EPA **IT/IM DIRECTIVE**
PROCEDURE

Information Security – Detecting Counterfeit Information and Communications Technology Products Procedure

Directive No: CIO 2150-P-27.0

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19

Information Security – Detecting Counterfeit Information and Communications Technology Products Procedure

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) requirements for detecting counterfeit information and communications technology (ICT) products. This procedure also addresses supply chain risk management security controls outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations.

2. SCOPE

These procedures address all United States EPA information and information systems to include information and information systems used, managed, or operated by a contractor, another agency or other organization on behalf of the EPA.

3. AUDIENCE

The audience is all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of the EPA.

4. AUTHORITY

- Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology of 2018 (https://www.congress.gov/115/plaws/publ390/PLAW-115publ390.pdf)
- E-Government Act of 2002, Public Law 107-347, Title III, Federal Information Security Management Act, as amended (https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf)
- Cybersecurity Act of 2015, Public Law 114-113 (https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf)
- Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283, to amend chapter 35 of title 44, United States Code (U.S.C.) (https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf)
- OMB Circular A-130, “Management of Federal Information Resources,” Appendix III, “Security of Federal Information Resources,” July 2016 (https://georgewbush-whitehouse.archives.gov/omb/circulars/a130/a130trans4.html)
- EPA Information Security Policy (https://www.epa.gov/sites/default/files/2019-09/documents/information_security_policy_20190820_508_vwn.pdf)

5. PROCEDURE

The early detection of counterfeit and/or compromised ICT products is vital to protecting the EPA from threat actors introducing and exploiting product vulnerabilities. Ensuring the authenticity and integrity of acquired ICT products, including new products, replacement parts and existing products that require upgrades, is an essential element of the EPA's information technology (IT) supply chain risk management (SCRM) program. This procedure provides guidance to Agency personnel responsible for the acquisition, operation, maintenance and disposal of ICT products. The objective of this procedure is to prevent the deployment of a counterfeit and/or compromised product into EPA's environment.

The most effective way to minimize the likelihood of deploying counterfeit and/or compromised ICT products is to understand the risks associated with the products and the product suppliers. This requires actions to be taken throughout the product lifecycle from acquisition to disposal (e.g., decommissioning). Agency personnel shall take reasonable steps to minimize the likelihood of introducing counterfeit and/or compromised ICT products into the Agency environment by employing the guidance outlined in this procedure.

The Agency approach to detecting a counterfeit and/or compromised ICT product is a risk-based approach. The risk-based approach considers two primary factors in assessing the risk, the type of product and the supplier of the product. For each factor, consideration will be given to the impact and likelihood of risk event occurrence when assessing risk. This approach is consistent with the EPA's Enterprise Risk Management Process and risk assessment procedure, *Information Security – Risk Assessment Procedures*. The risk assessment results inform which detection techniques are appropriate. Beginning with acquisition and prior to deployment, Agency personnel shall follow the steps and underlying processes of this procedure.

1. Assess product and supplier risk.
2. Perform detection techniques.
3. Contain, dispose, and report any known counterfeit and/or compromised products.

The following actions are part of the Agency's risk-based approach to detecting a counterfeit and/or compromised ICT product and shall be employed as appropriate throughout the product lifecycle.

5.1. PRODUCT RISK

To employ appropriate counterfeit detection techniques, it is important to understand the risk posed by the product and supplier, therefore, a risk assessment is required. The risk assessment determines the likelihood of occurrence and the impact if the risk is realized. The objective of the assessment is to understand the level of risk posed by the product and supplier, and determine the likelihood of occurrence, the impact and what steps shall be undertaken to respond to the risk(s). To accomplish this objective, the Agency analyzes threats, vulnerabilities and the associated uncertainties.

5.1.1. Impact

The magnitude of harm that can be expected to result from the consequences of acquiring and using a counterfeit product. Possible impacts from introducing counterfeit product include limited/decreased functionality and/or reliability, unexpected behavior, degraded performance, or increased susceptibility to malicious attack. The severity of the impact increases the risk to the Agency. Additional considerations include the criticalness and strategic value the product has to EPA's mission. For example, a product that is necessary/key to a high value asset (HVA) supporting a mission essential function will have a higher-level of criticalness to the Agency and warrant robust measures to minimize the risk of introducing counterfeit and/or compromised product. The impact level in conjunction with the likelihood of occurrence will determine the overall risk to the Agency and commensurate measures to be employed.

5.1.2. Likelihood

The probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities. Personnel shall take appropriate steps necessary to discover and prevent the deployment of counterfeited products into EPA's environment.

When evaluating the likelihood of a product being counterfeited, EPA personnel shall consider several factors that may increase the likelihood of product counterfeiting.

