Cyber Training

C3's new Cyber Training section partners with several internal and external entities to develop specialized cyber-related training for ICE employees.

Example of courses offered by C3 are as follows:

- Non-Forensics Supervisor Training
- Cyber Crimes Investigative Course (CCIC): Basic techniques for conducting cyber investigations
- Cyber Crimes Undercover Course (CCUC): Techniques for conducting undercover cyber investigations
- Peer-to-Peer Network Course (P2P): Specialized techniques for conducting investigations on file-sharing networks
- C3 101: Internal orientation on C3 for ICE employees
- Advanced Certification in Computer Forensics Training (ACERT)

ICE

Cyber Crimes Center
11320 Random Hills Road, Fairfax, VA 22030

Phone: 703-293-8005
Fax: 703-293-9127

www.ice.gov

To report drug smuggling:
1-866-DHS-2-*ICE*
1-866-347-2423

To report child exploitation:
www.cybertipline.com
(NCMEC)

04/2010

C3
Cyber Crimes Center

U.S. Immigration and Customs Enforcement

U.S. Immigration and Customs Enforcement (ICE), the largest investigative agency in the Department of Homeland Security (DHS), is charged with protecting national security by enforcing the nation's immigration and customs laws. One of ICE's leading priorities in this mission is combating criminal activity conducted on or facilitated by the Internet.

The ICE Cyber Crimes Center (C3) is responsible for delivering computer-based technical services to ICE components in support of domestic and international investigations into cross-border crime.

C3 brings together the Child Exploitation Section, the Computer Forensics Section and the Cyber Crimes Section in a state-of-the-art center that offers cyber crime support and training to federal, state, local and international law enforcement agencies. C3 also includes a fully equipped Computer Forensic Laboratory, providing specialized digital evidence recovery. In addition, C3 offers training in computer investigative and forensic skills.

Child Exploitation

C3 is a powerful tool in the fight against the sexual exploitation of children; the production, advertisement and distribution of child pornography; and child sex tourism.

C3's Child Exploitation Section uses sophisticated investigative techniques to target violators who operate on the Internet, including the use of Web sites, e-mail, chat rooms and file-sharing applications.

Major initiatives include the following:

- **Operation Predator**, ICE's flagship investigative initiative for targeting sexual predators, child pornographers and child sex;
- **The National Child Victim Identification System**, which was developed to assist law enforcement agencies in identifying victims of child sexual exploitation; and
- **The Virtual Global Taskforce**, an international alliance of law enforcement agencies working together to fight online child exploitation and abuse.

In addition, ICE has joined in partnership with other agencies (including the Internet Crimes Against Children Task Forces), foreign law enforcement agencies and non-governmental organizations (such as the National Center for Missing and Exploited Children). These partnerships have enabled C3 to successfully investigate leads and assist in identifying violators and associates all over the world.

Computer Forensics

As the use of computers and digital devices has become widespread, C3's Computer Forensics Section has grown to address the investigative challenges of a digital world. These devices have greatly increased the volume of data that ICE agents must examine during the course of an investigation. In addition, ICE investigators now must contend with forms of digital evidence that are highly volatile, mobile and subject to encryption by any user, making recovery and stewardship of evidence challenging.

Computer forensic agents (CFAs) are ICE special agents trained to perform forensic examinations of seized digital storage devices, such as computer hard drives, flash drives, PDAs, mobile phones, DVDs, CDs and tape media. CFAs use all available digital evidence recovery techniques to preserve the item's authenticity and integrity while maintaining a strict chain of custody.

CFAs are located in ICE field offices throughout the world to provide expertise on investigative strategies and to assist case agents in preparing search warrants targeting digital evidence. CFAs are also called upon to furnish expert computer forensic testimony in criminal trials and to provide support to state and local law enforcement.

Cyber Crimes

C3's Cyber Crimes Section is responsible for managing the cyber component of traditional immigration and customs investigative categories. C3 special agents conduct and coordinate national level investigations where the Internet is used to further criminal activities in the following areas:

- Identity and benefit document fraud;
- Money laundering;
- Financial fraud (including e-payment fraud and Internet gambling);
- Commercial fraud;
- Counter-proliferation investigations;
- Narcotics trafficking;
- Illegal exports;
- Human trafficking and smuggling; and
- General smuggling.