written vs typed or vice versa). • Labels have signs of being altered. • Expiration or cure dates are missing or incorrect for item. 	<div data-bbox="699 289 1409 640"> </div> <p data-bbox="865 646 1247 674"><i>Figure 28: Example Low Quality Print</i></p> <p data-bbox="691 695 1406 800">Counterfeit (left), Genuine (right). Notice the clarity in print on the genuine device and the fuzzy print on the counterfeit device.</p> <div data-bbox="703 867 1406 1308"> </div> <p data-bbox="808 1320 1300 1348"><i>Figure 29: Example Incorrect Manufacturer Label</i></p> <p data-bbox="691 1379 1419 1526">The blue-and-white colored GE label is authentic. GE does not affix black-and-white labels on boxes for this item nor should the product number be handwritten without any proper GE logo.</p>

General Indications- Configuration	Examples
<ul style="list-style-type: none"> • Items do not meet normal dimensional requirements or are far out of specifications. • Items are missing features (holes, taps, bolts). • Item contact surfaces do not line up correctly. • Inconsistent use of bolts, screws, rivets on same lot of items. • Inconsistent weight or materials used in same lot of items. 	 <p data-bbox="881 772 1133 800"><i>Figure 30: Configuration</i></p> <p data-bbox="597 821 1414 1003">Photograph from EPRI taken during inspection that shows “suspect counterfeit” capacitors and “genuine” capacitors. The OEM later confirmed that the suspected counterfeits were indeed counterfeit and that the “not suspect” capacitors were authentic. (Electric Power Research Institute (EPRI), 2014)</p>

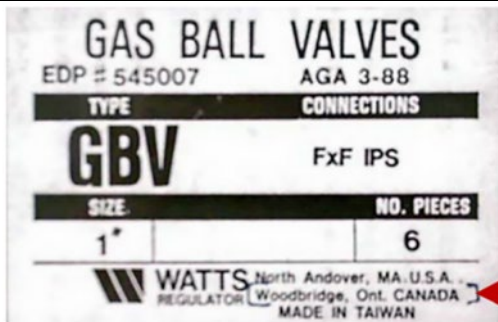
8.2 Indications Hoist, Lifting, and Rigging Equipment

Indications	Examples
<ul style="list-style-type: none"> • Missing manufacturer markings or logos. Many DOE sites implement and require a manufacturers name, trademark, or logo to be on Hooks and shackles (Reference DOE-STD-1090-2020, <i>Hoisting and Rigging</i>). • Worn or used appearance when ordered as new. • Original markings ground off and re-stamped. • Parts identified only as “China” only, or “Korea,” “Mexico,” “Thailand,” “India” (i.e., they are missing manufacturer marking). • Missing or incomplete documentation. • Trademark colored items that are missing logos. 	<div data-bbox="808 317 1382 594"> </div> <p data-bbox="846 600 1344 632"><i>Figure 31: Shackle Missing Manufacturer Marking</i></p> <p data-bbox="773 657 1419 821">The item shackle on the left is missing a manufacturer marking or logo and has a red colored screw pin which is a Crosby trademark. The item on the right is a genuine Crosby shackle with the Crosby logo for comparison.</p> <div data-bbox="865 854 1326 1077"> </div> <p data-bbox="943 1081 1248 1110"><i>Figure 32: Marking Alteration</i></p> <p data-bbox="773 1136 1380 1199">The original markings have been ground off and re-stamped.</p>

8.3 Indications specific to Suspect Piping and Piping Components including mechanical and metal products

Indications	Examples
<ul style="list-style-type: none"> Scratches on component outer surface. Components with no markings. Ground off casting marks. Stamped information where normally cast. Irregular or Inconsistent markings. Pitting or corrosion. External weld or heat indications. Questionable or meaningless numbers. Evidence of hand-made parts. Painted stainless steel. Ferrous metals that are clean and bright. Excess wire brushing or painting. 	 <p><i>Figure 33: Example Suspect Piping</i></p> <p>This photograph is of a new flange that appears to be previously used. There are indications of excess grinding, scratches, and clamp marks on the flange and bolt holes. (Picture are courtesy of Savannah River Site.)</p>

8.4 Indications of Suspect Valves

Indications	Examples
<ul style="list-style-type: none"> Incorrect data on documentation (validate it is correct and within specified parameters). Information on certificates has been altered or corrected without permission. Conflicting information on documentation or test data. 	 <p><i>Figure 34: Suspect WATTS Gas Ball Valve Label</i></p> <p>The WATTS Gas Ball Valve label is S/CI because WATTS does not have a Woodbridge, Ontario, Canada facility.</p>

Indications	Examples
<ul style="list-style-type: none"> • Wrench marks on valve packing glands, nuts, and bolts. • Nameplates attached with screws rather than rivets. • Poor fit between assembled valve parts. • Dirty internals. • Scratched or marred fasteners or packing glands. • Gate valve: gate off-center when viewed through open end. • Fresh sand-blasted appearance of valve bodies, eyebolts, fittings, and stems. • Loose or missing fasteners. • Several types of hand wheels on valves of the same manufacturer. • Some parts (e.g., hand wheels) look newer than rest of the valve. • Improper materials (e.g., bronze nut on a stainless stem). • Post-manufacturing alteration to identification/rating markings. • Indication of previous joint welding. • Excessive standards markings (e.g., Underwriter's Laboratory (UL), Factory Mutual (FM), Canadian Gas Association (CGA), American Gas Association (AGA)). • Valves will not open or close, even when wrench applied. • Substandard valves mixed in with standard valves (substitution). • Excess certification logos (i.e., "UL," "FM," "CGA," "AGA") all on one valve body – not normal, usually will have one or two logos plus ANSI or ASME. 	<p>Suspect WATTS Gas Ball Valve Label. The WATTS Gas Ball Valve label is S/CI because WATTS does not have a Woodbridge, Ontario, Canada facility.</p>  <p><i>Figure 35: Example Used When Ordered New</i></p> <p>Indications on the valve indicate previous use such as clamp marks, scratches, groove in bolt hole, and lack of cleanliness. (Picture courtesy of Savannah River Site.)</p>

