Operating Experience Summary

OES 2025-07 July 2025

SUSPECT/COUNTERFEIT ITEMS REPORTING DATA

Purpose

This Operating Experience Summary (OES) provides an overview of reporting data from the Department of Energy (DOE) Suspect/Counterfeit Items (S/CI) program. This OES was developed by the Office of ES&H Reporting & Analysis (EHSS-23) to review data trends, impacts of S/CIs at the DOE, and offer potential recommendations for improving S/CI reporting to support early identification and prevention in the future.

Recent Impacts of Suspect/Counterfeit Items

Suspect/Counterfeit Items (S/CIs), defined in DOE Order 414.1E (DOE O 414.1E), *Quality Assurance*, may be poor quality, misrepresented, fraudulent, tampered, or even maliciously tainted items that could make their way into critical safety or national security programs or projects. The results of inadvertently installing S/CIs can be varied, but impactful and disruptive to the mission. An increased prevalence of fraud in the marketplace and supply chain makes this issue more compelling to address.

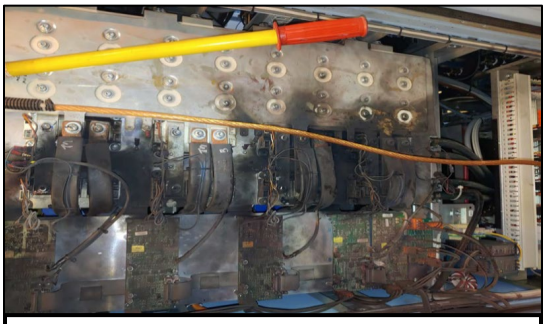

Figure 1: $1.8 Million Cabinet Arc Incident

MS Hi-Tech[1]

Between 2017 and 2020 the owner of M.S, Hi-Tech bribed a DOE Procurement Officer in exchange for $969,000 in DOE contracts. Some of the components ignited, causing more than $1.8 Million in fire damage to a DOE facility. The components, Insulated Gate Bipolar Transistors (IGBTs), were later identified as suspect/counterfeit. **Figure 1** shows damage from the cabinet arc incident reported into the Occurrence Reporting and Processing System (ORPS).

Figure 2: Aventura made $112 million selling Chinese equipment to US Military officials (**link**)

Aventura Technologies[2]

Between 2006 and 2019, Aventura sold Chinese-made surveillance equipment to the US government, while falsely claiming the products were made in the United States – a scheme that directly undermined national security. Court documents say the fraud resulted in a serious cyber security risk since the software deployed into US systems was known to have vulnerabilities that could potentially allow hackers to access networks and obtain sensitive data. During the timeframe, Aventura made more than $112 million in sales to the US Government – including the DOE, which ordered approximately $156,000 of automated turnstiles.

[1] https://www.justice.gov/usao-edny/pr/long-island-man-pleads-guilty-bribing-federal-official-obtain-nearly-1-million-federal
[2] https://www.justice.gov/usao-edny/pr/aventura-technologies-inc-pleads-guilty-wire-fraud-and-illegal-importation-reselling

Background

The use of distinguished marks to signify quality and craftsmanship is nothing new. Even in the Middle Ages craftsmen used “makers marks” to establish symbols of authenticity and created craft guilds to regulate specific trades.

In the U.S., civil remedies such as the Lanham Act[3] of 1946 were initially created to protect trademark owners at the Federal level from confusion, misleading marks, and false advertising. For many years there was a large gap in terms of criminal penalties for counterfeit marks and labels until the issuance of the Trademark Counterfeiting Act[4] in 1984. Additionally, growing concerns over the dangers of counterfeit products spurred Federal Agencies to create processes and procedures to confront these issues. For example, in 1993 DOE implemented its first S/CI related policy, DOE O 5000.3B Chg. 1, *Occurrence Reporting and Processing of Operations Information*, which required reporting Suspect/Counterfeit Items (S/CIs) into a centralized event reporting system. This policy is now contained in DOE O 232.2A, *Occurrence Reporting and Processing of Operations Information*.

Additional policies were later added that further addressed S/CI oversight, training, prevention, detection, control, reporting, and disposition. These include DOE O 440.1, *Worker Protection Management for DOE Federal, and Contractor Employees* (now archived) and later in 414.1, *Quality Assurance*.