- **Obsolescence** – Product that is no longer available from the original manufacturer or an authorized supplier. Obsolete products that are in high demand may become an attractive target of counterfeiters, increasing the likelihood that available products may be counterfeit and/or compromised.
- **Difficult to Procure** – Some products may be difficult to procure due to special requirements such as national security considerations, special waivers, import/export restrictions, environmental concerns, etc. Falsification of required documentation may allow noncompliant products to be sold fraudulently.
- **Extensive Lead Time** – Products requiring extensive lead time may become a target of counterfeiters who entice purchasers with shorter lead times.
- **Multiple Versions** – Products with multiple compatible versions may cause confusion amongst purchasers, presenting an opportunity which counterfeiters may exploit.
- **Item Type** – Certain product types are more likely to be counterfeited. For example, network hardware is commonly counterfeited and passed off as authentic.
- **Price and Volume** – Products at high price points or ordered in large volume present a significant profit motive to counterfeiters. Purchasers are lured by discounted pricing.
- **Common Commercial Material** – Items commonly used in commercial applications are more likely to exist in high volume as electronic waste or e-waste. This is product that has been used previously but has subsequently been reclaimed and refurbished. Products may be resold as new.
- **Widely Used** – Products widely used, especially those in the Federal Government, are targets for adversaries. Widely used software that is compromised has the potential to impact thousands of public and private entities.

- **Strategic Value** – Products that have strategic value become an attractive target of counterfeiters.

5.2. SUPPLIER RISK

Corrupt suppliers may use the aforementioned factors to take advantage of customers' needs to provide counterfeit products, this is especially relevant when cost and schedule are key considerations. The trustworthiness of a supplier is a determining factor as to the likelihood of a product being counterfeited or compromised. To minimize this risk, EPA personnel are encouraged to use available authoritative sources such as the General Services Administration's "GSA Advantage!" or other government acquisition vehicles to identify suppliers[1]. The Agency considers suppliers on these vehicles to be authorized.

Using suppliers other than these may significantly increase the likelihood of purchasing counterfeited product. However, there may be situations when product is not available through a government acquisition vehicle. This procedure presents guidance on how to measure risk and employ appropriate risk-mitigation tactics.

To assess the risk associated with suppliers, this procedure defines four supplier types: original manufacturers, aftermarket manufacturers, authorized suppliers and unauthorized suppliers, along with the varying degree of risk each presents.

- **Original Equipment Manufacturers (OEM)** – An OEM is the organization that owns the design, and/or engineers the product and has intellectual property rights. The OM typically warranties the product beyond replacement and has interest in assisting with failure analysis, reliability data and other support. The OEM typically has complete control over the entire production process. This type of authorized supplier presents the lowest risk profile.
- **Aftermarket Manufacturers (AM)** – An AM is authorized by the OEM to produce and sell replacement product. The AM may fill an ongoing need for a product the OEM has ceased to produce and may have intellectual rights as well. The relationship with the OEM is typified by a legal arrangement. Warranty support is equivalent to that of the OEM. This type of authorized supplier presents a risk profile similar, if not equal to, that of the OEM.
- **Authorized Suppliers** – Original and aftermarket manufacturers usually sell material through an authorized supply chain. An authorized supply chain can include authorized distributors, franchised distributors, sales representatives, etc. (collectively known as authorized suppliers). All the suppliers obtain material directly from the OEM or another authorized supplier, with a contractual agreement to do so. In the authorized supply chain, the original/aftermarket manufacturer will honor the complete warranty. Authorized suppliers present a low risk for counterfeit material, but higher than if the product were purchased directly from an original/aftermarket manufacturer. Authorized suppliers of specific product can be validated by the OEM. The Task Order Contracting Officer Representative (TOCOR) and Technical Point of Contact (TPOC) must have a solid understanding of the supplier types and associated counterfeit risks. The TOCOR and TPOC bear the responsibility of identifying the lowest risk supplier(s).

[1] Welcome to GSA Advantage!

- **Unauthorized Suppliers** – An unauthorized supplier presents the highest risk to Agency for counterfeit or compromised ICT products. Unauthorized suppliers typically do not have any formal relationship with the OEM and/or AM. Additionally, these suppliers' products are not available on a government acquisition vehicle. Warranty support is usually very limited with restrictive time frames. There are few assurances that the product being sold was part of the authorized supply chain. If possible, it is best to avoid unauthorized suppliers.

