



Homeland Security Investigations

Intellectual Property Investigations Handbook

HSI HB 17-02 / March 2, 2017



U.S. Immigration
and Customs
Enforcement

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

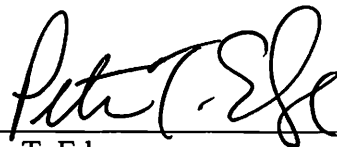
Foreword

The Intellectual Property Investigations Handbook provides a single 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 conducting investigations on intellectual property theft. This Handbook contains instructions and guidance to help ensure uniformity and operational consistency among all HSI field offices. Oversight over the Intellectual Property Investigations Program resides with the Assistant Director, National Intellectual Property Rights Coordination Center (IPR Center).

This Handbook is the originating and establishing Handbook on intellectual property investigations. It supersedes all policies or other documents on intellectual property investigations issued before the date of this Handbook.

The Intellectual Property Investigations Handbook is an internal policy of HSI. It is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter, nor are any limitations hereby placed on otherwise lawful enforcement prerogatives of ICE. This Handbook is For Official Use Only (FOUO) – Law Enforcement Sensitive. It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with the Department of Homeland Security policy relating to FOUO information and the ICE Directive on Safeguarding Law Enforcement Sensitive Information. This information shall not be distributed beyond the original addressees without prior authorization of the originator. 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’s Office, 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 pursuant to the law enforcement privilege. Any other requests 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 IPR Center.



Peter T. Edge
Executive Associate Director
Homeland Security Investigations

MAR - 2 2017

Date

INTELLECTUAL PROPERTY INVESTIGATIONS HANDBOOK

Table of Contents

Chapter 1. PURPOSE AND SCOPE.....	1
Chapter 2. INTRODUCTION.....	1
Chapter 3. DEFINITIONS	1
• 3.1 Adulterated.....	1
• 3.2 Certification Mark.....	2
• 3.3 Collective Mark	2
• 3.4 Copyright	2
• 3.5 Counterfeit Mark.....	2
• 3.6 Counterfeit Military Good or Service	2
• 3.7 Domain Name System	2
• 3.8 Entry.....	2
• 3.9 Entry Documents	3
• 3.10 Entry Summary	3
• 3.11 Gray Market.....	3
• 3.12 Harmonized Tariff Schedule.....	3
• 3.13 Letter of Credit.....	3
• 3.14 Patent Right.....	3
• 3.15 Piracy	4
• 3.16 Recordation	4
• 3.17 Service Mark	4
• 3.18 Trade Secret	4
• 3.19 Trademark	4
Chapter 4. AUTHORITIES/REFERENCES	4
• 4.1 Authorities.....	4
• 4.2 References.....	11
Chapter 5. RESPONSIBILITIES	11
• 5.1 Executive Associate Director, Homeland Security Investigations	11
• 5.2 Assistant Director, National Intellectual Property Rights Coordination Center.....	11
• 5.3 Special Agents in Charge and Attachés	11
• 5.4 Special Agents and Intelligence Research Specialists	12