8.5 Valve Manufacturer Information

In general, prior to installation, the valves and nameplates should be checked for proper identification to be sure the valve is the proper type and of suitable pressure class. If it is appropriate to do so, actuate the valve to check for damage from shipping and handling and to verify that the valve opens and closes as intended. Do not allow the valve to actuate in a rough manner that could cause damage to seating areas of the valve. Inspect the interior of both the valve and the adjoining pipe for cleanliness, since this a major cause of seat leakage and seat damage if foreign material is in the line. Also, inspect the end connections to be sure that pipe threads and flange faces are free of scratches, nicks, or dents.

Valves produced by the following manufacturers have the following acceptable features. If these features or information is missing, conflicting, or appears to have been altered the item should be considered suspect and information should be verified with the manufacturer to validate if the items are genuine.

If a valve manufacturer identifies discrepancies consistent with indications in the previous section or has data missing or conflicting with information on their products, valves should be reported as S/CIs following the organizations S/CI reporting process.

It is always recommended that datasheets, drawings, or other information is obtained directly from valve manufacturers as this will provide the most comprehensive information as to what should be identified on the valve. In general, a valve may have the following characteristics:

Valve body castings:

- Manufacturer name
- Pressure rating
- Pattern or drawing number
- Heat or melt number
- Grade of steel
- Valve size

Nameplate information:

- Valve serial number or identification number
- Valve class/ operating environment (example: water, oil, gas)
- Valve size and pressure rating

9 Counterfeiting of NRTL Certifications and Symbols

Nationally Recognized Testing Laboratories (NRTLs) are third-party organizations recognized by the Occupational Safety and Health Administration (OSHA) as having the capability to provide product safety testing and certification services to the manufacturers of a wide range of products for use in the American workplace. The testing and certifications are based on product safety standards developed by U.S.-based standards developing organizations and often issued by ANSI.

S/CI coordinators should verify with the NRTL if the markings are correct or genuine. NRTL's maintain strict traceability to their issued certifications and symbols.

For a current listing of OSHA recognized NRTLs and testing locations that operate under the program go [here](#)²⁴.

NRTL approved certification means that the NRTL determined that the product met the requirements of an appropriate consensus-based product safety standard either by successfully evaluating the product itself or by verifying that a contract laboratory has done so; and the NRTL has certified that the product met the requirements of the product safety standard.

NRTL regulations are contained in 29 CFR 1910.7. Many products "approval" requirements are found in OSHA's standards (29 CFR Parts 1910, 1915, 1918, and 1926). NRTL testing and certification is required for many types of products, including:

- Electrical equipment;
- Fire detecting and extinguishing equipment;
- Liquefied Petroleum Gas utilization equipment; and
- Equipment to be used in hazardous locations.

More products requiring NRTL approval can be located [here](#)²⁵.

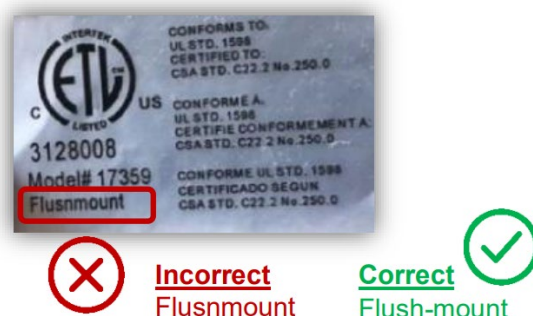


Figure 36: Suspect/Counterfeit NRTL Sticker (TIC, 2020)

²⁴ <http://www.osha.gov/dts/otpc/nrtl/>

²⁵ <https://www.osha.gov/nationally-recognized-testing-laboratory-program/products-requiring-approval>

10 Suspect/Counterfeit & Fraudulent Documentation and Certification

Manufacturers and suppliers that make the intentional decision to misrepresent, alter, forge, or otherwise create fraudulent and counterfeit documentation and/or certification marks are putting monetary gain above the safety and welfare of people. There are various indications to determine if documentation, such as test certificates, is genuine. Visually examining test documentation, certification papers, or labeling may provide enough verification to determine if it is genuine. Accredited certifications typically use specific and consistent formats for their test and certification reports. Manufacturers often will go to great lengths to ensure that labeling, certification marks, and documentation is correct. These efforts are intended to increase the difficulty for counterfeiters to falsify documents. Familiarity with a company's official documents and labels will help to identify when there is a deviation or if documents may be fraudulent.

General tips to avoid and detect S/CI and fraudulent documentation:

- 1) Use reputable sources for materials;
- 2) Verify test reports with manufacturer's if obtaining reports through third parties;
- 3) Verify consistency in information and that it is correct for the manufacturer or supplier;
- 4) Verify certificates are signed by individuals who have the authority to sign the document (e.g., was a test signed by the company's janitor or their Quality Control Inspector?); and
- 5) Verify NRTL or other accreditations through accreditation websites. For instance, if a product is Underwriters Laboratories listed, it will have a UL listing number, and the manufacturer and part or model number will be listed in the database. Many NRTLs have ways to verify and lookup if a product or listing is genuine either by number, manufacturer, product number, etc. They also typically have departments that specialize in addressing concerns on counterfeit mark questions.

A useful acronym that helps to remember the indications of fraudulent documentation is i-FRAUDS, which stands for:

- I. Information
- F. Font
- R. Reproduction
- A. Alteration
- U. Used
- D. Dates/Numerations
- S. Signature

See the subsections below for a further description on each of the letters in the acronym i-FRAUDS. Discrepancies that are identified in documentation should be further inspected and reported using the organizations S/CI Reporting Processes.