5.2.1. Approving Unauthorized Supplier

When a product is not available from an OEM or AM and only available from an unauthorized supplier, an alternative product shall be considered first. If alternatives are not suitable or available and redesign is not an option, consideration shall be given to identifying alternatives from unauthorized suppliers once appropriate steps have been taken to mitigate inherent risks. The use of unauthorized suppliers shall be considered only as a last resort. The TPOC most familiar with the product, working with the Contracting Officer Representative (COR) and TOCOR, shall take the following steps:

- Conduct extensive research on potential suppliers.
- Check online reviews, customer feedback, and industry reputation to make informed decisions.
- Verify authenticity, request documentation and certification from the supplier that proves the authenticity of the product. This may include product serial numbers, certificates of authenticity, and warranty information.
- Cross-verify this information with the OEM or official channels.
- Research the supplier to determine if anti-counterfeiting measures are in place.
- Utilize the NIST Supply Chain Risk Management Assessment Scoping Questionnaire in Special Publication 800-161, Rev 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*.

If at the completion of these activities and the use of an unauthorized supplier is still deemed necessary, the TPOC shall seek the formal approval of the respective region or program office Senior Information Official (SIO) via the **EPA Information Security Risk Determination Process**.

5.3. RISK ASSESSMENT

Assessing risk is achieved by weighing the likelihood that an event will occur against the impact of the occurrence. This procedure follows a basic risk matrix. Figure 1 illustrates risk level based upon likelihood and impact. The green, yellow and red boxes reflect the risk of acquiring counterfeit product based on product type and supplier.

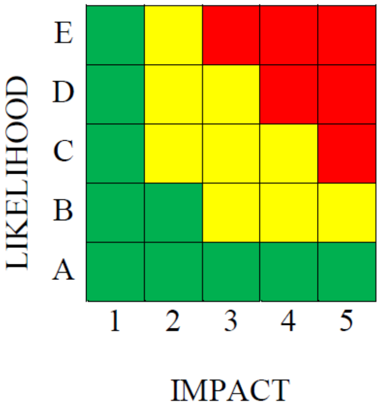

Figure 1 - Risk Assessment Matrix

Table 1 - Likelihood Assessment is a guide for determining the likelihood different suppliers pose for each product type. Using information gathered about supplier and product, EPA personnel can use that information to determine the likelihood of occurrence.

Table 1 - Likelihood Assessment

Level	Supplier Type	Product Type
A	Authorized	All Types
B	Unauthorized Approved	Low and medium risk product
C	Unauthorized Approved	High risk product
D	Unauthorized Unapproved	Low risk product
E	Unauthorized Unapproved	Medium and high-risk product

Table 2 - Impact Assessment provides guidance on determining the potential impact a counterfeit ICT product may have on the Agency.

Table 2 - Impact Assessment

Level	Impact
1	Minimal or no system impact
2	Minor system impact
3	Moderate system impact
4	Major system impact
5	Safety or mission impact

Use the information from Table 1 and Table 2 to determine likelihood and impact levels, and map those data points to Figure 1 - Risk Assessment Matrix. The result points to a recommended mitigation measure in Table 3 - Risk Mitigation. Personnel will use the result of the likelihood and impact analysis and corresponding mitigation measure (based upon the risk level) to determine which counterfeit detection technique to use.

Table 3 - Risk Mitigation

Risk Level	Recommended Mitigation
Green	No mitigation necessary
Yellow	Standard mitigation (inspection)
Red	Enhanced mitigation (inspection and test)

5.4. COUNTERFEIT DETECTION

Determining if an ICT product is authentic begins with employing some basic detection techniques that need to occur upon product receipt, preferably during the receiving process. These techniques include verifying consistency within the paperwork and visually inspecting the product and its packaging. Detailed guidance is provided under basic detection activities. Authenticating high risk products may require more sophisticated techniques, most likely requiring assistance from an independent third-party organization specializing in ICT product authentication. When possible, personnel shall apply additional industry detection standards that address the subjects of inspections and tests, sample sizes, other counterfeit product indicators, etc. Appendix B contains a reference list of some industry standards.

5.4.1. Basic Detection Techniques

Basic detection techniques for identifying counterfeit products involve reviewing/inspecting all associated product paperwork (including packaging and part labels) and physically inspecting the product. As the initial point of receipt, warehouse/receiving personnel shall perform basic detection techniques. Upon receipt of the product, the TPOC shall perform applicable basic detection techniques.

5.4.1.1. Paperwork Inspection:

The paperwork accompanying the product should provide some basic information, such as:

- Origin of shipment.
- Certification of inspection and/or testing.
- Date and lot codes, quantity, etc.

Is the paperwork accurate? Look for missing or suspicious information, such as:

- Misspellings, poor grammar, etc.
- Inaccurate company information (e.g., incorrect addresses, company names, logos).
- Incorrect product identifiers (e.g., product numbers, wrong or missing bar codes, incorrect product descriptions).