Reporting Requirements

The primary reporting requirements for S/CI are currently contained in DOE O 414.1E, *Quality Assurance*. This is the centralized departmental order for Suspect/Counterfeit Items, although other orders are referenced such as the following:

- DOE OPEXShare
  - Reference reporting requirements in DOE O 210.2A, *DOE Corporate Operating Experience Program*
- DOE Office of Inspector General (OIG)
  - Reference reporting requirements in DOE O 221.1B, *Reporting Fraud, Waste and Abuse to the Office of Inspector General*
- Occurrence Reporting and Processing System (ORPS)
  - Reference reporting requirements in DOE O 232.2A, *Occurrence Reporting and Processing of Operations Information*

In addition to reporting requirements referenced in DOE O 414.1E, there are also reporting requirements in the Federal Acquisition Regulation (FAR) 52.246-26, *Reporting Nonconforming Items.*

20-Year Data Analysis

This OES provides a compilation and high-level evaluation of S/CI-related data collected by EHSS-23 from DOE reporting over a 20-year timeframe to identify potential performance insights and trends. Industry data was also considered for additional insights and comparison. The goal of the evaluation is to recommend actions for improving mission outcomes through the increased use of leading indicators, cross-organizational sharing of information and, ultimately, preventing the installation of poor-quality components.

---

[3] The Lanham Act, 15 U.S.C. §§ 1051 et seq (https://www.law.cornell.edu/wex/lanham_act)
[4] The Trademark Counterfeit Act 18 U.S.C 2320 (https://www.justice.gov/archives/jm/criminal-resource-manual-1701-trademark-counterfeiting-introduction)

Methodology

ORPS is the centralized system used for S/CI reporting including the historical data regarding the discovery and disposition of S/CIs across the DOE complex. To more accurately gather data from ORPS, the Data Analytics and Machine Learning (DAMaL)[5] tool was used to aid in the data analysis and collection process. Data was collected using a date range from January 1, 2004 to July 8, 2025. Data was ***excluded*** that contained defective items (DI) and were not S/CI such as data found to be reported under DOE O 232.2A criteria *4C (3) Discovery of any defective item or material, other than a suspect/counterfeit item or material, in any application whose failure could result in a loss of safety function, or present a hazard to public or worker health and safety.*

Some reporting criteria included were flagged as S/CI because of keywords that are later entered by DOE Headquarters personnel because the item was determined to be S/CI or because the item was reported using two reporting criteria (e.g., Group 1 and Group 4). The following were the reporting criteria referenced in this analysis:

- Group 1, Operational Emergencies
- Group 2, Personnel Safety & Health
    - Subgroup D, Hazardous Energy
- Group 4, Facility Status
    - Subgroup A, Safety Structure/System/Component Degradation
    - Subgroup C, Suspect/Counterfeit and Defective Items or Material (excludes criterion #3, defective items or materials)
- Group 10, Management Concerns, and Issues

The reporting criteria outlined above may have been captured as S/CI in the analysis due to one of the two Headquarters Keywords being attached to the report such as:

- 11E, *Suspect/Counterfeit Items*
- 13G (Retired), *Suspect/Counterfeit or Defective Items Data Collection Sheet*

Additionally, trends were benchmarked against the U.S. Department of Homeland Security. Homeland Security Investigations (HSI) leads the National Intellectual Property Rights Coordination Center (IPR Center)[6], which is the U.S. government's response to stop global intellectual property theft and enforce trade laws. Comprising Federal agencies and industry experts, the IPR Center polices the sale and distribution of counterfeit goods on websites, social media, and the dark web. Every day, the IPR Center works with industries and agencies to stop Intellectual Property (IP) theft that threatens U.S. businesses, robs hardworking Americans of their jobs, and negatively impacts the economy.

Execution of the HSI and IPR Center missions relies on partnerships with the private sector, academic community, and across all levels of government.

Trends by Fiscal Year

Between January 1, 2004 and July 8,2025, the DOE had 924 Occurrence Reports related specifically to S/CI. Occurrence reports for S/CI ranged from 3 (at the lowest in FY 2020) to 100 (at the highest in FY 2005 and FY 2007) reference *Figure 2*.

---

[5] DAMaL Tools is a collection of data analytics tools with artificial intelligence components used to obtain insights from multiple reporting databases including ORPS.