10.1 Information

Information presented in a product's document(s) should match the product itself and be consistent. Inconsistencies in the information are red flags of falsified documents. Inspections may include comparisons of products, documentation, packaging, and labels to verify that they are all consistent. This could include verifying consistent serialization, specification numeration, or other identifying data. If there are inconsistencies, these should be verified with the manufacturer. If items were procured directly from the manufacturer and the manufacturers processes are in question, then the items should be reported using the appropriate S/CI reporting processes discussed in the reporting section of this handbook.

10.2 Font

If there are non-logical changes in font size, spacing, or consistency in font type usage these are red flags of potential fraudulent documentation. It would be *logical* to see some changes in fonts where it makes sense such as in titles of documents, section headings, or signature lines. Fonts should not change in the middle of a word, which would be considered *not logical*.

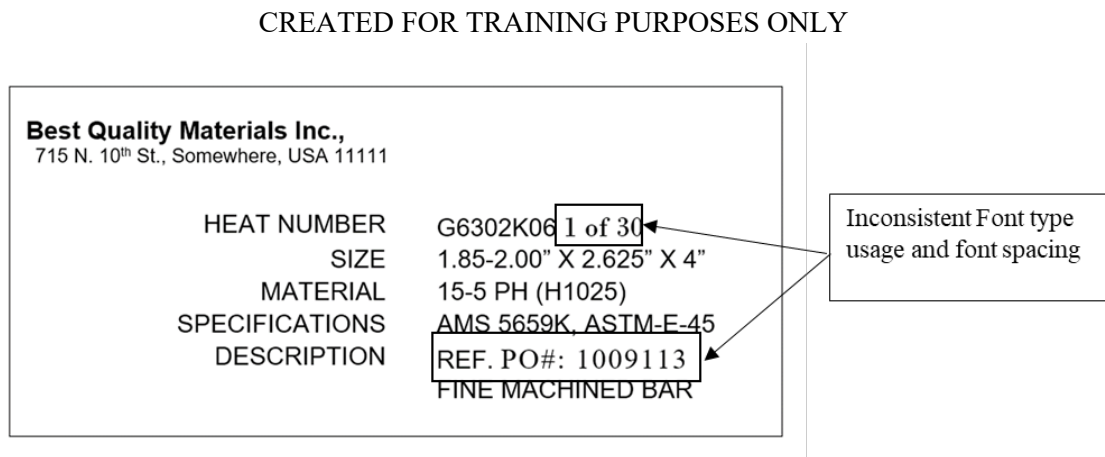


Figure 37: Font Indication Example

10.3 Reproduction

Documentation may be reproduced without authorization. Reproduced documentation may include the same or original information – such as serial, batch, or item numbers. This information may be expected to be different when purchasing multiple items but may appear to be the same. Documentation that does not have an original signature or has duplication of the same signature, could be an indication of unauthorized reproduction. With advances in copier technology, unauthorized reproductions are harder to spot and documentation such as certificates of conformance or other confirmatory documents should be examined carefully.

10.4 Alteration

Forgery—which is when a person creates a false document or alters a genuine document, certification, or other legal document with the intent to deceive or defraud—is a crime in most countries, including the U.S. Figure 38 is an indication of alteration in a document. Some alterations are more obvious than others such as the below where all or parts of the document has been removed, replaced, or copied over.

CREATED FOR TRAINING PURPOSES ONLY

Your Trusted Source
Honest Metals, Inc.

1815 N. Sample St.
Somewhere USA, 11111

CHEMICAL ANALYSIS

Specimen Heat #	C	Mn	Si	P	S	Cr	Ni	Cu	Mn
G123G123-1	.50%	.47%	.30%	.023%	.002%	14.56%	4.50%	2.20%	.15%

Notice the line under the .50% that indicates pasting of information over original information

SPECIMEN ID: 1

HEAT NUMBER: G123G123-1

METHOD OF ANALYSIS: XRF

TEST TEMPERATURE: ROOM TEMPERATURE 70°F / Humidity less than 50%

Font inconsistencies and information is askew and has indications of being copied over or pasted into this section

Information is handwritten into the document without a signature or initial and date. It is unclear who entered the information and information may be important to the test or other specified requirements.

Figure 38: Alteration Example

10.5 Used

Items for aging facilities may be ordered to be new. However, with the increasing age of DOE facilities and equipment, it is becoming increasingly difficult to procure and receive new parts and equipment. This can lead to vendors providing documentation that identifies the item as *new* when there is evidence the item has been previously used. Whether or not the item was procured for an older facility, if documentation identifies items as *new* when there is an indication of previous use this is an indicator of potential fraud. This documentation should be held as “suspect” and investigated further. In addition to this, the item should be further inspected or tested to verify if the item meets requirements for what was specified in the contract or order documents.

10.6 Dates & Numerations

An indication of potential fraud may be dates and numeration inconsistencies. For instance, documentation that is intended for a specific serialized product. The product may also be marked with a serial number. It is vital that the serial number on the product is compared against the documentation to verify:

- a. Product type;
- b. Model and/or part number; and
- c. Serial numbers are the same.

It is also important to verify dates on materials in which traceability was maintained and documents and certificates were provided from the foundry or original manufacturers through distributors. Date inconsistencies are a red flag of potential fraud.