Inspect the physical appearance of the paperwork for indications of counterfeiting.

- Altered Documents
  - Excessively faded, unclear or missing data.
  - Use of correction fluid or correction tape.
  - Type style, size or pitch change is evident.
  - Data on a single line is located at different heights.

    - Lines on forms are bent, broken or interrupted indicating data has been deleted or exchanged by "cut and paste."
    - Handwritten entries are on the same document where there is typed or pre-printed data.
    - Text on page ends abruptly and the number of pages conflicts with the transmittal.
- Signatures and Initials
    - Corrections are not properly lined-out, initialed and dated.
    - Document is not signed or initialed when required.
    - The name of the document approver or title cannot be determined.
    - Approver's name and signature do not match.
    - Document has missing or illegible signature or initials.
- Certification
    - Technical data is inconsistent with code or standard requirements.
    - Certification/test results are identical between all tested items, normal variation should be expected.
    - Documentation "Certificate of Conformance and Testing" is not delivered as required on the purchase order or is in an unusual format.
    - Document is not traceable to the items procured.

5.4.1.2. Physical Inspection

- Packaging
    - Exterior packaging is damaged, or packaging appears to have been opened.
    - Interior packaging is damaged or appears to have been previously opened.
- Product scratches, dents and tamper-evident seals
    - Product exhibits excessive signs of wear.
    - Tamper-evident seals are broken.
    - Product appears to have been disassembled and reassembled.

5.4.2. Advanced Detection Techniques

Authenticating some ICT products may warrant employing more advanced detection techniques. Beyond performing some basic functionality testing, EPA has limited in-house capability to perform advance product testing. In circumstances where the risk level for an ICT product is high and recommended mitigation includes testing, the TOCOR and TPOC may decide the associated risk level warrants procuring the services of an independent testing lab to authenticate the product.

5.5. AUTHENTICATING PRODUCT

After application of the detection techniques to authenticate the product, there may still be indications of possible counterfeiting. It is important to note the differences between authentic and counterfeit product can be very subtle. For example, it is possible that an authentic product may have scratches, dents, and other physical damage indicators as well as suspicious paperwork containing errors. Some physical indicators may occur as the result of being stored for a long period of time or occur during product transport. If counterfeit product is still suspected, there are two methods to increase the level of confidence as to the authenticity of the product.

1. Identify multiple suspect counterfeit indicators. A significant number of indicators that are substantial in nature may indicate counterfeit and/or compromised product.

    a) Minor - quality or handling issues (e.g., exterior packaging is damaged).

    b) Moderate - definite cause of suspicion for the product’s authenticity (e.g., exterior packaging is damaged, and documentation contains errors).

    c) Major - high risk that the product has been modified (e.g., damaged packaging, tamper-evident product seals are broken, physical assembly appears to have been disassembled and reassembled or paperwork is suspect).

    Counterfeit indicator guidance:

    - One major and one moderate;
    - Three or more moderate; or
    - Two or more moderate and two or more minor.

    Appendix C provides additional examples of tests, counterfeit indicators, and corresponding significance. If counterfeit indicators reach any of these guidance thresholds, the product shall be considered counterfeit.

2. Contact the OEM for further information to authenticate the product.

After applying these methods, if the TPOC has a high level of confidence as to the authenticity of the product, the product is ready for deployment. If indicators point to the product being counterfeit and/or compromised, proceed to the next section for further guidance.

5.6. CONTAINMENT, DISPOSAL, REPORTING

If counterfeiting is suspected, the product shall be isolated and visibly marked, indicating as such. If the product was part of a larger shipment of similar product (e.g., date and lot codes), those products shall also be considered counterfeit, and steps should be taken to isolate these products. The TPOC and TOCOR shall take these additional steps to contain exposure.

5.6.1. Containment

1) Notify the Computer Security Incident Response Capability (CSIRC), Information Security Officer (ISO), warehouse personnel and COR.

2) Isolate and secure the product.

3) Visibly mark the product as suspect counterfeit.

4) Contact the OEM for analysis.

5) Do not contact or return the product to the supplier.

6) Identify other product received from the supplier as possible counterfeits.

5.6.2. Disposal

Before suspected or confirmed counterfeit product is destroyed, appropriate Agency authorities shall be notified for approval. The COR and TOCOR shall notify the Office of Acquisition Solutions (OAS), Office of the Inspector General (OIG) and Office of General Counsel (OGC). With approval, the confirmed counterfeit product shall be destroyed according to Agency property management procedures.

