OE-3: 2022-01 October 2022

Suspect/Counterfeit and Fraudulent Networking Products

PURPOSE

This Operating Experience Level 3 (OE-3) document is being issued pursuant to DOE Order 210.2A, *DOE Corporate Operating Experience Program*, to raise awareness of suspect/counterfeit and fraudulent Cisco Systems, Inc. (Cisco) networking equipment that may have been procured from certain distributors across the Department of Energy (DOE) Enterprise.

Specifically, equipment provided to DOE may have originated from one or more entities listed in Attachment 1, and referred to in this OE-3 as, collectively, "Pro Network." According to a recently filed indictment,[1] Pro Network allegedly sold fraudulent and counterfeit Cisco networking devices in the United States and around the world. Pro Network may have sold the equipment to DOE either directly or through one or more other entities. We are providing this OE-3 so that DOE personnel can aid in determining if DOE obtained any Cisco networking equipment from Pro Network or suspect/counterfeit or fraudulent devices from other sellers.

The Pro Network indictment contains only charges and is not evidence of guilt.[2] The defendant in the case is presumed innocent and is entitled to a fair trial at which the government has the burden of proving guilt beyond a reasonable doubt.

BACKGROUND

According to the indictment, a federal grand jury charged the CEO of Pro Network with running an operation from 2013 to 2022 to traffic in fraudulent and counterfeit goods. During this period, he allegedly conspired with suppliers in China and Hong Kong to import low-quality, modified computer networking devices with counterfeit labels, stickers, boxes, documentation, and packaging that made the goods falsely appear to be new, genuine, and high-quality devices manufactured by Cisco. Pro Network allegedly then resold those devices to resellers and end users.

During the alleged conspiracy, Pro Network purportedly imported and resold tens of thousands of fraudulent and counterfeit Cisco devices. According to the indictment, had the devices been new and genuine products, they would have carried an estimated total retail value of over one billion dollars. Additionally, Cisco allegedly sent Pro Network a number of cease-and-desist letters that stated that "counterfeit technology products potentially pose serious health and safety risks to the end users of such products." According to the indictment, even after receiving these letters, Pro Network continued to sell counterfeit and fraudulent Cisco products.

[1] *See* Indictment, *United States v. Aksoy*, 22-cr-464 (District of New Jersey) and Press Release, CEO of Dozens of Companies and Entities Charged in Scheme to Traffic an Estimated $1 Billion in Fraudulent and Counterfeit Cisco Networking Equipment (July 8, 2022) (online file with Department of Justice, (July 8, 2022) (online file with Department of Justice, Office of Public Affairs).

[2] *See Indictment*

SUSPECT/COUNTERFEIT AND FRAUDULENT INDICATORS

Based on the indictment, possible indicators that Cisco networking equipment purchased by DOE is suspect/counterfeit or fraudulent could include the following:

1. Any product purchased directly or through another company that came from one of the entities listed in Attachment 1.

2. Items purchased from other entities that were not authorized Cisco resellers and/or that were sold significantly below the manufacturer's suggested retail price (MSRP).

3. Products containing falsified identifiers such as incorrect serial numbers.

4. Products that could not be registered into Cisco's SmartNet services. SmartNet provides technical support and additional Cisco services.[3]

RECOMMENDATIONS

Given the breadth and depth of DOE's missions, the undetected use of counterfeit or fraudulent parts has the potential to cause near and long-term adverse consequences, posing potential safety risks to workers, the public, the environment, and/or DOE missions. Furthermore, these items may pose potential security risks.

The DOE enterprise may use the information contained in this OE-3 to conduct a search of procurement information and determine if purchases have been made of suspect/counterfeit or fraudulent Cisco networking equipment. If items are found to have been purchased from Pro Network or are otherwise suspect/counterfeit or fraudulent, applicable requirements in 10 CFR Part 830, *Nuclear Safety Management,* Subpart A, *Quality Assurance Requirements*, and DOE O 414.1D, *Quality Assurance,* must be followed. Please note that DOE sites may have additional local processes or procedures for handling suspect/counterfeit items. The Department of Justice suggests that DOE might additionally reach out to Cisco for assistance in confirming whether an item is a genuine product.

