Nuclear Regulatory Commission
Office of the Chief Information Officer
Computer Security Process

Office Instruction:	**CSO-PROS-0006**
Office Instruction Title:	**Counterfeit and Compromised ICT Product Detection Process**
Revision Number:	**1.0**
Effective Date:	**14-Apr-2021**
Primary Contacts:	**Kathy Lyons-Burke**
Responsible Organization:	**OCIO/CSO**
Summary of Changes:	CSO-PROS-0006, "Counterfeit and Compromised ICT Product Detection Process," defines the process that must be used to identify Information and Communications Technology counterfeit products.
ADAMS Accession No.:	ML21048A050

Agency Official	**Approval Signature and Date**
Garo Nalabandian *for* Jonathan Feibus Chief Information Security Officer (CISO) Office of the Chief Information Officer (OCIO)	Garo Nalabandian Digitally signed by Garo Nalabandian Date: 2021.04.14 09:21:34 -04'00'

Table of Contents

Computer Security Process
CSO-PROS-0006
Counterfeit and Compromised ICT Product Detection Process

1 PURPOSE

In September of 2018, the Department of Defense (DOD) issued a report entitled “Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States” [EO 13806 Assess] to the President in Fulfillment of Executive Order 13806 [EO 13806]. The report identifies ten major risk archetypes and counterfeit issues are identified as part of those risks. The report further states:

> *“A global industrial base means increased supply chain risk associated with foreign provision, including counterfeits, lack of traceability, and insufficient quality controls throughout supply tiers. The Department of Commerce’s Bureau of Industry and Security surfaced several vulnerabilities in the electronics supply chain, including counterfeits, a lack of traceability, and insufficient quality controls throughout supply tiers. Imports of electronics lack the level of scrutiny placed on U.S. manufacturers, driving lower yields and higher rates of failures in downstream production, and raising the risk of “Trojan” chips and viruses infiltrating U.S. defense systems.”*

CSO-PROS-0006 defines the process that must be followed to identify Information and Communications Technology (ICT) counterfeit products prior to deployment.

2 GENERAL REQUIREMENTS

All systems and system components must be validated to be genuine and not altered prior to deployment and must be monitored continuously until the components are removed from operation to ensure they are not altered in an unauthorized manner.

The COR must notify the following when a counterfeit or potential counterfeit component is identified:

- Branch chief or immediate supervisor
- Chief Information Officer (CIO)
- CISO
- Contracting Officer (CO)
- Enterprise architect
- Government-Industry Data Exchange Program (GIDEP)
- Information system security manager

3 INFORMATION AND COMMUNICATIONS TECHNOLOGY COUNTERFEIT DETECTION ROLES AND RESPONSIBILITIES

Table 1 provides the roles and responsibilities associated with NRC detection of ICT counterfeit products.

Table 1: ITC Counterfeit Product Detection Roles and Responsibilities

Role	Responsibilities
Chief Acquisition Officer (CAO)	• Coordinates with other agency officials to ensure that security and privacy requirements are defined in organizational procurements and acquisitions. • Ensures appropriate requirements are in all acquisitions to address possible counterfeit products.
Chief Information Officer (CIO)	• Reviews and approves ITC acquisitions. • Works collaboratively with the CAO to identify needed modifications to the ICT acquisition methodology to address possible counterfeit products.
Chief Information Security Officer (CISO)	• Ensures OCIO processes and procedures exist to detect counterfeit and compromised ICT products prior to their deployment. • Ensures that the agency enterprise architecture includes ICT risk requirements to facilitate the allocation of ICT controls to agency information systems and the environments in which those systems operate. • Ensures that processes used to assess risk incorporate a supply chain risk assessment (SCRA).
Contracting Officer (CO)	• Has delegated authority to enter into, administer, and terminate Government contracts. • Manages contracts and oversees their implementation. • In collaboration with the CISO and CORs, ensures agency's contracting policies and contracts adequately address ICT security requirements and possible counterfeit products.
Contracting Officer's Representative (COR)	• Delegated by the CO to peform certain roles during the administration of the contract (see COR Delegation and Appointment Memordanum for specifics). • Performs contract management activities and functions to ensure contractors meet the commitment of their contracts and proper development of requirements, including detection of possible counterfeit products. When the COR is not at the location of product delivery, the COR must appoint a representative to perform potential counterfeit detection.
Enterprise Architect	• Assists with integration of the organizational risk management strategy and system-level security and privacy requirements into program, planning, and budgeting activities, the System Development Life Cycle (SDLC), acquisition processes, security and privacy (including supply chain) risk management, and systems engineering processes.