5.6.3. Reporting

The COR and TOCOR shall report counterfeit products to the OIG. Additionally, it is suggested that counterfeit product reports be filed with the Government Industry Data Exchange Program (GIDEP)[2].

5.7. GENERAL RULES TO FOLLOW

In conclusion, here are some general rules to follow to limit the likelihood of introducing counterfeit devices.

1) When possible, purchase material from OEMs and authorized suppliers only.

2) Always treat product purchased from unauthorized suppliers as suspected counterfeit product and take appropriate action(s).

3) Practice proactive Diminishing Manufacturing Sources and Material Shortages (DMSMS) management.

4) Manage the supply chain to ensure unauthorized suppliers are thoroughly vetted to reduce the risk of receiving counterfeit material.

5) Establish a risk-based set of inspections and tests proven to detect counterfeit product.

6) Report suspected counterfeit parts to all stakeholders (e.g., CSIRC, IMO, ISO, ISO, TPOC, TOCOR, COR).

7) Contractually require contractors and their sub-contractors to implement counterfeit mitigation practices.

5.8. COUNTERFEIT DETECTION TRAINING

Agency personnel involved in supply chain activities are encouraged to take advantage of training opportunities available from the Federal Acquisition Institute (FAI) (https://dau.csod.com/catalog/CustomPage.aspx?id=221000567&tab_page_id=221000567). FAI offers *LOG 0620 Counterfeit Prevention Awareness*, which introduces counterfeit

[2] *GIDEP is a cooperative activity between government and industry participants seeking to reduce or eliminate expenditures of resources by sharing technical information.* https://www.gidep.org/

awareness, products at risk and supply chain infiltration; and identifying, reporting and disposal of a counterfeit product.

6. ROLES AND RESPONSIBILITIES

Computer Security Incident Response Capability (CSIRC):

- Protect the Agency's information assets and network.
- Take actions to verify that an incident occurred upon learning of a potential incident.
- Determine the scope and impact of each incident and prioritize actions accordingly.
- Determine the magnitude of the incident once an incident is validated.
- Track and maintain an electronic log of all incidents.
- Ensure that incident tickets for actual and potential incidents are:
  - Updated throughout the incident management life cycle
  - Made available only to appropriate personnel.
- Report and coordinate incidents with stakeholders.

Contracting Officer (CO):

- Ensure contracts contain information security clauses and language for safeguarding Agency interests through its contractual relationships.
- Ensure, with the assistance of the COR, that products and services meet all Agency information security requirements.
- Ensure contractor(s) and product supplier(s) comply with EPA contractual requirements.
- Address and/or resolve any contractual issues with contractor(s) or product supplier(s). Refer technical issues to the TOCOR.

Contracting Officers Representatives (COR) or Contracting Officer Technical Representatives (COTOR):

- Ensure contractor(s) and product supplier(s) comply with EPA contractual requirements.
- Address and/or resolve any technical issues with contractor(s) or product supplier(s). Copies the CO on any communication with the contractor. Refers contractual issues to the CO, which include but are not limited to matters that impact cost, scope, and period of performance.
- Coordinate/communicate with product suppliers on product replacement, refunds, and warranty, etc.
- Whenever feasible, Agency personnel are encouraged to use authorized suppliers.
- Withhold approval/payment of invoices related to suspected counterfeit/compromised ICT Products.

Information Management Officer (IMO):

- Support the Senior Information Official (SIO) in implementing the SIO's supply chain risk management functions relating to the detection of counterfeit devices.
- Implement policies, procedures, control techniques and processes identified in the Agency supply chain risk management program.
- Develop and issue local information security procedures, control techniques and processes for local systems and operations as necessary to support and implement counterfeit detection procedures.
- Execute the appropriate security controls and processes for responding to a CSIRC security notification regarding counterfeit devices. Such notifications shall be complied with immediately.
- Coordinate with the Chief Information Officer (CIO), Risk Executive, Risk Executive Group, Chief Information Security Officer (CISO), ISOs, system and information owners and others involved with securing Agency information and systems to ensure adequate measures are in place to manage supply chain risks at an acceptable level.

Information Security Officer (ISO):

- Respond immediately to a reported incident.
- Provide management and logistical support to system administrators for timely reporting, tracking, resolving, and documenting detected computer security incidents.
- Coordinate with CSIRC and IT management to resolve and close outstanding incidents within service level agreement (SLA) timeframes established by CSIRC.
- Coordinate with the Office of Information Technology Operations (OITO) security staff and CSIRC (as needed) for technical support and direction required to provide management and logistical support to system administrators and to document the incident.
- Collect any needed information.
- Receive and forward all CSIRC notifications to individuals responsible for affected systems.