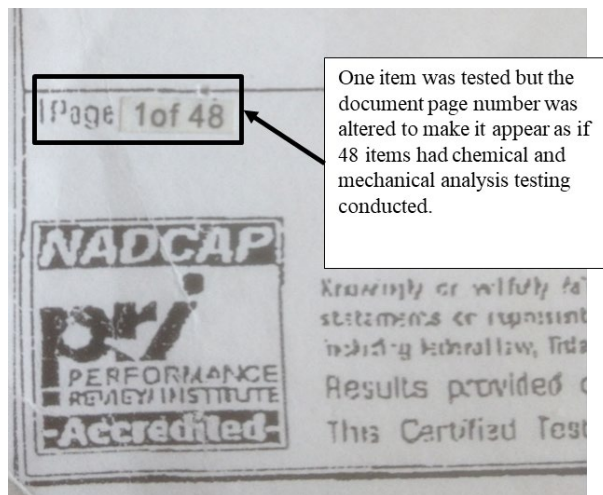


Figure 39: Dates and Numeration Example

10.7 Signatures

Validating signatures is not always possible without complex instruments, but there are still methods that can be employed when visually examining a document or Portable Document Format (PDF) file:

Potential red flags are:

- 1) Signatures are missing.
- 2) Digital signatures do not employ a secure signature to verify authenticity or singular use by individuals (indicates the document may have non-secure signatures that could be used by anyone).
- 3) Digital signatures were removed (indicates the document may have been edited); and
- 4) Document properties suggest it was edited after it was signed.

CREATED FOR TRAINING PURPOSES ONLY

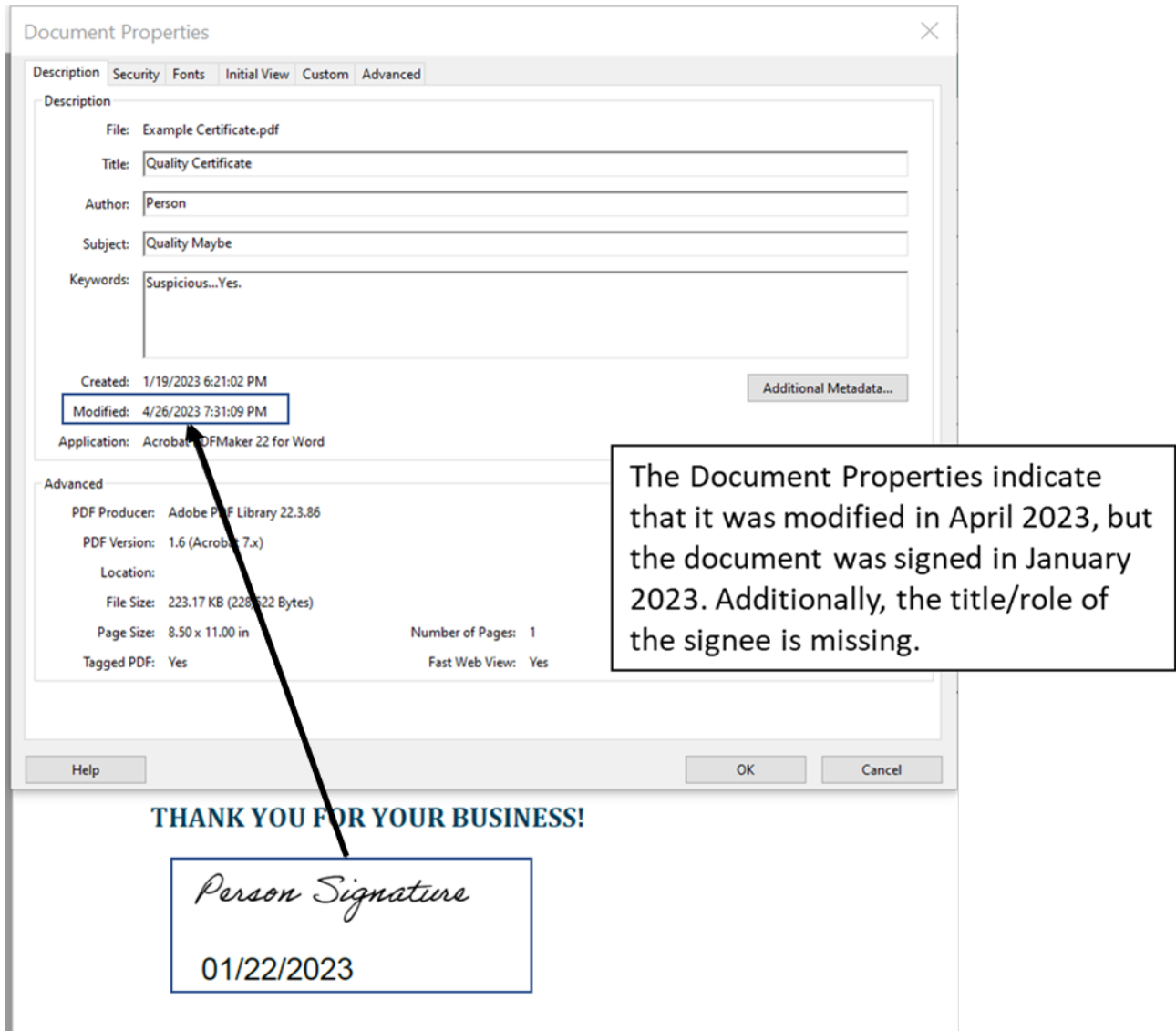


Figure 40: Signature Example

11 References

Current and draft directives and accompanying guidance relevant to S/CI can be found [here](#)²⁶.