[6] https://www.iprcenter.gov/

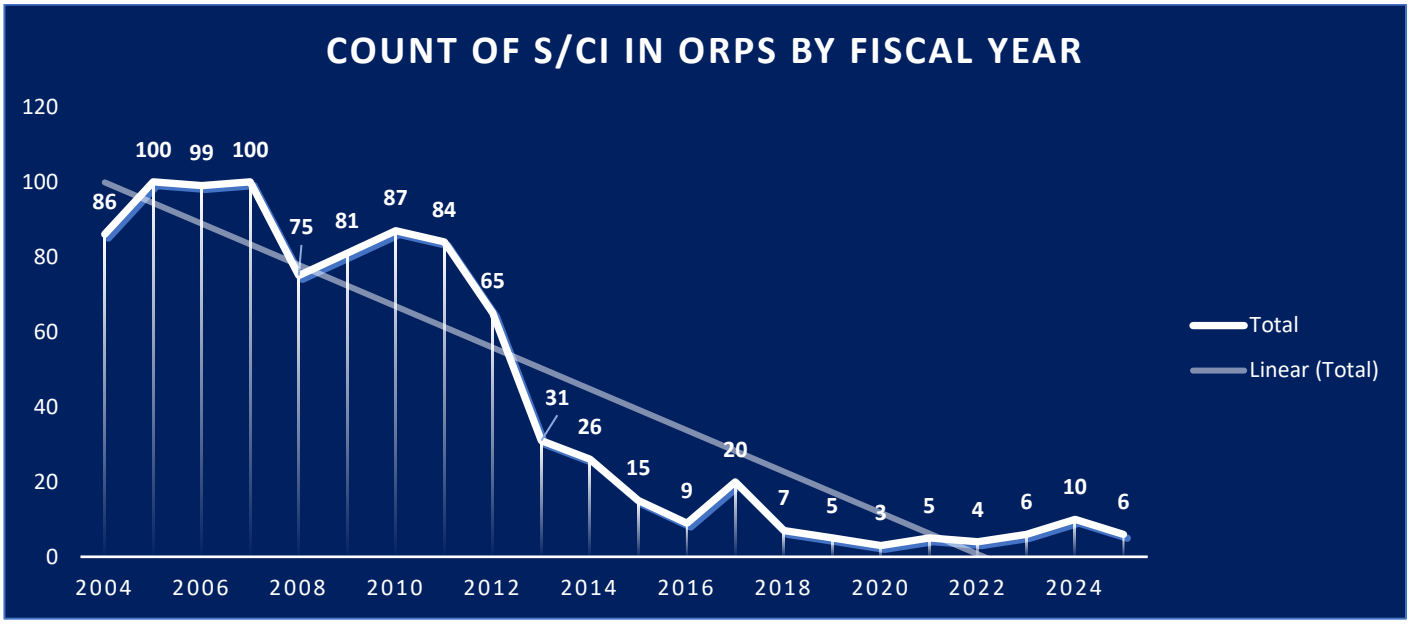

Figure 2 Suspect/Counterfeit reports in ORPS by Fiscal Year

The trend starts to decrease significantly starting in FY 2012, subsequent to a clarification to policy in DOE O 232.2 that previous year which states: Any *suspect/counterfeit or defective item or material found in receipt inspection is exempt from this Subgroup* (this is in reference to Group 4, Subgroup C*, Suspect/Counterfeit and Defective Items or Material*). At this point, sites were no longer required to develop ORPS reports for S/CIs identified in receipt inspection, as these would be prevented from being put into use and hence not present a safety concern. Additionally, the criteria for S/CIs in Group 4, Subgroup C Criterion 2 are considered *informational* for those items not identified in a safety class structure, system, or component. Informational reports can be tailored per Program Office direction to only be captured in local issues management systems and Program Offices have the authority to determine with informational level reports will be submitted to the ORPS database. Due to this, ORPS is not the most appropriate centralized reporting repository to capture S/CI related data

There are also numerous other concerns that S/CIs may present even if they are found during receipt inspection or even potentially in applications that may be excluded from reporting by a Program Office such as potentially with:

- Supply chain integrity;
- Security;
- Mission/Program integrity;
- And others.

When benchmarking against other agencies, one notes that the threats from S/CIs are not decreasing but are exponentially increasing. For instance, in the same timeframe, the U.S. Immigration and Customs Enforcement (ICE) Intellectual Property Rights (IPR) center posted statistics that present the opposite of what is found in DOE reports, such as a growing concern with counterfeit products entering the U.S. supply chain.