Chapter 6. OVERVIEW OF THE IMPORTATION PROCESS AND INTERNATIONAL TRADE FINANCE	12
• 6.1 Importation Process	12
• 6.2 International Trade Finance	12
Chapter 7. OVERVIEW OF INTELLECTUAL PROPERTY THEFT INVESTIGATIONS.....	13
• 7.1 Intellectual Property Theft Background.....	13
• 7.2 Intellectual Property Legislation.....	14
• 7.3 The Threat of Intellectual Property Crime.....	15
• 7.4 Intellectual Property Investigative Initiatives	16
Chapter 8. APPLICABLE MONEY LAUNDERING LAWS IN SUPPORT OF INTELLECTUAL PROPERTY THEFT INVESTIGATIONS	17
• 8.1 Money Laundering Laws	17
• 8.2 Specified Unlawful Activities Related to Intellectual Property Theft.....	18
• 8.3 Forfeiture Laws	19
• 8.4 Financial Investigative Methodology	19
Chapter 9. CATEGORIES OF COUNTERFEITING	20
• 9.1 Computer Hardware.....	20
• 9.2 Computer Software	20
• 9.3 Electrical Products	21
• 9.4 Food Products	21
• 9.5 Luxury Items.....	21
• 9.6 Microelectronics	21
• 9.7 Movies, Films, Videos, and Streaming.....	21
• 9.8 Pet Products	22
• 9.9 Pharmaceuticals and Personal Health Care and Beauty Products	22
• 9.10 Toys and Household Goods.....	23
• 9.11 Transportation and Heavy Industry Products	23
• 9.12 Wearing Apparel and Footwear	23
Chapter 10. VERIFICATION OF INTELLECTUAL PROPERTY.....	23
• 10.1 U.S. Copyright Office.....	23
• 10.2 U.S. Patent and Trademark Office.....	24
• 10.3 U.S. Customs and Border Protection	24
• 10.4 Brand Holders	24

Chapter 11. SOURCE AND TRANSSHIPMENT COUNTRIES.....25

Chapter 12. DISTRIBUTION CHANNELS AND MARKETPLACES OF COUNTERFEIT MERCHANDISE25

- 12.1 Retail Outlets25
- 12.2 Wholesale Outlets26
- 12.3 Business-to-Business (B2B) Online Marketplaces26
- 12.4 Business-to-Consumer (B2C) Online Marketplaces26
- 12.5 Virtual Currency27
- 12.6 The Dark Web27
- 12.7 Express Consignment28
- 12.8 Warez Groups28
- 12.9 File Sharing28
- 12.9.1 Peer-to-Peer (P2P) File Sharing Technology28
- 12.9.2 Cloud Computing Websites29
- 12.9.3 Downloads vs. Streaming Content29

Chapter 13. INTELLECTUAL PROPERTY THEFT INVESTIGATIONS.....29

- 13.1 Investigative Tools29
- 13.1.1 ICE (b) (7)(E)30
- 13.1.2 Open Source Internet Research30
- 13.1.3 Websites31
- 13.1.4 Google Analytics31
- 13.1.5 Preservation Letter32
- 13.1.6 Subpoena, Disclosure by Internet Service Providers, and Notification to Users32
- 13.1.7 Internet Pen Register/Trap and Trace32
- 13.1.8 Internet Search Warrants33
- 13.1.9 Online Marketplaces33
- 13.1.10 Financial Data Exploitation34
- 13.1.11 Money Service Businesses34
- 13.1.12 Financial Wire Transfers35
- 13.2 Coordination with a Prosecutor35
- 13.3 Joint Investigations36
- 13.4 Working with Brand Holders36
- 13.5 HSI Cyber Crimes Center37
- 13.6 ICE Suspension and Debarment37

Chapter 14. COORDINATING INTELLECTUAL PROPERTY CASES.....38

- 14.1 National Intellectual Property Rights Coordination Center38
- 14.1.1 National Cyber-Forensics and Training Alliance38

