Department of Homeland Security

U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations

Cyber Crimes Investigations Handbook

HSI HB 11-03

August 9, 2011

OFFICIAL USE ONLY

Foreword

The Cyber Crimes Investigations Handbook provides a uniform source of national policies, procedures, responsibilities, guidelines, and controls to be followed by U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agents when investigating crimes facilitated by the use of the Internet. This Handbook contains instructions and guidance to help ensure uniformity and operational consistency among all HSI field offices. Oversight over the national Cyber Crimes Program resides with the HSI Cyber Crimes Center. (Note: On June 9, 2010, the ICE Offices of Investigations (OI), International Affairs (OIA), and Intelligence were realigned under HSI. Throughout this Handbook, documents issued prior to the June 9, 2010, realignment are referred to by their original titles, which reflect the office that issued them, e.g., "OI" instead of "HSI".)

This Handbook is the originating and establishing HSI Handbook for cyber crimes investigations. It supersedes any previous issuances on cyber crimes investigations issued by the former U.S. Customs Service, the former Immigration and Naturalization Service, the former ICE OI, OIA, or Intelligence, or by ICE HSI prior to the date of issuance of this Handbook.

The Cyber Crimes Investigations Handbook is an internal policy of HSI and is not intended to confer any right or benefit on any private person or party. If disclosure of this Handbook or any portion of it is demanded in any judicial or administrative proceeding, the HSI Records and Disclosure Unit, as well as the Office of the Principal Legal Advisor at Headquarters and/or U.S. Attorney are to be consulted so that appropriate measures can be taken to invoke privileges against disclosure. This Handbook contains information which may be exempt from disclosure to the public under the Freedom of Information Act, Title 5, United States Code, Section 552(b), and protected from disclosure in civil discovery pursuant to the law enforcement privilege. Any further request for disclosure of this Handbook or information contained herein should be referred to the HSI Records and Disclosure Unit.

The HSI Policy Unit is responsible for coordinating the development and issuance of HSI policy. All suggested changes or updates to this Handbook should be submitted to the HSI Policy Unit, which will coordinate all revisions with the Cyber Crimes Center.

James A. Dinkins
Executive Associate Director
Homeland Security Investigations

8/9/2011
Date

CYBER CRIMES INVESTIGATIONS HANDBOOK

Table of Contents

Appendices

CYBER CRIMES INVESTIGATIONS HANDBOOK

Chapter 1. PURPOSE AND SCOPE

The Cyber Crimes Investigations Handbook establishes policies and procedures for U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agents (SAs) investigating crimes covered by HSI's investigative priorities and that are wholly or substantially facilitated by the use of the Internet.

Chapter 2. INTRODUCTION

HSI's jurisdictional responsibilities include Internet or high-technology facilitated crimes involving fraud, theft of intellectual property rights (IPR), money laundering, identity and benefit fraud, the sale and distribution of narcotics and other controlled substances, illegal arms trafficking and the illegal export of strategic/controlled commodities, the smuggling and sale of other prohibited items such as art, antiquities, and cultural property, the smuggling and trafficking of undocumented aliens, etc.

The Internet is an ever-expanding worldwide network of computers. These computers and servers are owned by universities, nonprofit organizations, governments, corporations, and individuals. The types of computers (ranging from personal computers to large mainframes) and communication links (from standard telephone lines to satellite connections) vary widely, as do the types of software used. These computers share only one common characteristic: they communicate with each other utilizing a single standard protocol. With the increasing number of individuals worldwide using the Internet and online services and with the advances in computer technology available to the public, many individuals are becoming quite accomplished in using computers for illegal purposes. Persons participating in criminal activities view this as a quick and secure method for facilitating their criminal activity while maintaining relative anonymity and avoiding detection by the authorities.

(b) (7)(E) [redacted]

(b) (7)(E)

[redacted]

Chapter 3. DEFINITIONS

The following definitions are provided for the purposes of this Handbook:

3.1 Bulletin Board System

A Bulletin Board System (BBS) is an electronic message center. Most bulletin boards serve specific interest groups. BBSs allow individuals to review messages left by others or leave their own message, if desired. BBSs are a particularly good place to find free or inexpensive software products. BBSs were very popular prior to the advent of the Internet; however, their function has been largely replaced by various online chat applications.

3.2 Chat

Online chat evolved out of the chat rooms offered on the early BBSs. Online chat includes direct one-on-one chat, text-based group chat using chat rooms provided by Internet providers or other sources, various topic specific forums, and instant messaging (IM). One of the first real online chat services on the Internet was Internet Relay Chat (IRC). IRC is free, but requires IRC client software to connect to an IRC server in order to participate in the chat rooms.