Between FY 2004 and FY 2024, the number of counterfeit products and intellectual property theft seizures increased from 7,255 at the lowest in FY 2004 to 34,143, which was the peak number of seizures in FY 2017. It is also important to note that when comparing seizures to monetary values of the items, the monetary value of the items seized is also increasing, with some of the highest values of items being seized in FY 2021 and FY 2022 (reference Figure 3).

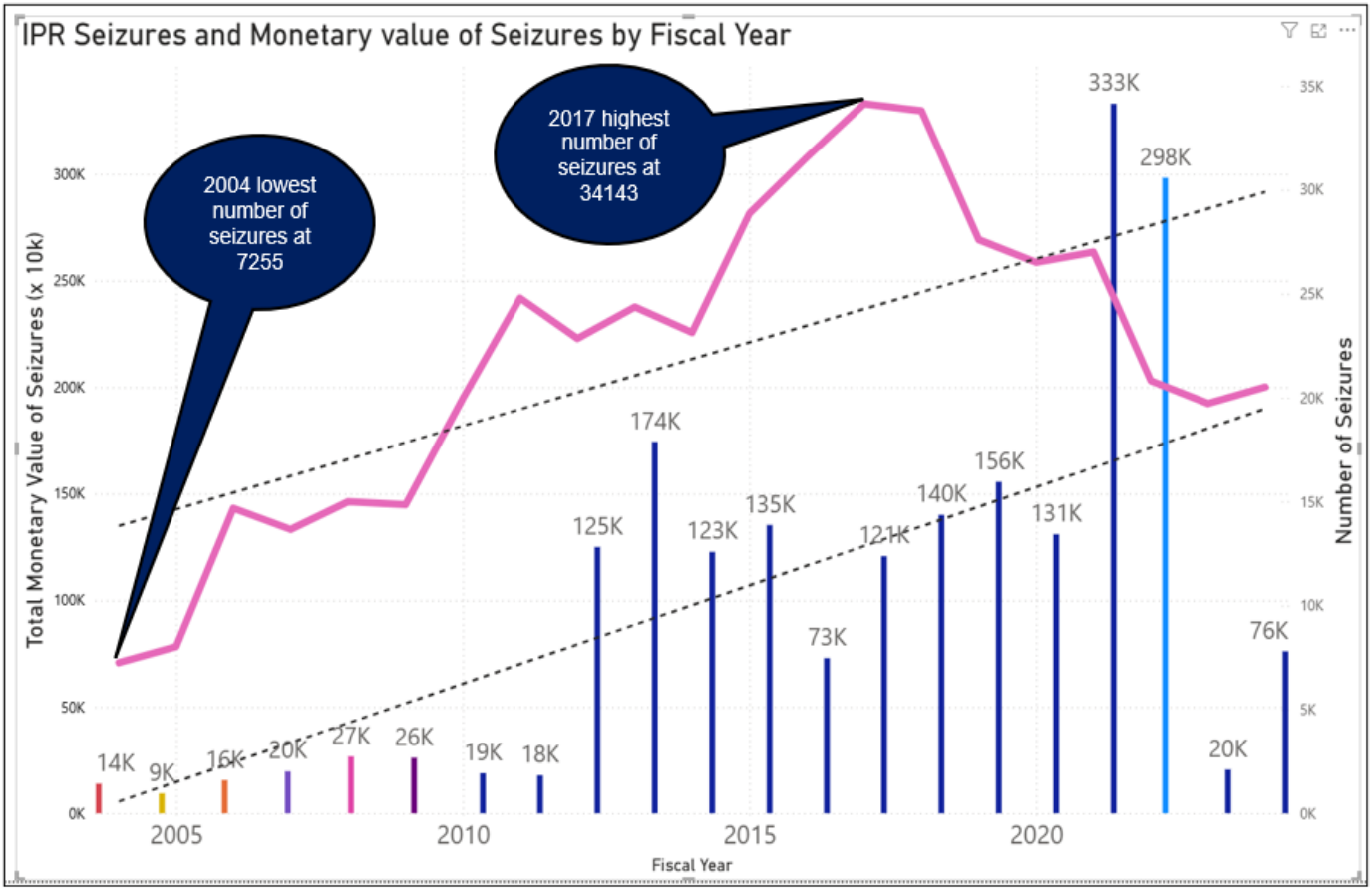

Figure 3 Intellectual Property Rights Center Seizures by Fiscal Year

Reported Items

The types of items reported as S/CI into ORPS were broken down into 7 main categories based on the number of reports. The descriptions of the 7 main categories and the sub items are included below:

1. Construction Equipment
    - Concrete, ladders, platforms, scaffolding, and handrails
2. Electrical Equipment
    - Transformers, circuit breakers, panels, switches, batteries, terminal blocks, heat exchangers, generators, electrical parts, adapters, receptacles, power strips & cords
3. Fasteners
    - General Use Fastener
        - Fasteners that are less than grade 5 or 8.8 or otherwise not used in critical application
    - High- Strength Fastener
        - Fasteners in critical applications or rated grade 5 or 8.8 or above.
4. Hoist, Lifting, and Rigging Equipment
    - Shackles, chains, hooks, slings, cranes, hoists, come-alongs, lifts, clamps,
5. Other
    - Aircraft

        - Items identified on aircraft such as helicopters or Federal Aviation Administration unapproved parts
    - Containers, Chemicals, and Gases
        - Containers, boxes, drums, seals, gases, chemicals, adhesives, and lubricants
    - Custom Order Product
        - Custom designed, fabricated, or order products with suspect indications
    - Documentation
        - Certified material test reports, documents, suspect test, or inspection documents, NRTL stickers
    - Electronic components
        - Transistors, amplifiers, rectifiers, diodes, integrated circuits, programmable logic controller
    - Fire Control Equipment
        - Fire suppression systems, sprinklers, and valves
    - Furniture
        - Office chairs
    - Hand tools
        - Shears, turnbuckles, presses, and drills
    - HEPA Filter
    - Instrumentation, Lab equipment, and measurement tools
        - Flow meters, calibrated test equipment, temperature sensors
    - Metallic Materials
        - Bar stock, rebar, steel plate, wire rope, weld & welding materials
    - Networking, Computing, and Telecommunications
        - Computer cable, network switches, computer modules
    - Personal Protective Equipment
        - Respirators and accessories, fall protection systems, gloves, personnel radiation monitors
6. Pressure Safety Equipment
    - Valves, pumps, piping, and piping accessories
7. Transportation
    - Ratchet tie-down
    - Automotive
        - Items identified on vehicles, trailers, motors, forklifts, electric carts