- 14.2 IPR Center Partner Agencies38
- 14.2.1 U.S. Customs and Border Protection38
- 14.2.2 Department of Commerce.....39
- 14.2.3 Consumer Product and Safety Commission40
- 14.2.4 Federal Bureau of Investigation.....40
- 14.2.5 Food and Drug Administration’s Office of Criminal Investigations...40
- 14.2.6 General Services Administration’s Office of Inspector General40
- 14.2.7 DOS’s Office of International Intellectual Property Enforcement40
- 14.2.8 National Aeronautics and Space Administration’s Office of
Inspector General40
- 14.2.9 Nuclear Regulatory Commission.....41
- 14.2.10 Defense Criminal Investigative Service.....41
- 14.2.11 Defense Logistics Agency’s Office of Inspector General41
- 14.2.12 U.S. Army Criminal Investigative Command’s Major
Procurement Fraud Unit.....41
- 14.2.13 U.S. Air Force’s Office of Special Investigations41
- 14.2.14 U.S. Naval Criminal Investigative Service42
- 14.2.15 U.S. Postal Inspection Service42
- 14.2.16 U.S. Postal Service Office of Inspector General.....42
- 14.2.17 U.S. Patent and Trademark Office42
- 14.2.18 International Criminal Police Organization42
- 14.2.19 Europol.....43
- 14.2.20 Government of Mexico, Tax Administration Service (Servicio de
Administración y Tributario)43
- 14.2.21 Royal Canadian Mounted Police43
- 14.2.22 Federal Maritime Commission43
- 14.3 DOJ Computer Crimes and Intellectual Property Section43
- 14.4 Investigative Support44
- 14.5 Outreach and Training44
- 14.6 International Operation Coordination44
- 14.7 Case Deconfliction.....44
- 14.8 IPR Center Deconfliction and Vetting Process.....44

Chapter 15. DOMAIN NAME SEIZURE PROTOCOLS.....46

- 15.1 Initial Lead Research46
- 15.2 Targeting a Subdomain or Subdirectory46
- 15.3 Targeting Violative Sites for Domain Name Seizure49
- 15.4 Creating (b) (7)(E) for
Domain Name Seizures.....50
- 15.5 Transferring Custody of a Forfeited Domain Name51

APPENDICES

Appendix A	Sample Affidavit.....	A-i
Appendix B	Acronyms.....	B-i

INTELLECTUAL PROPERTY INVESTIGATIONS HANDBOOK

Chapter 1. PURPOSE AND SCOPE

The Intellectual Property Investigations Handbook provides policies and procedures for U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agents and, as applicable, Intelligence Research Specialists and other HSI personnel when conducting or supporting intellectual property (IP) related investigations.

Chapter 2. INTRODUCTION

HSI is a leading agency in the investigation of criminal IP violations involving the illegal importation, exportation, and distribution of counterfeit merchandise and pirated works, as well as its associated financial crimes. HSI's goal is to disrupt the manufacturing, distribution, and financing segments of criminal organizations benefitting from IP infringement.

HSI's IP investigations program has significant national security, public health and safety, and economic implications, especially with respect to trends in IP theft such as the smuggling of counterfeit vehicle airbags, pharmaceutical medicine, and computer hardware intruding into the U.S. civilian government and military supply chain network. Internet technology has made it much easier for the proliferation of these types of crimes and made it easier for anyone in the world to conduct trafficking activities in the global marketplace. As a result, HSI strengthened its strategic position in protecting the United States' IP through enhanced investigative tools and techniques that better target these increasingly complex crimes. The guidance provided in this Handbook will aid SAs in supporting this investigative priority.

Chapter 3. DEFINITIONS

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

3.1 Adulterated

As it pertains to adulterated drugs, section 501(b) of the Food, Drug, and Cosmetic Act (FD&C Act) deems an official drug to be adulterated if it fails to conform to the standards of quality, strength, or purity. Standard tests have been established for drug characteristics, such as potency, sterility, dissolution, weight variation, and content uniformity. Section 601 of the FD&C Act states that a cosmetic is adulterated if it contains a poisonous, filthy, putrid, or decomposed substance, or if it has been prepared, packaged, or stored in unsanitary conditions.

3.2 Certification Mark

Any word, phrase, symbol, or design, or a combination thereof, owned by one party who certifies the goods and services of others when they meet certain standards. The owner of the mark exercises control over the use of the mark; however, the certification mark is used by others to indicate that their products meet certain standards.

3.3 Collective Mark

Any word, phrase, symbol, or design, or a combination thereof owned by a cooperative, an association, or other collective group or organization and used by its members to indicate the source of the goods or services.