3.3 Computer

A computer is a device that accepts data, processes it in accordance with a stored program, generates results, and usually consists of input, output, storage, arithmetic, logic, and control units. A computer is a functional unit that can perform substantial computation, including numerous arithmetic or logic operations, without human intervention during the execution of one or more computer jobs or programs.

3.4 Computer Forensics Agents and Computer Forensics Analysts

Computer Forensics Agents (CFAs) are General Schedule (GS) 1811 Criminal Investigators; Computer Forensics Analysts (also known as CFAs) are GS-0132 Intelligence Research Specialists. Intelligence Research Specialists have the requisite training and experience in the collection and analysis of computer-based evidence. These individuals are designated by the Cyber Crimes Center's (C3) Computer Forensics Section (CFS). (Note: For the purposes of this

Handbook, the acronym “CFA” will refer to both Computer Forensics Agents and Computer Forensics Analysts.)

3.5 Computer Hardware

Computer hardware is a computer and/or connected or associated physical apparatus directly involved in the performance of communications or data processing functions.

3.6 Computer Software

Computer software consists of programs that can be installed on a computer to provide various types of functionalities for the computer.

3.7 Digital Currency

Digital currency (also referred to as electronic currency or e-currency) is a system of currency facilitated by the Internet that is linked to the value of some other item that can represent cash, gold or precious metals, merchandise, or other commodities of value. Traits common to most digital currencies include the use of third party companies called Exchange Makers to fund the e-currency account, the ability to transfer value between account holders or purchase one e-currency using other e-currencies, and, most importantly, the close relationship between e-currencies and various stored value systems.

3.8 Domain Name

A domain name identifies one or more IP addresses that are used in Uniform Resource Locators (URLs) to identify particular Web pages. An example of a domain name is <mit.edu>. The name consists of two parts: the secondary domain (mit) and the top level domain (TLD) (edu). Each domain name can also have an associated IP address by which it can be identified and/or addressed. For example, a user can enter either www.ice.gov or its associated IP address, 149.101.23.4, to access the ICE Web site.

3.9 Electronic Commerce

Electronic commerce or “e-commerce” is business that is conducted over the Internet using any of the applications that rely on the Internet, such as e-mail, IM, shopping carts, Web services, Universal Description Discover and Integration, File Transfer Protocol (FTP), and Electronic Data Interchange, among others. E-commerce consists of buying and selling products and services over the Internet, including transmitting funds, goods, services, and/or data. E-commerce can be between two businesses (business-to-business) or between a business and a customer/consumer (business-to-consumer).

3.10 Electronic Mail

Electronic mail or “e-mail” is a widely utilized Internet application. It allows a user to send information to any other person or business with an e-mail address. Addresses are conventionally written in the form <username@domain>, where the domain is the name of the recipient's host computer (e.g., xyz.com).

3.11 (b) (7)(E) [redacted]

(b) (7)(E) [redacted]

3.12 Encryption

Encryption is the translation of data into a secret code for the purpose of achieving data security. Scrambled data can be decrypted only with a password, electronic key, or biometric device.

3.13 File Extension

The file extension indicates the type of file and generally controls which program is used to access that file. In a Windows environment, files have a name followed by a "." and a three or more character extension. For example, ".pdf" is a portable document file, ".tiff" is a targeted image format, ".htm" is a hyper text markup, ".jpg" is a compression scheme that supports most graphics, etc.

3.14 File Server

A file server is a computer that controls a central repository of data that can be downloaded or manipulated in some manner by a client. File servers are configured to permit users to log in and send and/or receive files.

3.15 File Transfer Protocol

FTP is the protocol for exchanging files over the Internet. FTP works in the same way as Hyper-Text Transfer Protocol (HTTP) for transferring Web pages from a server to a user's browser and Simple Mail Transfer Protocol (SMTP) for transferring e-mail across the Internet, all of which may use the Internet's Transmission Control Protocol (TCP)/IP protocols to enable data transfer. In addition to utilizing TCP/IP protocols, FTP requires special client software applications that are widely available on the Internet. FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server (e.g., uploading a Web page file to a server). (b) (7)(E) [redacted]

(b) (7)(E) [redacted]

3.16 Graphic Files

Graphic files are files that contain an image that can be displayed on a computer. There are many different types of graphic files; the most popular file extensions are jpg or jpeg, bmp, and gif. Because of their small size, jpg and gif files are the most common on the Internet and are used for Web page graphics. Bmp files are much larger and are typically associated with Windows wallpaper. The majority of pornographic and child pornographic images are in a jpg format, which offers good compression and quality.