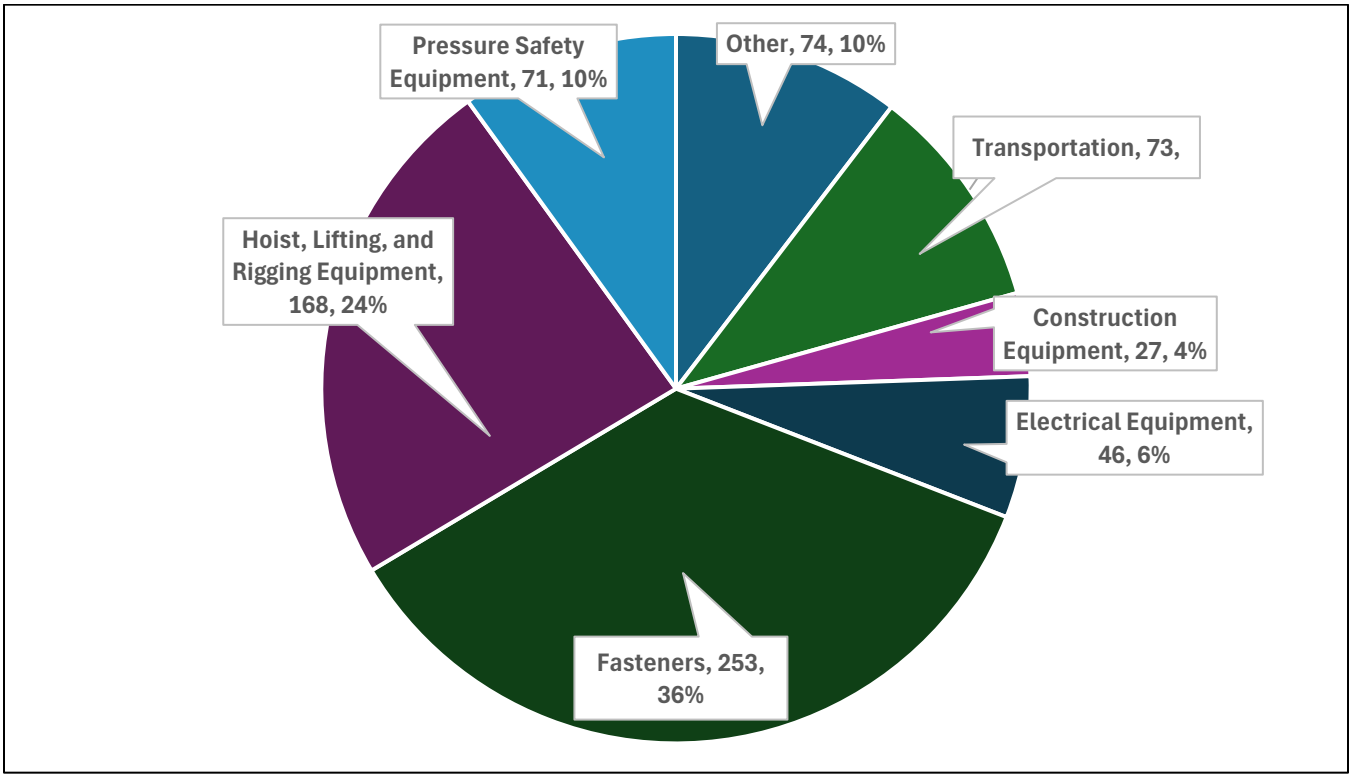

Figure 4 Types of Items (2004 to 2011 – Prior to ORPS Policy Change)

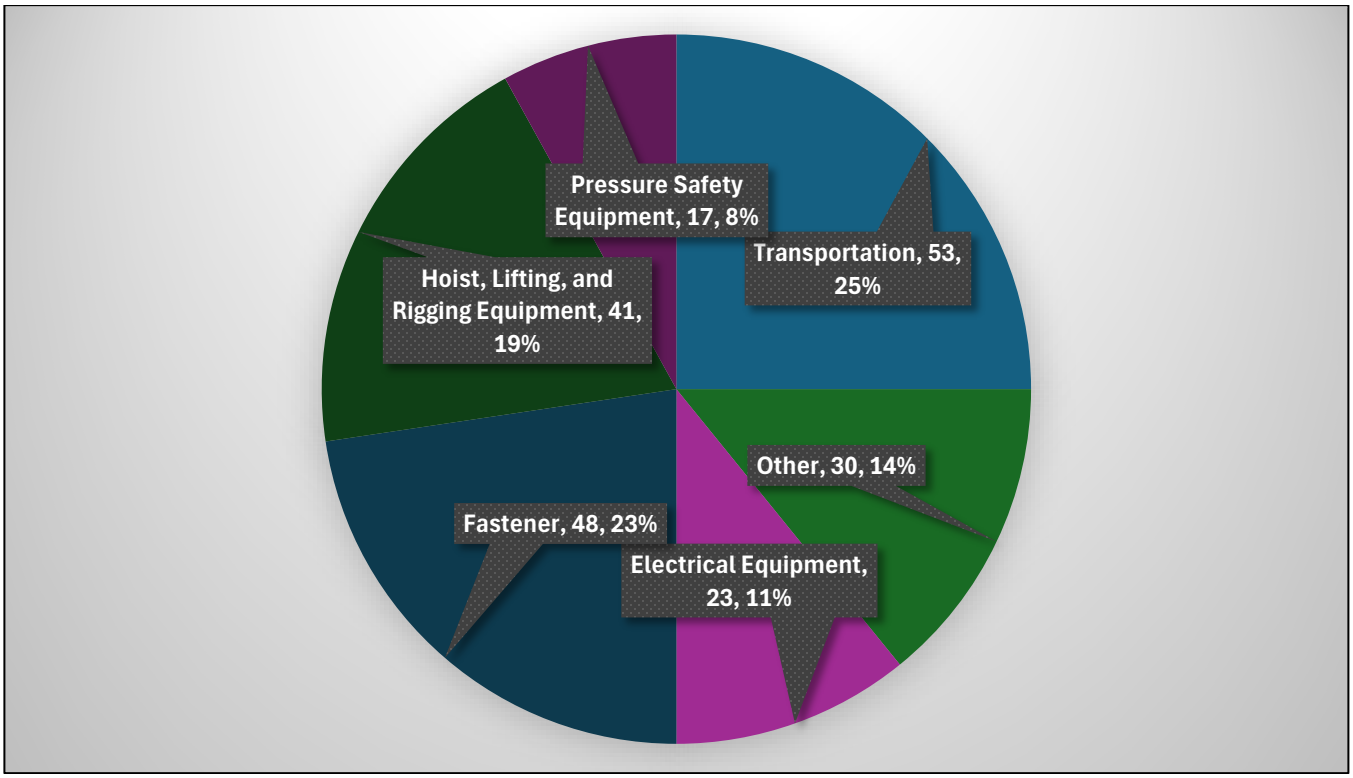

Figure 5 Types of Items (2012 to 2025- After ORPS Policy Change)