3.4 Copyright

A form of protection provided by the laws of the United States for “original works of authorship,” including literary, dramatic, musical, architectural, cartographic, choreographic, pantomimic, pictorial, graphic, sculptural, and audiovisual creations.

3.5 Counterfeit Mark

A spurious mark that is: (1) used in connection with trafficking; (2) identical or substantially indistinguishable from a mark registered with the U.S. Patent and Trademark Office (USPTO) and which is in use; (3) applied to or used in connection with goods or services for which the mark is registered, or applied to or consists of a label, patch, sticker, wrapper, badge, emblem, medallion, charm, box, container, can, case, hand tag, documentation, or packaging of any type or nature that is designed, marketed, or otherwise intended to be used on or in connection with the goods or services for which the mark is registered with the USPTO; and (4) the use of which is likely to cause confusion, mistake, or deception. Title 18, United States Code (U.S.C.), Section 2320(f)(1)(A).

3.6 Counterfeit Military Good or Service

A good or service that uses a counterfeit mark on, or in connection with, such good or service and that is: (1) falsely identified or labeled as meeting military specifications; or (2) intended for use in a military or national security application. 18 U.S.C. § 2320(f)(4).

3.7 Domain Name System

A hierarchical naming system that translates domain names into Internet Protocol addresses.

3.8 Entry

An entry begins when information is submitted to U.S. Customs and Border Protection (CBP) by documentation or pursuant to an electronic data exchange system to secure the release of merchandise. “Entry” is complete when goods are actually released into the commerce of the

United States. An “introduction,” on the other hand, commences when the goods are unloaded at a CBP port whether or not an entry has been made.

3.9 Entry Documents

Documents that show evidence of the admissibility of merchandise. Examples include the Entry Manifest (CBP Form 7533) and the Application and Special Permit for Immediate Delivery (CBP Form 3461). At times, a commercial invoice, a pro forma invoice, and a packing list could potentially be considered.

3.10 Entry Summary

The Entry Summary (CBP Form 7501) is the documentation required to assess the duties, taxes, and fees associated with an importation. This documentation includes the estimated duties, taxes, and fees that are due within 10 working days of the entry of merchandise.

3.11 Gray Market

Merchandise manufactured abroad bearing lawfully-applied trademarks intended for sale in foreign markets only but are imported into the United States without the consent of the trademark owner. Restrictions on the importation of gray market articles are found in Title 19, Code of Federal Regulations (C.F.R.), Section 133.23.

3.12 Harmonized Tariff Schedule

A hierarchical structure that describes the classification of goods in trade for duty, quota, and statistical purposes.

3.13 Letter of Credit

A contractual agreement whereby the issuing bank, acting on behalf of its customer (importer), promises to make payment to the exporter provided that the terms and conditions stated in the letter of credit have been met, as evidenced by the presentation of specified documents. (Note: A letter of credit is a common instrument in international finance that facilitates international trade. Typically, a letter of credit is accompanied by a bill of lading or air waybill, commercial invoice, packing list, etc.)

3.14 Patent Right

An IP right granted by the U.S. Government to an inventor to exclude others from making, using, offering for sale, or selling the invention throughout the United States, or importing the invention into the United States for a limited time in exchange for public disclosure of the invention after the patent is granted. Generally, patent rights are enforceable by HSI only in the context of violations involving merchandise subject to entry exclusion orders issued by the U.S. International Trade Commission pursuant to 19 U.S.C. § 1337.

3.15 Piracy

The unauthorized reproduction or distribution, including by electronic means, of a copyrighted work without the consent of the copyright owner and codified under 17 U.S.C. §§ 501(a) and 506 and 18 U.S.C. § 2319. Piracy may be referred to as “bootlegging” when discussing the unauthorized recordation of, or trafficking in, live musical performances, or “camcording” of unauthorized recording of motion pictures in a motion picture facility under 18 U.S.C. §§ 2319A and 2319B.