3.17 Header

A header is information typically found at the beginning of an e-mail or newsgroup message that contains "envelope information," including a date and time stamp, the name of the originator, and the name of the recipient, as well as the origination path of message distribution.

3.18 Host Server

The host server is part of a URL and is represented either as an IP address or a Domain Name System translation to text that provides access to the server.

3.19 Hyper Text Markup Language

Hyper Text Markup Language (HTML) is used extensively on the World Wide Web and is a markup language used to structure text and multimedia documents and to set up hypertext links between documents.

3.20 Internet

The Internet is a decentralized global network of computers, data transmission cables, and related network hardware that creates an infrastructure able to transmit data available on the physical network (graphics, audio, video files, and application programs) and the means of locating and retrieving that data.

3.21 Internet Forum

An Internet forum is an online discussion site where users can hold conversations in the form of posted messages. (b) (7)(E) [redacted]

3.22 Internet Protocol Address

An IP address is an identifier for a computer or device on a TCP network. All devices must have an IP address to communicate within a TCP/IP network. The IP address can be either IP version 4 (IPv4) or IP version 6 (IPv6). IPv4 is a 32-bits IP address that is commonly used; it can be 192.168.8.1, 10.3.4.5, or other 32 bits IP addresses. IPv4 can support up to 2^{32} (a little over 4 billion) addresses; however, due to an increasing number of devices requiring Internet access, the number of publically available IPv4 addresses is insufficient and near exhaustion. Therefore, IPv6 was developed as a replacement. IPv6 is 128 bits and can support up to 2^{128} (a little over 340 undecillion) addresses to meet future needs with better security and network related features.

3.23 (b) (7)(E)

(b) (7)(E)

3.24 Internet Relay Chat

IRC is a popular chat system that was developed in the late 1980s. Unlike previous chat systems, IRC is not limited to just two participants. Joining an IRC discussion requires an IRC client and Internet access. The IRC client is a program that runs on a computer and sends and receives messages to and from an IRC server. The IRC server, in turn, is responsible for making sure that all messages are broadcast to everyone participating in a discussion. There can be many discussions going on at once with each discussion being assigned a unique channel.

3.25 Internet Service Provider

An ISP is a company that commercially operates host computers, allowing subscribers to connect to the Internet through its network access. These service providers act as a gateway for their subscribers to the Internet and the World Wide Web.

3.26 (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

3.28 Modem (Modulate or Demodulate)

A modem is a device for transmitting digital data over telephone wires by modulating the data into an audio signal to send it and demodulating an audio signal into data to receive it.

3.29 Newsgroup

A newsgroup is an online discussion group conceptually similar to a virtual bulletin board. Unlike IRCs, newsgroups are not live and consist of postings under a particular group name. Viewing and posting messages to a newsgroup require a news reader, which is a program that runs on a computer and connects to a news server on the Internet, and, in many cases, a news server subscription. Most ISPs provide their customers with access to a news server as part of the customers' subscription. Third-party providers on the Internet also provide newsgroup access for a monthly subscription fee.

3.30 Network

A network is a system of interconnected computer systems and terminals. There are several types of networks; two of the most commonly known networks are local area networks (LANs) and wide area networks (WANs).

3.31 Online Payment Service

An online payment service is a type of financial service that enables global e-commerce by providing an easy payment process on the Internet. Online payment technology platforms allow buyers to complete purchases from e-commerce Web sites or just transfer funds without any business transactions.

3.32 Operating System

The operating system (OS) is the most important program that runs on a computer. Every general-purpose computer must have an OS to run other programs. OSs perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers. The most common OSs used (as of the date of issuance of this Handbook) for personal computing are Windows, OS X (Apple), Linux, and FreeBSD. FreeBSD is very popular for Internet Web Servers.

3.33 Peer to Peer

P2P is a term used to describe one computer directly linking to another computer to transfer files, including videos, images, music, software, and documents. There are many P2P file sharing applications for use on the Internet.

