

# Cyber Export Control Investigations

James Plitt,  
Director  
DHS ICE,  
Cyber Crimes Center  
703.293.6291  
[james.plitt@dhs.gov](mailto:james.plitt@dhs.gov)



U.S. Immigration  
and Customs  
Enforcement

Version: 1 November 2005

# Cyber Export Control Investigations

## Introduction:

### Law Enforcement for a changing world:

- Illegal export of strategic technology
- 11 September 2001
- Growth of state sponsored terrorism
- WMD proliferation
- Illegal financial transactions



U.S. Immigration  
and Customs  
Enforcement

# Cyber Export Control Investigations

## Introduction:

The creation of the U.S. Department of Homeland Security (DHS) and, within DHS, U.S. Immigration and Customs Enforcement (ICE) (March 2003):

- Prevent international criminals from obtaining strategic technology, licensable dual-use commodities, weapons, munitions, funds and technical support.
- Protect the American public from the introduction of WMD and other instruments of terror into the United States by investigating those predicate immigration and customs-related crimes, without which most acts of terrorism could not occur (Munitions Smuggling, Human Smuggling, International Money Laundering, Fraudulent Charities, etc.)



U.S. Immigration  
and Customs  
Enforcement



# Cyber Export Control Investigations

## Introduction:

The ICE Cyber Crimes Center (C3) is responsible for the Internet and Digital Data Media (computers and other digital storage devices) aspects of ICE's investigations, including those investigations involving export controls and the smuggling of humans and contraband that may be instrumental in national security threats:

- Cyber Investigative Services – Examples include the analysis of Internet file transfers and communication data and the establishment of undercover websites and email accounts.
- Cyber Technical Services – Examples include Digital Evidence Recovery and Data Mining.



U.S. Immigration  
and Customs  
Enforcement

# Cyber Export Control Investigations

## Unique Aspects of Cyber Export Control Investigations:

- Intangible Technology Transfer
- Cyber Trends and Outlook
- Internet Undercover Operations
- Computer Forensics



U.S. Immigration  
and Customs  
Enforcement

# Cyber Export Control Investigations

## Unique Aspects of Cyber Export Control Investigations:

### Intangible Technology Transfer:

- Traditional Technology Transfers -The commodities or technical data is in tangible form. The transfer moves across a clearly defined border.
- Intangible Technology Transfer - The technical data is intangible, for example electronic files on the Internet, and the border is less definitive. There are two types of Intangible Technology Transfers: General Intangible Transfers and Deemed Exports.



U.S. Immigration  
and Customs  
Enforcement

# Cyber Export Control Investigations

## Unique Aspects of Cyber Export Control Investigations:

### Intangible Technology Transfer:

#### General Intangible Transfers:

- Illegal Export of Technical Assistance – The transfer of technology during the delivery of services, such as training, consulting, or advisory contracts, via personal exchanges or telecommunications, including phone, email, blogs, and Internet Relay Chat (IRC)
- Electronic Transfer of Documentary Technology or Technical Data – The transfer of blueprints, diagrams, manuals, instructions, software, and/or engineering development, test, and performance data via telecommunications or stored digital media.



U.S. Immigration  
and Customs  
Enforcement

# Cyber Export Control Investigations

## Unique Aspects of Cyber Export Control Investigations:

### Intangible Technology Transfer:

#### Deemed Exports:

- Non-Traditional Border Concept – Usually occurs within a country, instead of across physical, international borders.
- Typically involves a transfer to one or more foreign nationals.



U.S. Immigration  
and Customs  
Enforcement

# Cyber Export Control Investigations

## Unique Aspects of Cyber Export Control Investigations:

### Cyber Trends and Outlook:

#### Trends:

- Network Intrusions – The number of intrusions into corporate and government computer networks is steadily increasing. Typical techniques include Hacking, Spyware, and Electronic and Non-Electronic Phishing.
- Tracking of Law Enforcement Personnel and Information Technology Assets – International criminals and terrorists identify and monitor investigators and electronic investigative inquiries. One method is to establish false websites that request Export Controlled Technology.



U.S. Immigration  
and Customs  
Enforcement

# Cyber Export Control Investigations

## Unique Aspects of Cyber Export Control Investigations:

### Cyber Trends and Outlook:

#### Trends:

- Encryption – Encryption, which hides and locks the contents of computer files such as emails and their attachments, is increasing as it becomes more readily available.
- Anonymizers – Those devices and Internet communications methods that hide the source of probes and the identity of the sender are increasing in complexity.
- Internet Payment Methods – Unregulated, Internet non-bank, banking and payment services disguise the source of illegal technology transfer investment capital and facilitate the money laundering of proceeds.



U.S. Immigration  
and Customs  
Enforcement

# Cyber Export Control Investigations

## Unique Aspects of Cyber Export Control Investigations:

### Cyber Trends and Outlook:

#### Outlook:

- Internet Growth – Use of the Internet by individuals and corporations is continuing to double every six months. There are more than 1 billion websites.
- Criminal Use of Cyber Security – Criminals and criminal organizations will continue to strengthen their own computer network security as these technologies become more easy to access and use and as technologies exponentially permeate society.



U.S. Immigration  
and Customs  
Enforcement

# Cyber Export Control Investigations

## Unique Aspects of Cyber Export Control Investigations:

### Internet Undercover Operations:

- Undercover websites and email accounts provide your undercover investigation with a “virtual” physical, credible presence or “storefront” and an electronic means of communications that offers unique intelligence on your suspects.
- Internet undercover assets include websites, emails, telecommunications connections, hardware, and software. These assets must be protected from viruses, software vulnerabilities, weak firewall programs, and erroneous storage of identity information.



U.S. Immigration  
and Customs  
Enforcement

# Cyber Export Control Investigations

## Unique Aspects of Cyber Export Control Investigations:

### Internet Undercover Operations:

- Internet undercover assets should have no connection to official government networks or systems and blind links to government intranet websites, should be clean of government administrative or investigative information, and should not have been purchased through government contracts.
- Internet undercover assets should take advantage of free email services and other vogue Internet methods.



U.S. Immigration  
and Customs  
Enforcement

# Cyber Export Control Investigations

## Unique Aspects of Cyber Export Control Investigations:

### Computer Forensics:

- Cyber Export Control Investigations typically involve the forensic analysis of computers near the end of the operation and often as a result of search warrants and court-authorized intercepts during the operation. This analysis collects information and evidence and recovers the historical activities of the crime to identify additional investigative targets.
- The computer forensic examiner will collect various information from the digital storage media, including emails, documents, user names and passwords, Internet search history, temporary files, and deleted files.



U.S. Immigration  
and Customs  
Enforcement

# Cyber Export Control Investigations

## Unique Aspects of Cyber Export Control Investigations:

### Computer Forensics:

- The average size of a computer hard drive seized by U.S. federal law enforcement is 100 Gigabytes (=100,000 Megabytes). The average forensic analysis time for 100 Gigabytes is six weeks. Computer forensics has surmounted the issues of data extraction and is now focusing on efficient data mining.



U.S. Immigration  
and Customs  
Enforcement

# Cyber Export Control Investigations

## Unique Aspects of Cyber Export Control Investigations:

### Computer Forensics:

- This seizure in San Francisco totaled approximately 8 Terabytes (=8,000 Gigabytes = 8,000,000 Megabytes = 5,5 Million 3.5-inch diskettes).



U.S. Immigration  
and Customs  
Enforcement