Department of Justice

FOR IMMEDIATE RELEASE
THURSDAY, FEBRUARY 28, 2008
WWW.USDOJ.GOV

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

DEPARTMENTS OF JUSTICE AND HOMELAND SECURITY ANNOUNCE INTERNATIONAL INITIATIVE AGAINST TRAFFICKERS IN COUNTERFEIT NETWORK HARDWARE

Over $76 Million in Counterfeit Cisco Hardware and Labels Seized

WASHINGTON - Assistant Attorney General Alice S. Fisher of the Criminal Division, Assistant Director James Finch of the FBI's Cyber Division, Assistant Secretary Julie L. Myers, U.S. Immigration and Customs Enforcement (ICE), Commissioner W. Ralph Basham, U.S. Customs and Border Protection (CBP), and Inspector Peter Goulet of the Royal Canadian Mounted Police (RCMP) today announced the results to date of an ongoing international enforcement initiative between the United States and Canada that targets the illegal distribution of counterfeit network hardware manufactured in China.

This ongoing initiative has resulted in more than 400 seizures of counterfeit Cisco network hardware and labels with an estimated retail value of more than $76 million. It is being led by ICE, CBP and the FBI working in conjunction with the Criminal Division's Computer Crime & Intellectual Property Section, U.S. Attorney's Offices across the country, and the RCMP.

The initiative targets the illegal importation and sale of counterfeit network hardware, in particular network routers, switches, network cards and modules manufactured by Cisco. By intercepting the counterfeit hardware at ports of entry and dismantling illegal supply chains in the U.S., the operation has achieved significant successes in protecting the public from the risk of network infrastructure failures associated with these counterfeits.

"Counterfeit network hardware entering the marketplace raises significant public safety concerns and must be stopped. This initiative shows that through collaboration among law enforcement agencies and prosecutors worldwide, we can achieve dramatic enforcement results and protect public safety," said Assistant Attorney General Alice S. Fisher of the Criminal Division. "It is critically important that network administrators in both private sector and government perform due diligence in order to prevent counterfeit hardware from being installed on their networks."

The FBI named its portion of this ongoing initiative Operation Cisco Raider - an international, coordinated investigation of 15 cases involving nine FBI field offices. The FBI worked closely with law enforcement partners including ICE, Defense Criminal Investigative Service, General Services Administration, Department of the Interior, Internal Revenue Service, and the RCMP. Over the last two years, Operation Cisco Raider has resulted in 36 search warrants that identified approximately 3,500 counterfeit network components with an estimated retail value of over $3.5 million, and has led to a total of ten convictions and $1.7 million in restitution.

"This operation illustrates the importance of working closely with our partners in both law enforcement and the private sector," said FBI Assistant Director James Finch. "Cisco Systems Incorporated specifically deserves praise for their level of cooperation in this initiative. We will continue these efforts to aggressively investigate counterfeit goods in order to protect U.S. consumers and corporations."

ICE and CBP opened a total of 28 investigations in 17 separate field offices since 2005; eight of those investigations were worked jointly with the FBI and several with the RCMP. ICE agents have conducted 115 seizures of counterfeit Cisco products having an estimated retail value of $20.4 million. ICE investigations have led to six indictments and four felony convictions to date. CBP has made 373 seizures of counterfeit Cisco network hardware since 2005, and 40 seizures of Cisco labels for counterfeit products. All together, ICE and CBP seized more than 74,000 counterfeit Cisco network components and labels with a total estimated retail value of more than $73 million.

"Crimes like these threaten international commerce, national security and the very safety of our citizens," said Julie L. Myers, Homeland Security Assistant Secretary for ICE. 'Throughout this investigation, the cooperation and partnership that we received from Cisco Systems, our law enforcement colleagues, and Chinese counterparts are a clear example of the results that can be realized through industry, interagency and international cooperation."

"The success of this operation demonstrates our commitment to work jointly with our law enforcement partners, as well as the private sector, to stop international trafficking in counterfeit items and protect our consumers and businesses from these dangerous goods," stated CBP Commissioner W. Ralph Basham.

Today in Toronto, Canada, the RCMP charged two individuals and a company with distributing large quantities of counterfeit network components to companies in the United States via the Internet. The RCMP seized approximately 1,600 pieces of counterfeit network hardware with an estimated value of $2 million. This prosecution resulted from a joint initiative between the RCMP, FBI, ICE, and CBP that was aimed at disrupting the flow of counterfeit Cisco networking components in North America.