3.34 Ports

In TCP/IP and User Datagram Protocol networks, ports provide an endpoint to a logical connection. The port number identifies the type of port. For example, port 80 is used for HTTP traffic (Internet browser). (b) (7)(E) [redacted]

3.35 Prepaid Cards

Prepaid cards (also known as stored value cards) provide access to prepaid funds which can be accessed electronically at point-of-sale terminals, automated teller machines (ATM), via the Internet, or wirelessly through contactless technology. The funds are usually held not on the card but within a central depository of the financial institution providing the service. There are two primary categories of prepaid cards: closed loop cards and open loop cards. Closed loop cards are single purpose cards such as one issued by a particular retailer or prepaid telephone cards. Open loop cards are multipurpose cards that can be used virtually anywhere or for any purpose. Some open loop cards can also be used at ATMs and can be reloaded with additional funds. User verification for these products is generally lower than for traditional credit or debit cards. (Note: Stored value is migrating toward wireless technology such as mobile-to-mobile transfers and other contactless mediums of financial exchange.)

3.36 Protocol

The protocol is part of a URL and is an agreed-upon format for transmitting data between two devices. The protocol determines the type of error checking and data compression method to be used, how the transmitting device will indicate that it has finished sending a message, and how the receiving device will indicate that it has received a message. Protocols are typically seen and recognized as <http://>. Other forms are <telnet://> and <https://>. The protocol gives clues as to what type of information may be transmitted over the Web interface.

3.37 Remailer (Anonymous)

A remailer is an Internet-based service that accepts e-mail messages and newsgroup messages, strips off the header (origination information), and then forwards the message to the intended recipient or newsgroup. Remailers prevent the recipient from determining the originator of the message.

3.38 Robots/Bots

Robots, commonly referred to as “Bots,” are computer programs that run automatically without human intervention. Typically, a robot is endowed with some artificial intelligence so that it can react to different situations it may encounter and perform human-like communication functions, such as replying to e-mails or responding to messages in a newsgroup. Bots are commonly used in chat rooms to authenticate users and perform other administrative functions connected to the chat room.

3.39 Server

A server is a computer or other device that resides on a network and manages the network resources. There are various types of servers that can be configured and used for specific dedicated purposes. Typically, each application (e.g., e-mail, Web, and FTP) operates using a different port. Servers can be set up to listen and respond to requests that are designated for a specific port. For example, a file server is a computer and storage device dedicated to storing files. Any user on the network can store files on the server. A print server is a computer that manages one or more printers, and a network server is a computer that manages network traffic. A database server is a computer system that processes database queries. A Web server is a computer that hosts Web pages that can be accessed with an Internet browser. A mail server handles the delivery, transmission, and storage of e-mail messages.

3.40 Spoofing

Spoofing is a generic term describing the falsification of information for the purpose of hiding the origin of an e-mail message, newsgroup message, or an IP address.

3.41 System Administrator

A system administrator is the individual responsible for the operation and maintenance of a computer system or network. This individual may also be responsible for computer security if there is no dedicated security administrator.

3.42 Uniform Resource Locator

A URL is the global address of files, documents, and other sources residing on the World Wide Web. The first part of the address is referred to as a protocol identifier, which indicates what protocol to use. The second part of the address is referred to as a resource name, which specifies the numeric IP address or the domain name.

3.43 Usenet

The term “Usenet” refers to Internet discussion groups, similar to Internet Forums that allow users to post public messages and replies. Interaction is not in real time and uses a news reader, similar to newsgroups, to post messages and replies. The Usenet could be considered to be a transition between newsgroups and Internet Forums.

3.44 Web Site

A Web site is a collection of files accessible via the Internet whereby a person or an entity can document or distribute information. Web sites can be created by individuals or businesses seeking to provide information that can be accessed through the World Wide Web. (See Appendix A for a comprehensive explanation of the differences between Web sites and affiliate Web sites.)

3.45 (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

3.46 World Wide Web

The World Wide Web is the collection of electronic files residing on computers throughout the Internet. A Web page may contain text, graphics, video, or audio in any combination. It may also include hypertext links (also termed "hot links" or "clickable links") to other Web pages anywhere on the Internet. Users visit Web pages by means of a browser program (e.g., Netscape Navigator or Microsoft Internet Explorer) that allows free movement among Web pages by selecting available links. The World Wide Web has no central index; however, extensive commercial indexes (search engines) enable users to perform keyword searches to locate sites on a given subject.

Chapter 4. AUTHORITIES/REFERENCES

The following statutes are specific to crimes facilitated by the Internet or via other wired or wireless communications technologies:

4.1 Authorities

A. Title 8, United States Code (U.S.C.), Section 1225, Inspection by immigration officers; expedited removal of inadmissible arriving aliens; referral for hearing.

B. 18 U.S.C. § 545, Smuggling goods into the United States.

C. 18 U.S.C. § 554, Smuggling goods from the United States.

D. 18 U.S.C. § 1028, Fraud and related activity in connection with identification documents, authentication features, and information.