Table 1: ITC Counterfeit Product Detection Roles and Responsibilities

Role	Responsibilities
	• Maintains information regarding counterfeit products that may impact NRC.
Information System Security Manager (ISSM) – formerly the ISSO	• Serves as a principal advisor on all matters, technical and otherwise, involving the controls for the system. • Assists in the development of the system-level security and privacy requirements. • Obtains an independent system risk assessment of supply chain related information and artifacts that assesses supply chain risks associated with systems, system components, and system services initially and when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain. • Ensures that information and Communications Technology counterfeit products are identified prior to deployment and during operations and maintenance.
Mission or Business Owner	• Establishes security and privacy requirements that ensure the successful conduct of the organization's missions and business operations, including counterfeit product detection.
Project Manager (PM)	• Performs program and project management activities and functions in developing accurate government requirements, defining measurable performance standards, and managing life cycle activities to ensure that intended outcomes are achieved • Works with the ISSM to ensure counterfeit products are identified prior to deployment
Security or Privacy Architect	• Ensures that stakeholder protection needs and the corresponding system requirements necessary to protect organizational missions and business functions and individuals' privacy are adequately addressed in the enterprise architecture including reference models, segment architectures, and solution architectures (systems supporting mission and business processes) • Serves as the primary liaison between the enterprise architect and the systems security or privacy engineer and coordinates with system owners, common control providers, and system security or privacy officers on the allocation of controls • Advises authorizing officials, chief information officers, senior accountable officials for risk management or risk executive (function), senior agency information security officers, and senior agency officials for privacy on a range of security and privacy issues • Maintains information regarding counterfeit products that may impact NRC

4 PRIOR TO ACQUISITION

Use CSO-PROS-0006, "Information and Communications Technology Acquisition Process" to perform supply chain risk management for the acquisition of ICT. Where possible, requirements

for the contractor to perform counterfeit detection and traceability before delivery shall be included within the standard contract template so that the requirements are included in all contracts.

Requirements identified in the statement of work for all systems, system components, and system services must include integrity verification of software and firmware components. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Security and Privacy Controls for Information Systems and Organizations" [SP 800-53] identifies integrity controls that may be used.

If the acquisition is for components, the COR consults with GIDEP reports on counterfeit components to determine if the components being acquired have known counterfeits.

5 PRIOR TO ACCEPTANCE

When the SOW requires the contractor to perform counterfeit detection and traceability, the COR must examine the documentation provided by the contractor that details the counterfeit detection work that was performed and the results of that work to ensure enough counterfeit detection effort was applied.

When the SOW does not require the contractor to perform counterfeit detection, the COR must perform the following due diligence to identify potential counterfeit components. The COR must not accept suspected or confirmed counterfeit components.

- For hardware and software:
  - Examine NRC enterprise architecture counterfeit database to determine if the components have been identified as potential counterfeit components at NRC previously. If so, contact the component manufacturer for assistance in counterfeit detection.
  - Examine GIDEP data to determine if the component has been counterfeited and use the information available to identify if the delivered component might be counterfeit. If so, contact the component manufacturer for assistance in counterfeit detection.
  - Examine the component manufacturer online information to see if any counterfeit detection information is available and if so, perform the suggested steps.
  - Use manufacturer method to ensure product has not been modified (e.g., visual scanning techniques for hardware and checking for digital signatures in software)

6 AFTER ACCEPTANCE

Once we have accepted a product/service, we have to continue to monitor the product to ensure we address counterfeit products.

Risk assessments performed on the system or service must include counterfeit checks (e.g., web application scanning, software integrity checks, visual examination).

Continuous monitoring must include counterfeit and traceability checks.

