Department of Justice

FOR IMMEDIATE RELEASE
THURSDAY, MAY 6, 2010
WWW.JUSTICE.GOV

CRM
(202) 514-2007
TDD (202) 514-1888

DEPARTMENTS OF JUSTICE AND HOMELAND SECURITY ANNOUNCE 30 CONVICTIONS, MORE THAN $143 MILLION IN SEIZURES FROM INITIATIVE TARGETING TRAFFICKERS IN COUNTERFEIT NETWORK HARDWARE

WASHINGTON - Operation Network Raider, a domestic and international enforcement initiative targeting the illegal distribution of counterfeit network hardware manufactured in China, has resulted in 30 felony convictions and more than 700 seizures of counterfeit Cisco network hardware and labels with an estimated retail value of more than $143 million.

The results of the operation were announced by Assistant Attorney General Lanny A. Breuer of the Criminal Division, Assistant Director Gordon Snow of the FBI's Cyber Division, Assistant Secretary John Morton of U.S. Immigration and Customs Enforcement (ICE) and Commissioner Alan Bersin of U.S. Customs and Border Protection (CBP). In addition to the convictions and seizures, according to the CBP there has been a 75 percent decrease in seizures of counterfeit network hardware at U.S. borders from 2008 to 2009. In addition, nine individuals are facing trial and another eight defendants are awaiting sentencing.

This operation is a joint initiative by the FBI, ICE and CBP working with the U.S. Attorneys' Offices around the country, the Criminal Division's Computer Crime and Intellectual Property Section and the National Intellectual Property Rights Coordination Center. Through aggressive investigation and prosecution, the initiative seeks to protect computer networks and the nation's IT infrastructure from failures associated with counterfeit network hardware, including network routers, switches, network cards, and devices that protect firewalls and secure communications that have been intercepted both domestically and abroad.

Today, as a part of this joint initiative, Ehab Ashoor, 49, a Saudi Citizen who resides in Sugarland, Texas, was sentenced in the Southern District of Texas to 51 months in prison and ordered to pay $119,400 in restitution to Cisco Systems. A federal jury found Ashoor guilty on Jan. 22, 2010, of charges related to his trafficking in counterfeit Cisco products. According to evidence presented at trial, Ashoor purchased counterfeit Cisco Gigabit Interface Converters (GBICs) from an online vendor in China with the intention of selling them to the U.S. Department of Defense for use by U.S. Marine Corps personnel operating in Iraq. The computer network for which the GBICs were intended is used by the U.S. Marine Corps to transmit troop movements, relay intelligence and maintain security for a military base west of Fallujah, Iraq. The case was investigated by ICE and the Defense Criminal Investigative Service and was prosecuted by the U.S. Attorney's Office for the Southern District of Texas.

On Jan. 25, 2010, in the Central District of California, Yongcai Li, 33, a resident of China, was sentenced to 30 months in prison and ordered to pay $790,683 in restitution to Cisco Systems

Inc., as a result of his conviction for trafficking in counterfeit Cisco computer products. Li carried out the scheme while doing business as Gaoyi Tech, a company located in Shenzhen, China. Li procured counterfeit Cisco products in China in response to orders and then shipped the products to the United States. Li was arrested by FBI agents in January 2009 while visiting Las Vegas and was prosecuted in Los Angeles. This case was investigated by FBI and prosecuted by the U.S. Attorney's Office for the Central District of California.

"Trafficking in counterfeit computer components is a problem that spans the globe and impacts most, if not all, major network equipment manufacturers. As this operation demonstrates, sustained cooperation between law enforcement and the private sector is often a critical factor in disrupting and dismantling criminal organizations that threaten our economy and endanger public safety," said Assistant Attorney General Breuer. "Through the IP Task Force, and with recently announced additional resources, we are intensely focused on bringing to justice those who engage in piracy and counterfeiting."

To date, ICE agents have seized counterfeit Cisco products having an estimated retail value of more than $35 million. ICE investigations have led to eight indictments and felony convictions to date. CBP has made 537 seizures of counterfeit Cisco network hardware since 2005, and 47 seizures of Cisco labels for counterfeit products. In total, ICE and CBP seized more than 94,000 counterfeit Cisco network components and labels with a total estimated retail value of more than $86 million during the course of the operation.

"These cases involve greedy businessmen hocking counterfeit and substandard hardware to any buyer—whether it could affect the health and safety of others in a hospital setting or the security of our troops on the battlefield," said John Morton, Assistant Secretary of Homeland Security for ICE. "They pose a triple threat to our nation by stealing from our economy, threatening U.S. jobs and potentially putting the safety of our citizens at risk."

"Operation Network Raider is an outstanding example of cooperation between CBP and its law enforcement partners to combat counterfeiting that threatens our economy," said CBP Commissioner Alan Bersin. "Protecting businesses against these threats is a top priority for CBP, and we are committed to continuing our work with law enforcement and the private sector to ensure the safety and security of the American people."

The FBI, building upon its earlier success in Operation Cisco Raider, worked closely with law enforcement partners including ICE, Defense Criminal Investigative Service, General Services Administration, Department of Interior, Internal Revenue Service and the Royal Canadian Mounted Police. During the last four years as part of Operation Network Raider and Cisco Raider, the FBI has executed 36 search warrants seizing counterfeit network components with an estimated retail value of more than $7 million.

"Individuals who break the law by attempting to profit from counterfeit technology do the marketplace great harm," said FBI Assistant Director Gordon M. Snow. "This case illustrates how effectively the private sector and law enforcement organizations work together to combat fraudulent goods and preserve the integrity of U.S. computer networks and infrastructure."

To date, international enforcement efforts have resulted in five convictions internationally, including one in Canada and four in China. Foreign investigations have led to seizures in France,

China and Canada totaling $17 million worth of counterfeit networking equipment. U.S. law enforcement authorities continue to work with China's Ministry of Public Security (MPS) to combat the manufacture and export of counterfeit network hardware from China. This ongoing work is being facilitated by the IP Criminal Enforcement Working Group of the U.S. -China Joint Liaison Group for law enforcement, which is co-chaired by the Criminal Division and the MPS. The Working Group is dedicated to increasing cooperation in intellectual property enforcement efforts and pursuing more joint IP criminal investigations with China.

The global nature of the problem of trafficking in counterfeit electronics is further reflected in seizures of counterfeit semiconductor devices. From November 2007 to present, CBP and ICE have made more than 1,300 seizures involving 5.6 million counterfeit semiconductor devices. Semiconductors are used extensively in modern products and their proper functioning is critical to the safe and reliable operation of electronics in the aerospace, military, automotive, communications, industrial and consumer electronics sectors. More than 50 seized counterfeit shipments were falsely marked as military or aerospace grade devices. Shipments of seized semiconductors were affixed with counterfeit trademarks from 87 North American, Asian and European semiconductor companies and were destined for importers in the United States and 15 other countries.

Cisco Systems Inc., has provided exceptional assistance throughout these investigations and prosecutions.

Report information on counterfeiting and trademark violations at (866) IPR-2060.