Office of Acquisition Solutions (OAS):

- Develop SCRM acquisition policies and procedures.
- Develop and provide terms and agreements to suppliers regarding Agency SCRM requirements.
- Minimize risk to the Agency by limiting product acquisition to authorized suppliers whenever possible.
- Assist and guide Agency personnel through the product acquisition process.

Office of Inspector General (OIG), Office of Investigations (OI):

- Determine if an incident identified by CSIRC is criminal in nature.
- Serve as the primary point of contact for coordination with law enforcement.
- Conduct criminal investigations of incidents as determined.
- Assist CSIRC and ISO in forensic capabilities, when possible and needed.

Office of General Counsel (OGC):

- Review incident reports to be provided to external entities for criminally related incidents.
- When warranted, provide counsel to OAS on risks to the Agency of utilizing unapproved suppliers during the Acquisition Evaluation Process.

Office of Information Security and Privacy (OISP):

- Develop policies, procedures, and guidelines to address cybersecurity risks in the Agency's supply chain.
- Assist with response and resolution efforts regarding incidents of counterfeiting in the Agency's supply chain.

Technical Point of Contact (TPOC):

- Perform counterfeit detection techniques.
- Report any suspected counterfeit products to appropriate stakeholders.
- Take appropriate action to isolate product and limit exposure to the Agency if counterfeiting is suspected.
- Assist in any incident response activities.
- Withhold approval/payment of invoices related to suspected counterfeit/compromised ICT Products.

Warehouse/Receiving Personnel

- Perform basic counterfeit detection techniques.
- Notify CSRIC and stakeholders of suspected counterfeit product.
- Contain, report, and dispose of any suspected counterfeit product.

7. RELATED INFORMATION

- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures
- NIST SP 800-53 Rev 5, Security and Privacy Controls for Information Systems and Organizations (nist.gov) (PM-30, RA-3, SA-15, SR-5, SR-9, SR-9(1), SR-10, SR-11, SR-11(1) and SR-12)
- NIST SP 800-37 Rev 2, Risk Management Framework for Information Systems and

Organizations (nist.gov)

- NIST SP 800-161 Rev 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (nist.gov)

8. DEFINITIONS

- **Counterfeit:** Counterfeit material refers to items that are unauthorized copies or substitutes that have been identified, marked, or altered by a source other than the items' legally authorized supplier or have been misrepresented to be authorized items of the legally authorized supplier.
- **Decapsulation:** Decapping or delidding of an integrated circuit is the process of removing the protective cover or integrated heat spreader of an integrated circuit so that the contained die is revealed for visual inspection of the micro circuitry imprinted on the die.
- **Diminishing Manufacturing Sources and Material Shortages (DMSMS) Management**: The concept that Agency lifecycles may be longer than product lifecycles, increasing the likelihood of needing to purchase from unauthorized suppliers.[3]
- **Information and Communications Technology (ICT) Product:** Encompasses the products used for capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer and interchange of data and information.
- **Supply Chain**: A linked set of resources that can be subject to cybersecurity risk in the supply chain from suppliers, their supply chains and their products or services.
- **Wirebond**: The method of making interconnections between an integrated circuit (IC) or other semiconductor device and its packaging during semiconductor device fabrication.

9. WAIVERS

Waivers or deviations may be requested through the EPA Risk Determination Process based on a substantive business need and the implementation of compensating controls that provide a suitable alternative to the mandated protection.

Only EPA's Chief Information Officer may authorize Agency-wide waivers or deviations from the standards herein.

10. DIRECTIVE(S) SUPERSEDED

Not applicable.

[3] *Standards Related Document 22 (SD-22) "Diminishing Manufacturing Sources and Material Shortages A Guidebook of Best Practices for Implementing a Robust DMSMS Management Program", Department of Defense, Defense Standardization Program Office, January 2021.*

11. CONTACTS

For further information, please contact the Office of Mission Support (OMS) or the Office of Information Security and Privacy (OISP) at Infosec@epa.gov.

VAUGHN NOGA Digitally signed by VAUGHN NOGA
Date: 2023.08.21 08:19:31 -04'00'

Vaughn Noga
Deputy Assistant Administrator for Environmental Information and Chief Information Officer
U.S. Environmental Protection Agency