E. 18 U.S.C. § 1029, Fraud and related activity in connection with access devices.

F. 18 U.S.C. § 1030, Fraud and related activity in connection with computers.

G. 18 U.S.C. § 1343, Fraud by wire, radio, or television.

H. 18 U.S.C. § 1362, Communication lines, stations or systems.

I. 18 U.S.C. §§ 2510 - 2522, Wire and electronic communications interception and interception of oral communications.

J. 18 U.S.C. §§ 2701-2712, Stored wire and electronic communications and transactional records access.

K. 18 U.S.C. §§ 3121-3127, Pen registers and trap and trace devices.

L. 19 U.S.C. § 1509, Examination of books and witnesses.

M. 21 U.S.C. § 967, Smuggling of controlled substances; investigations; oaths; subpoenas; witnesses; evidence; production of records; territorial limits; fees and mileage of witnesses.

N. 22 U.S.C. § 2778, Control of arms exports and imports.

O. 50 U.S.C. App. § 2411, Enforcement.

4.2 References

A. Computer Forensics Handbook (HSI Handbook (HB) 11-01), dated April 27, 2011, or as updated.

B. Undercover Operations Handbook (Office of Investigations (OI) HB 08-04), dated April 14, 2008, or as updated.

C. OI Memorandum, “Issuance of Rebranded/Updated Subpoenas Forms,” dated December 3, 2009, or as updated or superseded.

D. Seized Asset Management and Enforcement Procedures Handbook (SAMEPH) (U.S. Customs Service HB 4400-01A, dated January 2002, or as updated).

E. Online Investigative Principles for Federal Law Enforcement Agents, Department of Justice (DOJ) Computer Crimes & Intellectual Property Section, dated November 1999. (Note: This document is listed for informational purposes only.

HSI SAs will comply with undercover operation policies contained in the Undercover Operations HB (OI HB 08-04, dated April 14, 2008, or as updated) and cyber crimes investigative policies provided in this HB. A copy of the Online Investigative Principles for Federal Law Enforcement Agents can be obtained from the Computer Crimes & Intellectual Property Section, DOJ.)

Chapter 5. RESPONSIBILITIES

5.1 Executive Associate Director, Homeland Security Investigations

The Executive Associate Director of HSI has the overall responsibility for the oversight and implementation of the policies and procedures set forth in this Handbook.

5.2 Section Chief, Cyber Crimes Section

The Section Chief of the Cyber Crimes Section (CCS) is responsible for developing and coordinating certain cyber-based criminal cases (where criminal activities are wholly or substantially facilitated by the use of the Internet) that have national and international impact; developing and forwarding certain cyber-based investigative leads to HSI field offices; and providing coordination between field offices in regards to CCS-authorized HSI-initiated cyber-related cases that impact more than one field office. (b) (7)(E) [redacted]

5.3 Special Agents in Charge

Special Agents in Charge (SACs) are responsible for implementing the provisions of this Handbook in their respective area of responsibility (AOR).

5.4 Attachés

Attachés are responsible for implementing the provisions of this Handbook in their respective AOR.

5.5 Computer Forensics Agents and Computer Forensics Analysts

CFAs are responsible for the identification, preservation, acquisition, analysis, and presentation of electronic evidence and media, and for complying with the provisions of this Handbook.

5.6 Special Agents

SAs are responsible for complying with the provisions of this Handbook.

Chapter 6. CYBER INVESTIGATIVE STRATEGIES

6.1 Obtaining Information from Web Sites

(b) (7)(E)

[redacted]

6.2 Identifying Networks and User Information

(b) (7)(E) [redacted]

[redacted]

6.3 Preservation of Online Communications

(b) (7)(E) [redacted]

(b) (7)(E) [redacted]

(b) (7)(E) [redacted]

6.4 Investigative Protocols and Precautions Regarding Wireless Networks

(b) (7)(E)

6.5 Recording Online Communications and Handling Recorded Evidence

(b) (7)(E)

[redacted]

6.6 (b) (7)(E)

(b) (7)(E)

(b) (7)(E) [redacted]
(b) (7)(E)

6.7 (b) (7)(E) [redacted]

(b) (7)(E) [redacted]

[redacted]

6.8 International Issues

SAs conducting online investigations should use reasonable efforts to ascertain whether any pertinent computer related data, witness, subject, or informant is located in a foreign jurisdiction. If this computer data or people are from a foreign country, the appropriate HSI Attaché should be contacted. It is not necessary to contact the HSI Attaché if SAs are gathering open-source information from foreign Web sites configured for public access.