3.16 Recordation

Bringing a valid, federally registered (USPTO or U.S. Copyright Office) right to CBP in order to protect against infringing imports. The recordation process allows CBP to collect and retain information relative to those rights (trademark/tradename/copyright) for a specified time, during which CBP, either of its own initiative or with the assistance of the rights holder, can actively monitor imports in order to prevent the importation of violative articles.

3.17 Service Mark

A word, phrase, symbol, or design, or a combination thereof, that identifies and distinguishes the source of a service of one party from those of others.

3.18 Trade Secret

Any secret formula, pattern, device, or compilation of information used in a business that has some independent economic value, and is used to obtain an advantage over competitors who do not know or use it and the owner of which has taken reasonable measures to keep secret. 18 U.S.C. § 1839(3).

3.19 Trademark

Any word, name, symbol, or device, or any combination thereof “used by a person... to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods.” 15 U.S.C. § 1127.

Chapter 4. AUTHORITIES/REFERENCES

4.1 Authorities

A. 18 U.S.C. § 2318

Trafficking in Counterfeit Labels, Illicit labels, or Counterfeit Documentation or Packaging Accompanying a Work (e.g., counterfeit labels attached to a pirated work to make it look like the copyright holder authorized the copy or distribution of his or her work).

B. 18 U.S.C. § 2319A

Trafficking in Unauthorized Recordings of Live Musical Performances (“Bootlegging”).

C. 18 U.S.C. § 2319B

Unauthorized Recording of Motion Pictures in a Motion Picture Exhibition Facility (“Camcording”).

D. 18 U.S.C. § 2320

Trafficking in Counterfeit Merchandise

Trademark, unlike copyright, can be charged as a felony even if there is only one item sold. There is no misdemeanor trademark violation; however, there are civil penalties available for import violations under 19 U.S.C. § 1526. There are four distinct criminal trademark infringement violations under 18 U.S.C. § 2320:

- 1) The intentional trafficking (meaning any import, export, or transfer of the merchandise for personal or financial gain) of merchandise or services while knowingly using a counterfeit mark;
- 2) The intentional trafficking in labels, cases, packaging, etc., with knowledge that a counterfeit mark has been applied to such labels, cases, packaging, etc. – the use of which is likely to cause confusion or a mistake, or to deceive;
- 3) The intentional trafficking in counterfeit military goods or services with knowledge of the counterfeit or knowledge that the use, malfunction, or failure of the goods or services is likely to cause serious bodily injury or death, disclosure of classified information, impairment of combat operations, or other significant harm; or
- 4) The intentional trafficking in counterfeit drugs.

E. 15 U.S.C. § 1124

Importation of Goods Bearing Infringing Marks or Names Forbidden.

F. 15 U.S.C. § 1125

False Designations of Origin, False Descriptions, and Dilution Forbidden (the Lanham Act).

G. 17 U.S.C. § 506(a)(1); 18 U.S.C § 2319(b)(1)

Criminal Copyright Infringement

Copyright infringement is a crime if the defendant acted willfully (1) for commercial advantage or private financial gain (2) by reproducing or distributing infringing copies of works with a total retail value of over \$1,000 over a 180-day period or (3) by distributing a “work being prepared for commercial distribution” (such as an unreleased motion picture) by making it available on a publicly-accessible computer network. 17 U.S.C. § 506(a)(1). Copyright infringement is a felony if the infringement involved the reproduction or distribution of at least 10 copies of copyrighted works worth in total more than \$2,500 in a 180-day period, or involved distribution of a “work being prepared for commercial distribution” over a publicly-accessible computer network. 18 U.S.C. § 2319. Copyright infringement otherwise constitutes a misdemeanor under 18 U.S.C. § 2319(b)(3).