APPENDIX A: ACRONYMS & ABBREVIATIONS

AM	Aftermarket Manufacturer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COR	Contracting Officer Representative
COTOR	Contracting Officer Technical Representative
CSAM	C-Mode Scanning Acoustic Microscopy
CSIRC	Computer Security Incident Response Capability
DC	Date Code
DMSMS	Diminishing Manufacturing Sources and Material Shortages
EPA	Environmental Protection Agency
ESD	Electrostatic Discharge
FAI	Federal Acquisition Institute
FISMA	Federal Information Security Modernization Act
GIDEP	Government Industry Data Exchange Program
GSA	General Services Administration
HIC	Humidity indicator card
HVA	High Value Asset
ICT	Information and Communications Technology
IMO	Information Management Officer
ISO	Information Security Officer
IT	Information Technology
MS	Mineral Spirits
NIST	National Institute of Standards and Technology
OAS	Office of Acquisition Solutions
OGC	Office of General Counsel
OIG-OI	Office of Inspector General, Office of Investigations
OISP	Office of Information Security and Privacy
OITO	Office of Information Technology Operations
OEM	Original Equipment Manufacturer
OMB	Office of Management and Budget
OMS	Office of Mission Support
SCRM	Supply Chain Risk Management
SIO	Senor Information Official
SLA	Service Level Agreement
SP	Special Publication
TOCOR	Task Order Contracting Officer Technical Representative
TPOC	Technical Point of Contact
U.S.C.	United States Code

APPENDIX B: INDUSTRY STANDARDS

The following Industry Standards provide counterfeit avoidance and risk mitigation information. This list is not an all-inclusive list. There may be a cost associated with some of these standards.

- SAE ARP6178 – "Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors".
- SAE ARP6328 – "Guideline for Development of Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Systems".
- SAE AS5553 – "Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition"
- SAE AS6081 – "Fraudulent/Counterfeit Electronic Parts: Detection, Mitigation, and Disposition– Distributors"
- SAE AS6171 – "Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts"
- SAE AS6174 – "Counterfeit Material: Assuring Acquisition of Authentic and Conforming Material"
- SAE AS6301 – "Compliance Verification Criterion Standard for SAE AS6081,
- Fraudulent/Counterfeit Electronic Parts: Detection, Mitigation, and Disposition – Distributors"
- SAE AS6462 – "AS5553, Counterfeit Electronic Parts, Avoidance, Detection, Mitigation, and Disposition Verification Criteria"
- SAE AS6496 – "Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Authorized/Franchised Distribution"

APPENDIX C: INDICATORS OF COUNTERFEIT ICT PRODUCTS[4]

Test Type	Counterfeit Indicator	Strength of Indicator
External Package Inspection	Erroneous OEM Logo on external packaging	Major
	Wrong part number on external packaging	Moderate
	Misspelled wording on external packaging	Minor
	Shipping damage to external packaging	Minor
Internal Package Inspection	Bar code mismatch (scan vs human) on box/tube/tray/reel	Major
	Erroneous OEM Logo on box/tube/tray/reel	Major
	Humidity indicator card (HIC) (HIC does not change with humidity)	Major
	Inconsistent design of tubes/trays/reels	Moderate
	Incorrect size for tube/tray	Moderate
	Use of non- Electrostatic Discharge (ESD) protected material	Moderate
	Wrong part number on box/tube/tray/reel	Moderate
	Wrong/inconsistent orientation in tube/tray/reel	Moderate
	Misspelled wording on box/tube/tray/reel	Minor
	Not in a sealed moisture barrier bag	Minor
	Not in original manufacturer's packaging	Minor
	Shipping damage to box/tube/tray/reel	Minor
	Wrong quantity notes on box/tube/tray/reel	Minor
Documentation Inspection	Erroneous OEM Logo on documents	Major
	Evidence of tampering in documentation	Moderate
	Mismatch in part number or lot/ DC in documentation	Moderate
	Mismatch in part quantity in documentation	Minor
	Misspelled wording in documentation	Minor
Part Marking / ID Inspection	Three or more date codes or lots in the same box/tube/tray/reel	Moderate
	Marking on part does not match documentation or packaging	Moderate
	Lot/DC on part does not match documentation or packaging	Moderate
	Impossible lot/DC on part or packaging (obsolete)	Major
	Inconsistent part indentation (pin 1, etc.), top or bottom	Major
	Inconsistent country of origin information	Major

[4] *Source: “Counterfeit Material Process Guidebook, Guidelines for Mitigating the Risk of Counterfeit Material in the Supply Chain”, Published by the Office of the Assistance Secretary of the Navy (Research, Development & Acquisition) Acquisition and Business Management, June 2017.*