- Aguirre, J. (2021). NPM Hijackers at It Again: Popular ‘coa’ and ‘rc’ Open Source Libraries Taken Over to Spread Malware. Retrieved from <https://blog.sonatype.com/npm-hijackers-at-it-again-popular-coa-and-rc-open-source-libraries-taken-over-to-spread-malware>.
- ANSI/ASQC Z1.4-2008 (2008), Sampling Procedures and Tables for Inspection by Attributes.
- ASME NQA-1 (2022), Quality Assurance Requirements for Nuclear Facility Applications.
- American Society of Testing Materials, ASTM A193/A193M (2023), Standard Specification for Alloy- Steel and Stainless-Steel Bolting for High Temperature or High-Pressure Service and Other Special Purpose Applications.
- AS5553D (2022), Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts, Avoidance, Detection, Mitigation, and Disposition.
- AS6171A (2018), Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts.
- Berger, A. (2021, 12 17). What is Log4Shell? The Log4j vulnerability explained (and what to do about it). DynaTrace. Retrieved from <https://www.dynatrace.com/news/blog/what-is-log4shell/>
- Cimpanu, C. (2020). Mozilla has banned nearly 200 malicious Firefox add-ons over the last two weeks. ZDNet. Retrieved from <https://www.zdnet.com/article/mozilla-has-banned-nearly-200-malicious-firefox-add-ons-over-the-last-two-weeks/>.
- Code of Federal Regulations, 10 CFR 830 (2020), Nuclear Safety Management, Definitions.
- Code of Federal Regulations, 29 CFR 1910.7 (1974), Occupational Safety and Health, Definition and Requirements for a Nationally Recognized Testing Laboratory.
- DOE Acquisition Regulation Acquisition Letter 95-08 (1995).
- DOE-STD-1090-2020, Hoisting and Rigging.
- DOE Guide 414.1-2B (2013), Quality Assurance Guide.
- DOE Order 232.2A (2019), Occurrence Reporting and Processing of Operations Information.
- DOE Order 252.1A (2011), DOE Technical Standards Program.
- DOE Order 414.1D, chg. 2 (2020), Quality Assurance.
- Electric Power Research Institute (EPRI)/NP-5638 (1988) Guidelines for Preparing Specifications for Nuclear Power Plants.
- Federal Acquisition Streamlining Act of 1994.
- EPRI NP- 5652 (2014), Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications.
- EPRI NP-6406 (2006), Guidelines for the Technical Evaluation of Replacement Items in Nuclear Power Plant.

²⁶ DOE Directives website: <http://www.directives.doe.gov>

- Harold “Woody” Hewett, Electro-Comp Services, Inc. (2010). Methods Used in the Detection of counterfeit Electronic Components. Clearwater, FL, USA: SMTA Int’l. Retrieved from https://www.circuitinsight.com/pdf/methods_detection_counterfeit_components_smta.pdf.
 - Krill, P. (2023). Attackers could easily spoof popular Visual Studio Code extensions and trick developers into downloading them, Aqua Nautilus researchers report. InfoWorld. Retrieved from <https://www.infoworld.com/article/3685542/researchers-warn-of-malicious-visual-studio-code-extensions.html>.
 - International Atomic Energy Agency, IAEA-TECDOC-1169 (2000), Managing Suspect and Counterfeit Items in the Nuclear Industry.
International Business Machines Corporation, Petitioner v. Lufkin Industries, LLC (2018), Respondent, 17-0666 (Supreme Court of Texas). Retrieved from <https://www.txcourts.gov/media/1443741/170666.pdf>.
 - Independent Distributors of Electronics Association (IDEA) Standard 1010-B (2011), Acceptability of Electronic Components Distributed in the Open Market.
 - International Data Corporation (IDC). (2013). The Dangerous World of Counterfeit and Pirated Software. Framingham: Microsoft Corporation. Retrieved from <https://news.microsoft.com/download/presskits/antipiracy/docs/IDC030513.pdf>.
- Newman, L. H. (2020). The Anatomy of a Cisco Counterfeit Shows Its Dangerous Potential. Wired, 1-2. Retrieved from <https://www.wired.com/story/counterfeit-cisco-switch-teardown/>.
- <https://www.nist.gov/standardsgov/compliance-faqs-fastener-quality-act-fqa>
 - OECD and European Union Intellectual Property Office. (2022). Dangerous Fakes: Trade in Counterfeit Goods that Pose Health, Safety and Environmental Risks. Illicit Trade. Paris, France. Doi: <https://doi.org/10.1787/117e352b-en>.
 - Office of Management and Budget (OMB) Policy Letter 91-3 (1991), Reporting Nonconforming Products.
 - OMB Memo M-22-18 (2022), Enhancing the Security of the Software Supply Chain through Secure Software Development Practices.
 - Saheed Oladimeji, S. M. (2022). SolarWinds hack explained: Everything you need to know. Retrieved from WhatIs.com TechTarget: <https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>.
 - Sharma, A. (2021). Popular 'coa' NPM library hijacked to steal user passwords. Retrieved from <https://www.bleepingcomputer.com/news/security/popular-coa-npm-library-hijacked-to-steal-user-passwords/>.
 - Society of Automotive Engineers, SAE AS9120B (2016), Quality Management Systems-Requirements for Aviation, Space, and Defense Distributors.
 - The Software Alliance (BSA). (2018). Software Management: Security Imperative, Business Opportunity. DC: The Software Alliance/ BSA. Retrieved from https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf#page=4.
 - Sokoloff, L (2006). Thread Repair in the Aluminum Head of Mercedes-Benz Ponton Engines. Retrieved from <http://www.mbzponton.org/valueadded/maintenance/thread/repair.htm>.
 - TIC Council Anti-Counterfeiting Committee (2020) Falsified: Test Reports & Certificates: Identification and Impact of Counterfeit Test Reports and Certificates in the Global Marketplace.

Appendix A – Suspect/Counterfeit and Defective Fastener Inspection

The DOE Suspect/Counterfeit and Defective Fastener Inspection document is available [here](#)²⁷.