(Note: Federal courts have held that the unauthorized streaming of copyrighted content online constitutes an “unauthorized public performance” under the Copyright Act and, absent evidence to the contrary, involves the unlawful copying or distribution of copyrighted works. As a result, the Department of Justice (DOJ) considers streaming piracy to be a misdemeanor offense under 17 U.S.C. § 506(a)(1)(A) and 18 U.S.C. § 2319(b)(3).)

H. 17 U.S.C. § 506(a)(1)(B); 18 U.S.C § 2319(c)(1)

Felony Infringement Not for Financial Gain

I. 17 U.S.C. § 506(a)(1)(B); 18 U.S.C § 2319(c)(3)

Misdemeanor Infringement Not for Financial Gain

J. 17 U.S.C. § 506(a)(1)(A); 18 U.S.C § 2319(b)(3)

Misdemeanor Infringement for Private Financial Gain

K. 17 U.S.C. § 506(a)(1)(C); 18 U.S.C § 2319(d)(2)

Felony Infringement for Financially Motivated Uploading of Pre-release Works

L. 17 U.S.C. § 506(a)(1)(C); 18 U.S.C § 2319(d)(1)

Felony Infringement for Non-financially Motivated Uploading of Pre-release Works

M. 17 U.S.C. § 506(a)(2)

Criminal Infringement

Evidence – For purposes of this subsection under 17 U.S.C. § 506, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement of a copyright.

N. 17 U.S.C. § 1201(a)(1)

Circumvention of Technological Measures

O. 17 U.S.C. § 1201(a)(2)

Manufacture, Import, or Traffic in Circumvention Technology

P. 17 U.S.C. § 1201(a)(3)

Definitions Relating to Circumvention of Technology

Q. 17 U.S.C. § 1204(a)

Criminal Offenses and Penalties

R. 18 U.S.C. § 541

Entry of Goods Falsely Classified

This statute covers the knowing entry of goods at less than the true weight or measure, or upon false classification as to quality or value, or by payment of less than the amount of duty legally due.

S. 18 U.S.C. § 542

Entry of Goods by Means of False Statements

This statute covers several separate violations which do not all involve an actual or potential loss of revenue:

- 1) The knowing entry or introduction (or attempt), by means of false statements, oral or written, of merchandise into the commerce of the United States.
- 2) The knowing entry or introduction (or attempt), by means of any false or fraudulent practice or appliance, of merchandise into the commerce of the United States. This includes situations in which no actual falsity occurs in the entry documentation, but where the entry process itself is knowingly used to commit

other violations. For example, someone may legally import merchandise that bears the required country of origin markings with the intention of removing those markings after release of the merchandise from CBP custody. CBP has held that entry under such circumstances was completed by means of a false practice, in violation of this statute.

- 3) Making any false statement in any declaration without reasonable cause to believe the truth of that statement. This differs from the two violations listed above in that the mere making of a knowingly false statement becomes a violation without requiring the U.S. Government to show that the entry of goods was by means of the false statement. If the importer submits information in the entry summary or in any other entry document knowing that the information is false, this act constitutes a violation of this section. SAs should note that there is a restrictive interpretation in the Fifth and Ninth Circuits.
- 4) Procuring the making of any material false statement.
- 5) Any willful act or omission whereby the United States shall or may be deprived of any lawful duties. As opposed to the provisions discussed in Subsections 1-4 above, use of this provision of the statute requires that the act or omission had an impact on duty liability.

This statute is designated as a Specified Unlawful Activity (SUA) under 18 U.S.C. § 1956(c)(7). In addition, property which constitutes or is derived from proceeds traceable to violations of this provision are subject to civil or criminal forfeiture under 18 U.S.C. §§ 981 and 982. Merchandise which is stolen, smuggled, or clandestinely introduced is also subject to civil forfeiture pursuant to 19 U.S.C. § 1595a(c) which is not subject to the requirements of the Civil Asset Forfeiture Reform Act (CAFRA) of 2000. Similarly, any “thing” used to aid in, or facilitate, an import violation contrary to U.S. law is subject to seizure and forfeiture under 19 U.S.C. § 1595a(a).