Chapter 7. PROACTIVE ONLINE CYBER INVESTIGATIONS

7.1 (b) (7)(E)

(b) (7)(E)

7.2 (b) (7)(E)

(b) (7)(E)

7.3 (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

A. (b) (7)(E)

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

E. (b) (7)(E)

[redacted] [redacted]

[redacted] [redacted]

(b) (7)(E)

A. (b) (7)(E)

(b) (7)(E) [redacted]

B. (b) (7)(E) [redacted]

C. (b) (7)(E) [redacted]

(b) (7)(E) [redacted]

(b) (7)(E) [redacted]

(b) (7)(E) [redacted]

7.6 (b) (7)(E) [redacted]

(b) (7)(E) [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

7.7 Internet Communications

(b) (7)(E) [redacted]

[redacted] [redacted]

(b) (7)(E)

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

(b) (7)(E) [redacted]

7.8 (b) (7)(E) [redacted]

(b) (7)(E) [redacted]

[redacted]

(b) (7)(E) [redacted].

7.9 Liability to Innocent Third Parties

(b) (7)(E) [redacted]

(b) (7)(E) [redacted]

7.10 Prohibited Use of ICE Network Computers for Investigations

All personnel should be advised that ICE network computers are provided as administrative tools, not investigative ones. (b) (7)(E) [redacted]

(b) (7)(E) [redacted]

(b) (7)(E) [redacted]

(b) (7)(E) [redacted]

7.11 (b) (7)(E) [redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

(b) (7)(E) [redacted]

7.12 (b) (7)(E)

(b) (7)(E)

Chapter 8. OBTAINING ELECTRONIC EVIDENCE

8.1 Preservation Letter

A Preservation Letter (see Appendix B), issued by a government entity under the authority of 18 U.S.C. § 2703(f), orders the system administrator to "take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process." The period of retention is 90 days, which may be extended for an additional 90-day period upon a renewed request by the government entity. This is only for information that is already available and is not intended to retain future information. For the purposes of this Handbook, the "government entity" is the C3 Unit Chief at HQ, the Assistant Director of the IPR Center, or a SAC, or their designees.

8.2 Administrative Summons and Subpoenas

HSI's authority to use administrative summonses and subpoenas is restricted within certain statutory limits. SAs should contact the Office of the Principal Legal Advisor (OPLA) at HQ or their local OCC for legal questions regarding the proper usage of these administrative procedures. C3 should be contacted when issuing an administrative summons or subpoena to an unfamiliar ISP. C3 will advise whether or not the ISP is deemed compliant, reliable, and trustworthy. C3 should also be contacted if SAs need guidance or templates ("go-bys") on summons/subpoena language. (See OI memorandum entitled, "Issuance of Rebranded/Updated Subpoenas and Summons Forms," dated December 3, 2009, or as updated or superseded.)

8.2.1 Obtaining Subscriber Information

Pursuant to 18 U.S.C. § 2703(c), SAs can use an administrative summons or subpoena to obtain basic subscriber information from an electronic communications service, including name, address, local and long distance telephone numbers, connection records or records of session times and duration, length of service, types of service utilized, and telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and the means and source of payment for such service, including any credit card and/or bank account number, rendered.

8.2.2 Obtaining Electronic Communications in Storage for More than 180 Days

Pursuant to 18 U.S.C. § 2703(b), there are several ways to obtain e-mail content. Due to some court decisions, certain jurisdictions are limited in the processes that can be used. Due to these limitations, SAs should coordinate with their local USAO and contact their local OCC.

8.2.3 Controlled Substances Enforcement Subpoena

A Controlled Substances Enforcement Subpoena (ICE Form 73-021) may be issued pursuant to 21 U.S.C. § 967. Under this authority, the Secretary of Homeland Security is authorized to issue subpoenas for testimony and documents or other tangible evidence in investigations relating to violations of 18 U.S.C. § 545 (Smuggling goods into the United States) with respect to controlled substances.

8.2.4 Export Enforcement Subpoena

An Export Enforcement Subpoena (ICE Form 73-022) is issued pursuant to 50 U.S.C. App. § 2411(a)(1) and implementing regulations, and 22 U.S.C. § 2778(e) and implementing regulations. It is used in investigations relating to the Export Administration Act, the Arms Export Control Act, the International Emergency Economic Powers Act, and 18 U.S.C. § 554 (Smuggling goods from the United States).