SUMMARY

Suspect/counterfeit or fraudulent networking equipment may pose potential safety or security risks. This OE-3 is not limited to any specific Cisco part number or part type. The DOE complex may have such suspect/counterfeit or fraudulent devices, especially if the items came from any of the entities listed in Attachment 1, either directly or through another entity. If so, requirements of 10 CFR Part 830, Subpart A, and DOE O 414.1D may be applicable. Additional specific actions and further consultation and coordination with local legal counsel and contacting Cisco to confirm whether the device in question is genuine is recommended. EHSS recommends that sites perform a search through their procurement systems to determine whether purchases have been made of suspect/counterfeit or fraudulent Cisco networking equipment and, if so, take appropriate action.

REFERENCES

10 CFR Part 830, *Nuclear Safety Management*, Subpart A, *Quality Assurance Requirements*

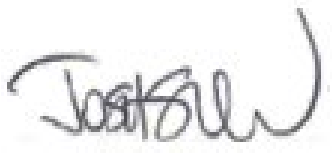
DOE O. 414.1D, *Quality Assurance*

Indictment, *United States v. Aksoy*, 22-cr-464 (District of New Jersey).

[3] More information about how to identify suspect/counterfeit or fraudulent items is in DOE O 414.1D, *Quality Assurance*, and at Cisco's website at https://www.cisco.com/c/en/USabout/legal/brand-protection/identity-counterfeit-products.html.

Questions regarding this OE-3 document can be directed to Gabrielle Holcomb at 240-255-8299 or gabrielle.holcomb@hq.doe.gov or to counterfeit@hq.doe.gov.

This OE-3 document requires no formal follow-up report or written response. However, EHSS would appreciate being informed if sites identify Pro Network purchases by contacting counterfeit@hq.doe.gov.



Josh Silverman
Director
Office of Environmental Protection and ES&H Reporting
Office of Environment, Health, Safety and Security

ATTACHMENT 1: LIST OF PRO NETWORK ENTITIES

Pro Network operated through multiple business entities and online storefronts. Entities listed in the indictment are as follows:

Pro Network Companies	Approximate Month and Year of Formation	State of Formation
Pro Network LLC	August 2013	New Jersey
Netech Solutions LLC	November 2016	Florida
Target Network Solutions LLC	January 2017	Florida
Easy Network LLC	April 2017	New Jersey
ACE NETUS LLC (a/k/a Ace Network)	April 2017	New Jersey
My Network Dealer LLC	April 2017	New Jersey
1701 Doral LLC	May 2017	New Jersey
Maytech Trading LLC	August 2017	Florida
NFD Trading LLC	September 2017	Florida
Kenet Solutions LLC	September 2017	Florida
Team Tech Global LLC	January 2018	New Jersey
Tenek Trading LLC	January 2018	Florida

Pro Network Companies	Approximate Month and Year of Formation	State of Formation
The Network Gears LLC	February 2018	Florida
All Networking Solutions LLC (a/k/a All Network)	April 2018	Florida
San Network LLC	October 2018	Florida
Pro Network US Inc.	January 2019	Florida
Jms Tek LLC	August 2019	Florida
Renewed Equipment LLC	August 2021	Florida
Pro Ship US LLC	August 2021	Florida

Amazon Storefronts

Pro Network Amazon Storefront	Approximate Date of Earliest Known Activity
Albus Trade Hub	January 2014
EasyNetworkUS	March 2014
Get Better Trade	July 2015
Mercadeal	February 2017

Pro Network Amazon Storefront	Approximate Date of Earliest Known Activity
Netech Solutions	February 2018
Netkco LLC	September 2014
NFD Trading LLC	January 2018
Palm Network Solutions	June 2017
Renewed Equip	August 2017
Servtaur	August 2019
Smart Network	July 2017
SOS Tech Trade	August 2017
Target-Solutions	September 2020
TeamTech Global	March 2016
TradeOrigin US	August 2015

eBay Storefronts

Pro Network eBay Storefront	Approximate Date of Earliest Known Activity
connectwus	March 2014

Pro Network eBay Storefront	Approximate Date of Earliest Known Activity
futuretechneeds	July 2017
getbettertrade	July 2017
getontrade	April 2016
maytechtradingllc	October 2017
netechsolutions	April 2017
netkco	September 2014
nfdtrading	February 2018
smartnetworkusa	January 2014
tenektradingllc	May 2018