"Counterfeit products greatly undermine the integrity of our economy," stated Inspector Peter Goulet, Officer in Charge of the RCMP Greater Toronto Area Federal Enforcement Section. "In many cases the end users were unaware that counterfeit products were being placed on their computer networks, and depending on the function of those networks, this could cause serious health and safety concerns."

Some of the cases involved with this initiative across the United States include the following:

- On February 14, 2008, in the Northern District of Georgia, Todd Richard, 33, was sentenced to 36 months' imprisonment and ordered to pay $208,440 in restitution to Cisco Systems, Inc., as a result of his conviction for trafficking in counterfeit Cisco computer products. From late 2003 until early 2007, Richard imported shipments of counterfeit Cisco computer components from China, and separate shipments of counterfeit Cisco labels. He then affixed the fake labels to the fake components and sold the products on eBay, claiming that they were legitimate

Cisco items. Richard sold over $1 million worth of counterfeit Cisco products in this manner. This case was investigated by ICE and prosecuted by the U.S. Attorney's Office for the Northern District of Georgia.

- On January 4, 2008, in the Southern District of Texas, a federal grand jury returned an indictment charging Michael Edman, 36, and his brother Robert Edman, 28, with trafficking in counterfeit Cisco products. The indictment alleges that the Edmans purchased and imported the counterfeit computer network hardware from an individual in China. They later sold the counterfeit Cisco products to retailers of computer network products throughout the United States. According to the indictment, the Edmans shipped some of the counterfeit hardware directly to the Marine Corps, Air Force, Federal Aviation Administration, FBI, defense contractors, universities and financial institutions. These entities had purchased the product from a computer retailer serving as a middleman, which in turn purchased the products from the Edmans (a process known as "drop shipping"). The case was investigated by ICE and is being prosecuted by the U.S. Attorney's Office for the Southern District of Texas.

- On April 17, 2007, in the Northern District of Texas, Mark Thomas Geis, 37, was sentenced to five years in prison and ordered to pay $1.5 million in restitution to Cisco Systems Inc. as a result of his conviction for conspiracy to traffic in counterfeit network hardware. The court found that Geis, doing business as VARGlobal and conducting business via eBay, conspired to traffic in approximately $4.2 million of counterfeit Cisco hardware. This case was investigated by the FBI. Geis had previously been convicted and sentenced to 46 months imprisonment in 2001 for conspiracy to defraud Microsoft Corporation. The case was investigated by the FBI and prosecuted by the U.S. Attorney's Office for the Northern District of Texas.

The problem of trafficking in counterfeit computer components is a global problem, as reflected by last week's announcement by the European Union (EU) and U.S. officials of the first EU-U.S. customs joint operation resulting in the seizure of more than 360,000 counterfeit computer parts and integrated circuits. The joint initiative between the European Commission Tax and Customs Directorate and CBP took place during a three-week period in November and December of 2007. A probe in five countries uncovered a pattern of trade in counterfeit networking equipment and integrated circuits passed off as products from 40 of the world's largest European, U.S., Japanese, and Korean technology companies. Most arrived via air shipment from China, but some were also shipped from Taiwan and Hong Kong.

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 of the U.S. Department of Justice and the MPS. The Working Group is dedicated to increasing cooperation in intellectual property law enforcement efforts and pursuing more joint IP criminal investigations with China.

The initiative announced today is part of a broader Department of Justice initiative to combat all forms of intellectual property crime, including economic espionage, copyright

infringement, and trafficking in counterfeit goods. This broader initiative has led to significant increases in criminal enforcement over the past three years. Through the dedicated efforts of U.S. Attorney's Offices and federal law enforcement across the country, in FY2007, 287 defendants were convicted and sentenced on intellectual property charges, representing a 35 percent increase over FY2006 and a 92 percent increase over FY2005. Additionally, the Department filed 217 intellectual property cases last year, representing a 7 percent increase over cases reported in FY2006 and a 33 percent increase over cases reported in FY2005.

Cisco Systems, Inc. has cooperated with U.S. and Canadian law enforcement authorities and provided exceptional assistance throughout these investigations.

The investigations are ongoing throughout the U.S.

###

08-150