Legacy Fastener Headmark List: Manufactured Prior to 1999

All fasteners listed below that are identified as having been manufactured prior to 1999 and as a best practice should be considered suspect/counterfeit or defective and replaced without any further testing. Additional verification may be needed or conducted on fasteners prior to use. This may be especially true if a site is unsure if a fastener is considered a “legacy fastener” produced prior to 1999. Some of these listed fasteners may still be found in distributors’ stock, inventories, or other points of sale and therefore may be provided in more recent procurements. It may be necessary to determine the date of manufacture, obtain CMTRs, C of Cs, or other documentation of some of these fasteners to confirm they are not defective, suspect, counterfeit, or fraudulent. Additionally, if the fastener is determined to be one of these legacy fasteners and will be used, all of the following should be completed:

- 1) Validation or testing to ensure the fasteners meet requirements.
- 2) Marking or tagging of the fasteners.
- 3) Documentation to demonstrate that testing/validation has occurred; and
- 4) Documentation maintained until the fasteners are removed from service.




















Grade A 325			Grade 5		Grade 8.2
			 		
Type 1	Type 2	Type 3			
Grade 8					
<div><div></div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div></div>					
Note: Hollow Triangle (Greater than 1/2-inch diameter)					

Figure 41: Legacy Fastener List

²⁷ <https://www.energy.gov/ehss/articles/suspect-counterfeit-defective-fastener-inspection>

Marking	Manufacturer	Country
A	Asahi Mfg.	Japan
E	Daiei	Japan
FM	Fastener Co	Japan
H	Hinomoto Metal	Japan
J	Jinn Her	Taiwan
KS	Kosaka Kogyo	Japan
KY	Kyoei Mfg	Japan
M	Minamida Sieybo	Japan
MS	Minato Kogyo	Japan
NF	Nippon Fasteners	Japan
RT	Takai Ltd.	Japan
UNY	Unytite	Japan
Hollow Triangle	Infasco	Canada, Taiwan, Japan

Table 5: Legacy Fastener List Codes that correspond to Figure 41

Appendix A-1 Current Suspect Fastener Headmark List: All Fasteners 1999 to Current

High strength fasteners (e.g., tensile strength of SAE grade 5 or around 120,000 psi or greater) that are missing manufacturer markings, such as the examples shown below, should be considered “suspect.” Further evaluation should be conducted to conclude if they are substandard, defective, or counterfeit. NOTE: this is not a comprehensive list of “suspect” high-strength fasteners.

Grade 5	Grade 8
	
Metric 8.8	Metric 10.9
	

Table 6: High Strength Fastener Examples

Fasteners that are marked with dual non-compatible standards or conflicting information should be treated as defective. Note there may be instances where dual markings are acceptable and are a part of normal manufacturer processes. See below for dual non-compatible marking examples.

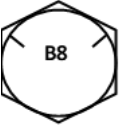

18-8 Stainless steel dual marked as “B8”	F593 marked as “B8”- there is no “B8” material type in this standard
	

Table 7: Non-Compatible Standard Example

Appendix A-2 Badge Reminders: Suspect/Counterfeit and Defective Item Fastener Inspection

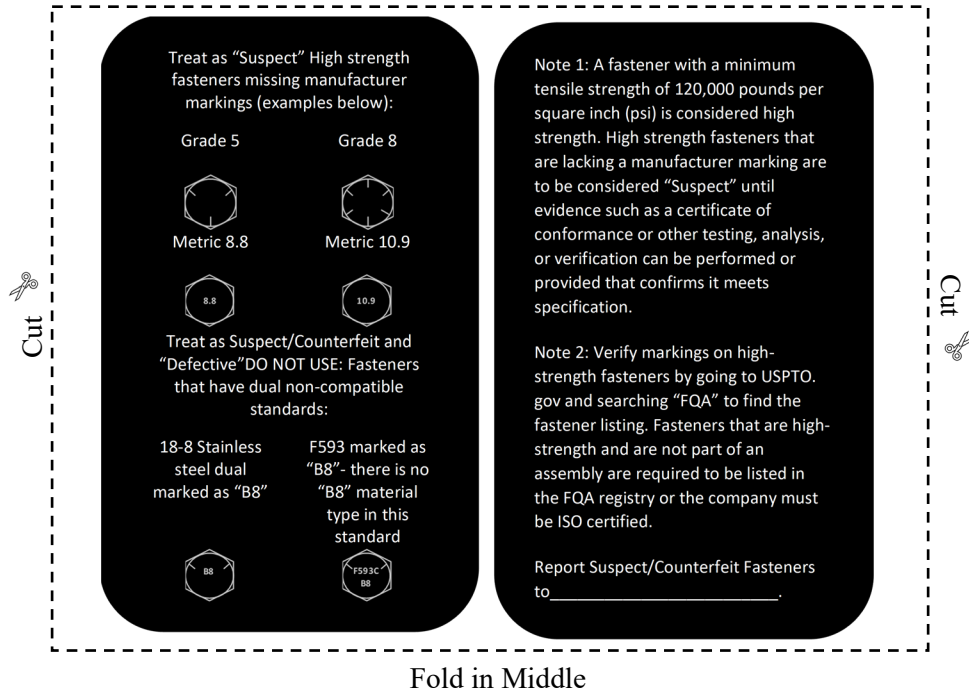


Figure 42: Badge Reminder

Appendix B – Other Information Related to S/CI

Resource information on NRC's initiative to prevent the intrusion of counterfeit, fraudulent, and suspect items (CFSI) into NRC regulated facilities can be found at the following websites:

- *Actions to Improve the Detection of Counterfeit and Fraudulently Marked Products (Generic Letter 89-02)* GL89002, <https://www.nrc.gov/reading-rm/doc-collections/gen-comm/gen-letters/1989/gl89002.html>.
- *Counterfeit, Fraudulent, Suspect Items (CFSI) Project Update*, <https://www.nrc.gov/docs/ML1222/ML12227A917.pdf>
- 2012 Vendor Oversight Workshop, <https://www.nrc.gov/reactors/new-reactors/how-we-regulate/oversight/quality-assurance/vendor-oversight/past/2012/index.html>
- *Counterfeit Parts Supplied to Nuclear Power Plants (Information Notice 2008-04)* IN2008-04, <https://www.nrc.gov/docs/ML0807/ML080790266.pdf>
- *Licensee Commercial-Grade Procurement and Dedication Programs (Generic Letter 91-05)*, GL91005g, <https://www.nrc.gov/docs/ML0311/ML031140508.pdf>
- SECY-11-0154, *An Agency wide Approach to Counterfeit, Fraudulent, and Suspect Items*, <https://www.nrc.gov/docs/ML0311/ML031140508.pdf>
- *Staff Review of Counterfeit, Fraudulent, and Suspect Items (CFSI)*, ML112130293, <https://www.nrc.gov/docs/ML1204/ML120440268.pdf>
- *U.S. Patent and Trademark Office Fastener Insignia Register Active Insignias*, <https://www.uspto.gov/trademarks/laws/fastener-quality-act-fqa/fastener-quality-act-fqa>

Appendix C – Resources

C-1 Internal DOE Resources

Below is a list of internal to DOE resources for S/CI:

- **Department of Energy**
Office of Environment, Health, Safety and Security Office of Corporate Safety Analysis, EHSS-23, Email: counterfeit@hq.doe.gov. DOE Germantown 19901 Germantown Road Germantown, Maryland 20874.
- **DOE OPEXShare**
DOE builds a resilient safety and quality program through the use and sharing of operating experience in accordance with DOE O 210.2A, DOE Corporate Operating Experience Program. Sites should participate and add information as much as reasonably possible to share lessons learned, best practices, and other valuable operating experience information that may relate to suspect/counterfeit items prevention, detection, program practices into DOE OPEXShare at <https://doeopexshare.doe.gov/>. Online registration is required.
- **DOE Organizational Excellence (OrgEx)**
The DOE OrgEx website is a collaborative platform used for transferring relevant knowledge throughout the DOE. OrgEx enables DOE to become agile and effective in order to advance the national, economic, and energy security of the United States and to promote scientific and technological innovation in support of our mission. <https://orgex.energy.gov/>.
- **DOE Occurrence Reporting and Processing System (ORPS)**
The Department of Energy's Occurrence Reporting Program provides timely notification to the DOE complex of events that could adversely affect public or DOE worker health and safety, the environment, national security, DOE's safeguards, and security interests, functioning of DOE facilities, or the Department's reputation. This includes certain suspect/counterfeit items that meet the criteria stated in DOE O 232.2A, Occurrence Reporting and Processing of Operations Information. <https://www.energy.gov/ehss/occurrence-reporting-and-processing-system>.
- **Suspect/Counterfeit and Defective Items (S/CI-DI) websites:**
 - S/CI-DI Webpage (S/CI Coordinator Access Only): To request access, go to <https://reportspw1.doe.gov/sci/register>.
 - The DOE Office of ES&H Reporting and Analysis (EHSS-23) maintains a website for relevant S/CI information and related reference documents at: <https://energy.gov/ehss/policy-guidance-reports/databases/suspectcounterfeit-and-defective-items>.
 - S/CI Webpage on Powerpedia (available to DOE Federal and Contractors) to access go to https://powerpedia.energy.gov/wiki/Suspect_or_Counterfeit_Items_and_Defective_Items.

C-2 External to DOE Resources

Below is a list of some key industry resources for S/CI information or to aid in prevention:

- **Automotive Electronics Council (AEC)** (<http://www.aecouncil.com>)
AEC-Q101, Failure Mechanism Based Stress Test Qualification For Discrete Semiconductors.
- **American National Standards Institute (ANSI)** reference <https://ansi.org/>
ANSI works in close collaboration with stakeholders from industry and government to identify and develop standards- and conformance-based solutions to national and global priorities.
- **American Society for Testing and Materials (ASTM)** reference <https://www.astm.org/>
ASTM is committed to serving global societal needs, by positively impacting public health and safety, consumer confidence and overall quality of life.
- **American Society of Mechanical Engineers (ASME)** reference <https://www.asme.org/>
ASME is a not-for-profit professional organization that enables collaboration, knowledge sharing and skill development across all engineering disciplines, while promoting the vital role of the engineer in society.
- **Department of Commerce National Institute of Standards and Technology** reference <https://www.commerce.gov/bureaus-and-offices/nist>
The National Institute of Standards and Technology (NIST) was founded in 1901 and is part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. NIST measurements support the smallest of technologies to the largest and most complex of human-made creations—from nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair up to earthquake-resistant skyscrapers and global communication networks.
- **Destructive Physical Analysis Resource**
 - SSQ-25000, *Destructive Physical Analysis Testing Specification for the Space Station Program*
- **Government-Industry Data Exchange Program (GIDEP)** reference <https://www.gidep.org/>
GIDEP is a cooperative activity between government and industry participants seeking to reduce or eliminate expenditures of resources by sharing technical information essential during research, design, development, production, and operational phases of the life cycle of systems, facilities, and equipment.
- **Industrial Fasteners Institute (IFI)** reference <https://www.indfast.org/>
IFI is committed to being the leader in providing fastener technology leadership. IFI members receive technical support in product design, manufacturing practices, quality assurance, and standards development and interpretation.
- **Joint Electron Device Engineering Council (JEDEC)** reference <https://www.jedec.org/>
JEDEC is the global leader in developing open standards for the microelectronics industry, with more than 3,000 volunteers representing over 350 member companies.
 - JESD22-B101, External Visual