8.2.5 Immigration Enforcement Subpoena

An Immigration Enforcement Subpoena (DHS Form I-138) may be issued in furtherance of the enforcement of immigration laws pursuant to section 235(d) of the Immigration and Nationality Act, 8 U.S.C. § 1225(d), and may require the attendance and testimony of witnesses and the production of books, papers, and documents relating to immigration matters.

8.2.6 Summons

The 19 U.S.C. § 1509 Summons (DHS Form 3115) is a broad summons used in the enforcement of customs laws.

8.3 Grand Jury Subpoenas

Grand jury subpoenas may be obtained through the USAO. For electronic communication in storage for more than 180 days or opened e-mail, a grand jury subpoena or administrative subpoena with notice to the subscriber is legally sufficient in some jurisdictions. Due to these limitations, SAs should coordinate with their local USAO and contact their local OCC.

8.4 Search Warrants

For electronic communications in storage for 180 days or less, SAs must obtain a search warrant.

8.5 (b) (7)(E)

(b) (7)(E)

8.6 Open Source

In addition to information obtained through legal or administrative processes, SAs can also obtain electronic evidence through open sources via the Internet. (b) (7)(E)

(b) (7)(E)

8.7 Guidelines for Searching and Seizing Computers

If SAs believe that items sought are stored within a computer or on magnetic or digital storage devices associated with a computer, (b) (7)(E) (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Appendix A

DIFFERENCES BETWEEN WEB SITES AND AFFILIATE WEB SITES

Web Site:

A Web site is a collection of files accessible via the Internet whereby a person or an entity can document or distribute information. Web sites can be created by individuals seeking to provide information about themselves or their personal opinions or interests, or by private groups who are seeking to connect with others who have like interests. Web sites can also be created by businesses in order to market their company or products and may also be used to sell their products online. Depending on their purpose, Web sites can contain multiple screens called Web pages. If a Web site has multiple Web pages, they are linked together through a home page, which is the base page of a Web site that connects all the Web pages together via a system of hyperlinks. Each Web site and Web page can be accessed through a unique Internet address. This address is entered into a Web browser that requests the data making up the Web site or Web page from the servers upon which the information resides, and then receives, compiles, and displays the information in the Web site or Web page format on the requesting computer. These Internet addresses are called Uniform Resource Locators (URLs) and are comprised of pieces of data, which, when put together in a string, identify the location of the files on the Internet.

The pieces of data that make up a URL are the protocol and the domain name, but a URL may also contain a path or file name. The protocol establishes the way in which the information will be transferred over the Internet. Some common protocols used in URLs are <http://>, <https://>, <ftp://>, and <smtp://>. The domain name is the core of the URL, and usually most, if not all, Web pages affiliated with a Web site will have this as the common base. The domain name has a "name" chosen by the entity developing the Web site, usually to make the Web site readily identifiable with the content that will be displayed. For example, most businesses will choose a domain name containing the name or a version of the name of the company, such as <www.barclays.co.uk>. The domain name is comprised of labels separated by a period and is read from right to left. The top level domain (TLD) is the right-most part of the domain name and signifies the starting point through which the computer will attempt to find the data. The TLD can be generic such as .com, .org, or .net, but may also be a specified country code such as "uk" or "ca". The TLD is followed by a second-level domain, and so on, including the chosen "name" of the Web site. For example, in "barclays.co.uk," "uk" is the TLD, "co" is the second level domain, and "barclays" is the third level domain. The computer will navigate through each level domain in turn to locate all the information that comprises the Web site or Web page. The leftmost part of the domain name designates the kind of server that the information resides on. For example, "www" indicates that the information is on a World Wide Web server. As noted, some URLs contain a path or file name that is an extension of the domain name that further defines the location of the information. Path names may be used to access a certain Web page of a Web site, or identify documents linked to the Web site, but some Web sites use file names as a part of their home page. As a final example to summarize the configuration of a URL, in the URL <https://www.xyz.org/index.html>, the protocol is https://, the domain name is www.xyz.org, and the path name is /index.html.