Conclusions, Tools, and Recommendations

While ORPS does not provide a full picture of S/CI in the supply chain, it does provide a glimpse of the items that have passed incoming inspections and have potential to impact mission delivery. ORPS data can also be used to supplement S/CI data that is collected locally at each site by procurement or quality assurance organizations following their procedures for incoming quality control.

The results of this OES identify the potential benefit of a centralized reporting repository for S/CIs that can consolidate ***all*** reports from receipt inspection to items found in-use to help understand the true impact of S/CIs at the DOE.

Supplementary resources and tools to help with trends, risk, benchmarking, training, and improving S/CI prevention and detection include use of operating experience information such as:

- Lessons learned;
- Best practices;
- Data collection sheets;
- Operating Experience level 1, 2, and 3 documents;
- Operating Experience Summaries; and
- Operational Awareness documents.

Organizations throughout the DOE may use the data obtained in this OES to:

- Support their local risk analysis;
- Perform benchmarking;
- Understand trends in S/CIs reported;
- Share their trends and observations with other DOE organizations for prevention; and
- Train personnel.

Are you collecting data locally?
Share your leading indicators to help us all prevent a mission impact!

Do you have a productive method for evaluating incoming material at your site? Are you effectively identifying and removing potentially problematic components from your supply chain and capturing the performance data in your local systems? **We want to learn from you!**

How can you help?

- Write a lessons learned document and publish it in DOE OPEXShare
- Collaborate with us to use the Data Analytics and Machine Learning (DAMaL) tools to gain insights and identify trends from your local data set
- Contact Gabby Holcomb at Gabbrielle.Holcomb@hq.doe.gov to discuss your ideas and suggestions!

References

- (Archived) DOE O 5000.3B Chg. 1, *Occurrence Reporting and Processing of Operations Information*
- DOE O 232.2A, *Occurrence Reporting and Processing of Operations Information*
- Data Analytics and Machine Learning (DAMaL) tool
- Occurrence Reporting and Processing System (ORPS)
- DOE O 414.1E, *Quality Assurance*
- DOE OPEXShare
- DOE O 210.2A, *DOE Corporate Operating Experience Program*
- DOE O 221.1B, *Reporting Fraud, Waste and Abuse to the Office of Inspector General*
- FAR 52.246-26, *Reporting Nonconforming Items*
- National Intellectual Property Rights Coordination Center (IPR Center), https://www.iprcenter.gov/
- *The Lanham Act*, 15 U.S.C. §§ 1051 et seq., https://www.law.cornell.edu/wex/lanham_act
- *The Trademark Counterfeit Act*, 18 U.S.C 2320 (https://www.justice.gov/archives/jm/criminal-resource-manual-1701-trademark-counterfeiting-introduction)
- U.S. Department of Justice, *Long Island Man Pleads Guilty to Bribing Federal Official to Obtain Nearly $1 Million in Federal Contracts* (05/03/2023). https://www.justice.gov/usao-edny/pr/long-island-man-pleads-guilty-bribing-federal-official-obtain-nearly-1-million-federal
- U.S. Department of Justice, Aventura Technologies, Inc. Pleads Guilty to Wire Fraud and Illegal Importation for Reselling Chinese Goods as U.S.-Made (03/19/2024). https://www.justice.gov/usao-edny/pr/aventura-technologies-inc-pleads-guilty-wire-fraud-and-illegal-importation-reselling

For further information or questions about this OES, please contact Gabrielle Holcomb at gabrielle.holcomb@hq.doe.gov or the EHSS Office of ES&H Reporting and Analysis (EHSS-23) by email at OEC@hq.doe.gov.

Operating Experience Summary
Operating Experience Summary (OES): An informative operating experience-based article published by the Office of Environment, Health, Safety, and Security (EHSS) and distributed across the DOE complex through the DOE Corporate Operating Experience Program to promote safety and mission success through the open exchange of valuable experiences, good practices, and performance summaries. Learn more at: Operating Experience Summaries | Department of Energy