- JESD22-B107, Marking Permanency
- JESD22-A104, Temperature Cycling
- JESD22-A113, Preconditioning of Non-hermetic Surface Mount Devices Prior to Reliability Testing
- J-STD-020, Joint IPC/JEDEC Standard Moisture/Reflow Sensitivity Classification for Non-hermetic Surface Mount Devices (SMDs)
- J-STD-035, Joint IPC/JEDEC Standard for Acoustic Microscopy for Non-Hermetic Encapsulated Electronic Devices
- **The Electronic Resellers Association International (www.era.com)**
The ERAI provides its global members with supply chain risk mitigation solutions, including the world's largest searchable database of counterfeit components and high-risk suppliers.
- **The Independent Distributors of Electronics Association (IDEA) reference <https://idofea.org/>**
IDEA employs a comprehensive approach that focuses on programs and best practices that establish and increase quality standards, provide industry with a conduit to improve the access to and sharing of relevant knowledge, and advance industry ethics and integrity.
- **The International Anti-Counterfeiting Coalition (IACC) (www.iacc.org.)**
The IACC brings together thousands of people from various industries, educational institutions, and government at all levels to share with and learn from each other on key strategies and practical solutions to addressing counterfeiting and piracy. IACC members benefit from a global community.
- **The U.S. Patent and Trademark Office (USPTO) reference <https://www.uspto.gov/>**
The USPTO provides numerous resources that may aid those performing inspections on products including resources on the Fastener Quality Act and current insignia registry and a Trademark Electronic Search System (TESS) which can be used to validate registered manufacturer markings, location of manufacturers, manufacturer contacts, and other vital information that may not be easily discoverable. <https://tmsearch.uspto.gov/>.
- **TrustedParts.com (<https://www.trustedparts.com>)**
TrustedParts.com was created by the Electronic Components Industry Association (ECIA) in collaboration with participating distributors as a free service to support the authorized electronic components industry by giving users access to aggregated price and availability data for genuine parts from only authorized sources. It is still recommended that DOE sites review, assess, and determine if sources meet their specific project needs and criteria using a graded approach.
- **IDEA-STD-1010, *Acceptability of Electronic Components Distributed in the Open Market***
- **Society Automotive Engineers (SAE) reference <https://www.sae.org/>**
SAE International is a global association of more than 128,000 engineers and related technical experts in the aerospace, automotive and commercial-vehicle industries. Our core competencies are life-long learning and voluntary consensus standards development. SAE has numerous counterfeit prevention and detection standards which include:

- AIR6273, Terms, Definitions, and Acronyms Counterfeit Materiel or Electrical, Electronic, and Electromechanical Parts.
- ARP6178, Fraudulent/Counterfeit Electronic Parts, Toll for Risk Assessment of Distributors.
- ARP6328, Guideline for Development of Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Systems.
- AS5553D, Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts, Avoidance, Detection, Mitigation, and Disposition.
- AS6081A, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition-Independent Distribution.
- AS6171A, Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts which can also be broken down into the following test method processes and procedures:
 - AS6171/1, Suspect/Counterfeit Test Evaluation Method.
 - AS6171/2A Techniques for Suspect/Counterfeit EEE Parts Detection by External Visual Inspection, Remarking and Resurfacing, and Surface Texture Analysis Using SEM Test Methods.
 - AS6171/3, Techniques for Suspect/Counterfeit EEE Parts Detection by X-Ray Fluorescence Test Methods.
 - AS6171/4, Techniques for Suspect/Counterfeit EEE Parts Detection by Delid/Decapsulation Physical Analysis Test Methods.
 - AS6171/5, Techniques for Suspect/Counterfeit EEE Parts Detection by Radiological Test Methods.
 - AS6171/6, Techniques for Suspect/Counterfeit EEE Parts Detection by Acoustic Microscopy (AM) Test Methods.
 - AS6171/7, Techniques for Suspect/Counterfeit EEE Parts Detection by Electrical Test Methods.
 - AS6171/8, Techniques for Suspect/Counterfeit EEE Parts Detection by Raman Spectroscopy Test Methods.
 - AS6171/9, Techniques for Suspect/Counterfeit EEE Parts Detection by Fourier Transform Infrared Spectroscopy (FTIR) Test Methods.
 - AS6171/10, Techniques for Suspect/Counterfeit EEE Parts Detection by Thermogravimetric Analysis (TGA) Test Methods.
 - AS6171/11, Techniques for Suspect/Counterfeit EEE Parts Detection by Design Recovery Test Methods.
- AS6174A, Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel.
- AS6462C, AS5553C, Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts, Avoidance, Detection, Mitigation, and Disposition Verification Criteria.

- AS6810 Requirements for Accreditation Bodies when Accrediting Test Laboratories Performing Detection of Suspect/Counterfeit in Accordance with AS6171 General Requirements and the Associated Test Methods.
- AS6832, Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Fasteners.
- AS6886, Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Refrigerant.
- AS6496, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition- Authorized/Franchised Distribution.
- **Software Resources:**
 - NIST Secure Software Development Framework: <https://csrc.nist.gov/Projects/ssdf>.
 - OMB Memo M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices: <https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf>.
 - Software Composition Analysis: https://owasp.org/www-community/Component_Analysis.
 - Sonatype Nexus Repository: <https://www.sonatype.com/products/nexus-repository>.
- **Underwriters Laboratory reference <https://www.ul.com/>**
UL Solutions helps companies to demonstrate safety, enhance sustainability, strengthen security, deliver quality, manage risk, and achieve regulatory compliance.
- **United States Nuclear Regulatory Commission reference <https://www.nrc.gov/>**
The U.S. Nuclear Regulatory Commission (NRC) was created as an independent agency by Congress in 1974 to ensure the safe use of radioactive materials for beneficial civilian purposes while protecting people and the environment. The NRC regulates commercial nuclear power plants and other uses of nuclear materials, such as in nuclear medicine, through licensing, inspection, and enforcement of its requirements.