Domain names are "user friendly" versions of an Internet Protocol (IP) address. An IP address is in numeric characters in four segments separated by periods. For example, the domain name of the General Motors Web site is <www.gm.com>; however, the IP address is <170.224.60.167>. Domain names simply are an easier way for people to remember Web sites, while the IP address is a computer's way of accessing Web sites. It is important to note that a single domain name can be located at multiple IP addresses, and that multiple domain names can be located at the same IP address. Domain names are converted into IP addresses through the Domain Name System (DNS). All domain names have associated name servers that contain a DNS database to store hostnames and associated IP addresses and that process requests for this information. Since the name server acts as the primary means of converting domain names into IP addresses, most domains will also have a secondary name server to act as a back-up to the primary name server to ensure that there is always a functional name server at all times. A name server may be maintained by the operator of the Web site, but most Web sites pay an Internet Service Provider (ISP) to maintain the name server. Once the name server converts the domain name into an IP address, the IP address is used to locate the files that comprise a Web site or Web page from the Web server on which the information is stored. This information can be stored on a single Web server or on multiple servers, depending on the size and the amount of content on a Web site or Web page. As with name servers, some Web site operators may maintain their own Web servers or may use the services of an ISP. A single Web server can host information from numerous Web sites.

In order for a Web site to become accessible on the Internet, the domain name of the Web site must be registered and the Web site data must be hosted on a Web server. The operator of the Web site must arrange for both. First, the chosen domain name must be registered through a domain name registration service, or registrar, each of which charges varying fees for its services. Registration of a Web site is a contract, usually in yearly increments, and must be renewed within a set time or the domain name will be released upon expiration for others to register. The registrar registers the domain name with the Internet Corporation for Assigned Names and Numbers, which is responsible for ensuring the uniqueness and correct mapping of each domain name. Registration of a domain name adds the name to a domain name register and the information is then stored on the DNS server. In registering a domain name, the individual registering the site is required to provide registration and contact information, which is publicly available through the Whois databases that are maintained by the registrars. (b) (7)(E) [redacted]

(b) (7)(E)

Affiliate Web Sites

As the Internet is increasingly being used to market and sell goods, new ways to increase Web site traffic and generate online orders have come to prominence. One of these methods is affiliate marketing. Affiliate marketing is a means by which a business or Web site operator can recruit people to establish Web sites that redirect Web sales to the operator's business for a commission or percentage of the sales that their site generates. These affiliate Web sites can cause confusion because they appear, for all intents and purposes, to be independent Web sites selling their own products and not overtly linked to the business that recruited them. (b) (7)(E) (b) (7)(E)

A common misconception that some Internet users have is that ordering products from a Web site via the Internet is always an A to Z operation, where the people who own the site where the order is placed also process the order, collect the payment, and ship the product purchased. (b) (7)(E)

(b) (7)(E)

(b) (7)(E) [redacted]

(b) (7)(E) [redacted]

(b) (7)(E) [redacted]

(b) (7)(E) [redacted]

(b) (7)(E)

[redacted]

Appendix B

Preservation Letter Template

(b) (7)(E)

[redacted]

Appendix C

ACRONYMS

A

AOR	Area of Responsibility
ATM	Automated Teller Machine

B

BBS	Bulletin Board System

C

C3	Cyber Crimes Center
CCS	Cyber Crimes Section
CFA	Computer Forensics Agent or Computer Forensics Analyst
CFS	Computer Forensics Section

D

DHS	Department of Homeland Security
DNS	Domain Name System
DOJ	Department of Justice

E

ECPA	Electronic Communications Privacy Act
ELSUR	Electronic Surveillance

F

FTP	File Transfer Protocol

G

GS	General Schedule

H

HB	Handbook
HQ	Headquarters
HSI	Homeland Security Investigations

HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol

I

ICE	U.S. Immigration and Customs Enforcement
IM	Instant Messaging
IMT	International Mobile Telecommunications
IP	Internet Protocol
IPAV	Internet Protocol Address Verifier
IPR	Intellectual Property Rights
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
IRC	Internet Relay Chat
ISP	Internet Service Provider

J–K

L

LAN	Local Area Network

M

MAC	Media Access Control

N

O

OCC	Office of the Chief Counsel
OI	Office of Investigations
OPLA	Office of the Principal Legal Advisor
OS	Operating System

P

P2P	Peer to Peer

Q

R

REP	Reasonable Expectation of Privacy

S

SA	Special Agent
SAC	Special Agents in Charge
SAMEPH	Seized Asset Management and Enforcement Procedures Handbook
SEACATS	Seized Asset Case Tracking System
SMTP	Simple Mail Transfer Protocol

T

TCP	Transmission Control Protocol
TLD	Top Level Domain

U

UPM	Undercover Program Manager
URL	Uniform Resource Locator
USAO	U.S. Attorney’s Office
USC	U.S. Code

V

VOIP	Voice over Internet Protocol

W

WAN	Wide Area Network
WIMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WWAN	Wireless Wide Area Network

X-Z