Test Type	Counterfeit Indicator	Strength of Indicator
	Incorrect/erroneous manufacturer logo	Major
	Texture within part indentations	Minor
	Misaligned markings on parts	Minor
	Inconsistent laser etch depth/width	Minor
	Part markings are poor quality	Minor
Physical Dimensions	Package dimensions fail specifications	Major
	Pin count is incorrect	Major
Part Surface Inspection	"Ghosted" markings visible on part surface	Major
	Evidence of flat lapping	Major
	Evidence of micro blasting	Major
	Heat stress (bulges or blisters) on part	Major
	Internal die or wirebonds exposed to surface of part	Major
	Sanding visible across part surface	Major
	Inconsistent texture or color on parts in same lot/DC	Moderate
	Major mechanical damage (chips, scratches, etc.)	Moderate
	Chemical residue or other contamination on part	Minor
	Superficial scratches or chips on part	Minor
	Suspicious laser markings	Minor
	Suspicious texture or color on part	Minor
Lead / Solder Ball Inspection	Reattached leads on part	Major
	Replated part leads (no tooling marks)	Major
	Evidence of micro blasting	Moderate
	Excessive scratches or scrapes on leads	Moderate
	Lead design varies on parts in same lot/DC	Moderate
	Missing leads/balls	Moderate
	Solder splash on leads/balls	Moderate
	Wrong solder ball size	Moderate
	Bent leads on part	Minor
	Deformed leads/balls	Minor
	No exposed copper on end of leads	Minor
	Oxidized/corroded leads/balls	Minor
Marking Permanency	Hidden "ghosted" markings uncovered by mineral spirits (MS)/alcohol	Major
	Internal die or wirebonds exposed by MS/alcohol	Major

Test Type	Counterfeit Indicator	Strength of Indicator
	Sanding underneath surface uncovered by MS/alcohol	Major
	Surface coating is removed by MS/alcohol	Major
	Ink marking is removed by MS/alcohol	Moderate
Surface Scrape	Sanding underneath surface exposed by razor knife	Major
	Surface coating is removed by a razor knife	Major
Surface Finish Permanency	Hidden "ghosted" markings uncovered by acetone	Major
	Hidden "ghosted" markings uncovered by aggressive solvents	Major
	Internal die or wirebonds exposed by acetone	Major
	Internal die or wirebonds exposed by aggressive solvents	Major
	Sanding underneath surface uncovered by acetone	Major
	Sanding underneath surface uncovered by aggressive solvents	Major
	Surface coating is removed by acetone	Major
	Surface coating is removed by aggressive solvents	Major
	Ink marking is removed by acetone	Minor
X-Ray Fluorescence	Incorrect lead plating composition	Moderate
	Inconsistent lead plating composition	Minor
Radiological (X-ray)	Cracked or damaged die	Major
	Damaged or deformed lead frame	Major
	Double ball bonds	Major
	Inconsistent die size or design on parts in same lot/DC	Major
	Inconsistent lead frame size or design on parts in same lot/DC	Major
	Inconsistent wire bond placement on parts in same lot/DC	Major
	Incorrect wire bond material	Major
	Missing wire bonds	Major
	Inconsistent die/lead frame thickness on parts in same lot/DC	Minor
	Inconsistent wire bond thickness on parts in same lot/DC	Minor
	Misaligned die	Minor
Scanning Acoustic Microscopy	Hidden "ghosted" markings visible by shallow scan	Major
	Inconsistent die size or design on parts in same lot/DC	Major
	Inconsistent lead frame size or design on parts in same lot/DC	Major
	Die delamination visible with CSAM scan	Minor
Decapsulation	Cracked or damaged die	Major
	Impossible date code (die year after part DC)	Major

Test Type	Counterfeit Indicator	Strength of Indicator
	Inconsistent die design on parts in same lot/DC	Major
	Inconsistent die size or design on parts in same lot/DC	Major
	Inconsistent lead frame design on parts in same lot/DC	Major
	Inconsistent OEM or logo on parts in same lot/DC	Major
	Inconsistent part number on parts in same lot/DC	Major
	Incorrect wire bond material	Major
	Wrong OEM or logo	Major
	Misaligned die	Minor
	Mismatched part number	Minor
	Part is more difficult to decap compared to known good	Minor
	Poor quality (e.g., traces, spacing, contamination)	Minor
Electrical Test	Code/programming left over in parts	Major
	Electrical failures are gross (wrong/damaged)	Major
	One-time programmable parts can't be programmed	Major
	25% or higher electrical failure rate	Moderate
	10% or higher electrical failure rate	Minor
	5% or higher electrical failure rate	Minor
	Electrical failures are marginal (stress)	Minor
	Non-traditional electrical test variation	Minor
Known Good Part Comparison	Unmatched pin 1 indicator	Moderate
	Unmatched dimple placement	Moderate
	Unmatched font or lot format	Moderate
	Unmatched lead design	Moderate
	Unmatched lead frame	Minor
	Unmatched die markings	Minor
OEM Support	Component manufacturer states parts are likely counterfeit	Major
	Component manufacturer states parts are possibly counterfeit	Moderate