APPENDIX A ACRONYMS

CAO	Chief Acquisition Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CO	Contracting Officer
COR	Contracting Officer's Representative
CSO	Computer Security Organization
DOD	Department of Defense
EO	Executive Order
GIDEP	Government-Industry Data Exchange Program
GSA	General Services Administration
ICT	Information and Communications Technology
ICT	Information and Communications Technology
ISSM	Information System Security Manager
ISSO	Information System Security Officer
NIST	National Institute of Standards and Technology (NIST)
NRC	Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
PM	Project Manager
SCRA	Supply Chain Risk Assessment
SDLC	System Development Life Cycle
SOW	Statement of Work
SP	Special Publication

APPENDIX B REFERENCES

LAWS AND EXECUTIVE ORDERS

[EO 13806] Executive Order (EO) 13806, "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," July 21, 2017

[FISMA] Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.govinfo.gov/app/details/PLAW-113publ283

[FITARA] Federal Information Technology Acquisition Reform Act (P.L. 115-88), November 2017. https://www.govinfo.gov/app/details/PLAW-115publ88

POLICIES, REGULATIONS, DIRECTIVES, AND INSTRUCTIONS

[OMB A-123] Office of Management and Budget Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf

[OMB A-130] Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

STANDARDS, GUIDELINES, AND REPORTS

[CDA_FL] Tehranipoor, M., "Counterfeit Detection and Avoidance: Introduction to Hardware Security & Trust," University of Florida, April 5, 2018

[CDSE_SCRM] Center for Development of Security Excellence (CDSE) Deliver Uncompromised: Supply Chain Risk Management

[Conun_2020] The Counterfeit Conundrum: 5 Best Practices for Mitigating Counterfeit Issues in the Electronics Industry, 2020

[Detect_Meth] Hewett, H., "Methods Used in the Detection of Counterfeit Electronic Components," Electro-Comp Services, Inc., Clearwater, FL, USA

[DIBA_Counterfeit] Defense Industrial Base Assessment: Counterfeit Electronics, U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, January 2010

[DoD_Parts_2014] Gansler, J. S., Lucyshyn, W., and Rigilano, J., Addressing Counterfeit Parts in the DoD Supply Chain, Center for Public Policy and Private Enterprise, School of Public Policy, March 2014

[EO 13806 Assess] Defense Industrial Base Assessment: Counterfeit Electronics, U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, January 2010 Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States; Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806, September 2018

[FIPS 200]	NIST Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006. https://doi.org/10.6028/NIST.FIPS.200
[GIDEP]	Government-Industry Data Exchange Program
[Mandate]	Hayward , H. A., Meraglia , J., and Miller, M., The new Federal anti counterfeiting mandate for military electronics: what will it take to comply with Sec. 818? The costs of counterfeiting vs. the costs of compliance, Applied DNA Sciences, Inc.
[SP 800-161]	NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, April 2015. https://doi.org/10.6028/NIST.SP.800-161
[SP 800-37]	NIST SP 800-37, Risk Management Framework for Information Systems and Organizations, Revision 2, December 2018. https://doi.org/10.6028/NIST.SP.800-37
[SP 800-39]	NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011. https://doi.org/10.6028/NIST.SP.800-39
[SP 800-53]	NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations, September 2020. https://doi.org/10.6028/NIST.SP.800-53r5
[SW_Assur]	Software Assurance in Acquisition: Mitigating Risks to the Enterprise, Software Assurance (SwA) Acquisition Working Group, Mary Linda Polydys and Stan Wisseman, National Defense University, Information Resources Management College, February 2009
[Test_Meth]	Ya A Shchenikov et al, Model for selecting test methods of detecting fraudulent electronic components, 2020, J. Phys.: Conf. Ser. 1515 022059

NRC DOCUMENTS

[CSO-PLAN-0100]	CSO-PLAN-0100, “Enterprise Risk Management Program Plan”
[CSO-PROS-0005]	CSO-PROS-0005, “Information and Communications Technology Acquisition Process”
[CSO-PROS-1323]	CSO-PROS-1323, Information Security Continuous Monitoring Process
[MD 11.1]	Management Directive 11.1, NRC Acquisition of Supplies and Services
[MD 12.5]	Management Directive 12.5, NRC Cybersecurity Program
[Risk strategy]	NRC Risk Management Strategy, Revision 1.0, ML20266G443
[SCRM Strategy]	NRC Supply Chain Risk Management Strategy, Revision 1.0, September 2020, ML20310A085

CSO-PROS-0006 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
14-Apr-21	1.0	Initial release	Monthly Office Meetings.	None needed.