T. 18 U.S.C. § 545

Smuggling Goods into the United States

Two violations within this statute are applicable to the illicit importation of merchandise:

- 1) Cases in which a violator knowingly and willfully, with intent to defraud the United States, “makes out or passes, or attempts to pass, through the customhouse any false, forged, or fraudulent invoice, or other document or paper.” This could include the use of fraudulent or forged documents to enter merchandise subject to quota restrictions or invoices that contain false prices or other information.
- 2) Cases in which a violator “fraudulently or knowingly imports or brings into the United States any merchandise contrary to law.” Use of this section requires

proof that some other provision of law or regulation was violated in the import transaction. For example, the underlying “predicate” offense could be failure to comply with the entry requirements set forth under 19 U.S.C. §§ 1481 and 1485, mismarking country of origin in violation of 19 U.S.C. § 1304, the unauthorized importation of merchandise bearing a U.S. trademark in violation of 19 U.S.C. § 1526, or trafficking in counterfeit merchandise in violation of 18 U.S.C. § 2320. Essentially, any import-related violation may qualify as a predicate offense provided that an SA can demonstrate that the violation was done fraudulently or knowingly for the purposes of 18 U.S.C. § 545.

This statute is designated as an SUA under 18 U.S.C. § 1956(c)(7). In addition, property which constitutes or is derived from proceeds traceable to violations of this provision are subject to civil or criminal forfeiture under 18 U.S.C. §§ 981 and 982. Merchandise which is stolen, smuggled, or clandestinely introduced is also subject to civil forfeiture pursuant to 19 U.S.C. § 1595a(c) which is not subject to the requirements of CAFRA. Similarly, any “thing” used to aid in, or facilitate, an import violation contrary to U.S. law is subject to seizure and forfeiture under 19 U.S.C. § 1595a(a).

U. 18 U.S.C. § 371

Conspiracy to Commit Offense or Defraud the United States

V. 18 U.S.C. § 546

Smuggling Goods into Foreign Countries

W. 18 U.S.C. § 554

Smuggling Goods from the United States

X. 18 U.S.C. § 1001

Statements or Entries Generally (False Statements)

This statute generally prohibits the making of any material false statement in a matter within the jurisdiction of any agency of the United States. The elements of a violation of 18 U.S.C. § 1001 are included in the elements of a violation of 18 U.S.C. § 542. However, Section 1001 does not require an “importation by means of” the false statement, as does Section 542. Thus, Section 1001 may be considered as an alternative to Section 542 in those circuits where the courts have narrowly defined the materiality requirement of Section 542 or in instances in which a false statement made to CBP is not clearly tied to an import transaction, such as in some drawback fraud and North American Free Trade Agreement cases. It should also be noted that Section 1001 carries penalties (a maximum of 5 years imprisonment) that are higher than those imposed by Section 542 (2 years imprisonment).

A material oral or written false statement provided to an SA during an interview of involved parties can result in this statute being added to an indictment as a stand-alone charge. It can also be used as an admonition by an SA before starting an interview in order to obtain true and accurate information from subjects.

Y. 18 U.S.C. §§ 1341 and 1343

Mail and Wire Fraud

The mail fraud statute (18 U.S.C. § 1341) provides criminal penalties for any use of the U.S. Postal Service (USPS) or of private or commercial interstate carriers, such as the United Parcel Service or Federal Express, in furtherance of any scheme to defraud or obtain money under false or fraudulent pretenses. The wire fraud statute (18 U.S.C. § 1343) provides similar criminal penalties for any use of wire, radio, or telephone communications in interstate or foreign commerce. SAs should always consider the use of mail and wire fraud charges in trade fraud or IP rights infringement cases. Individuals and companies involved in legitimate international trade and importing make extensive use of the USPS and express delivery services and, increasingly, of wire communications such as telephones, facsimiles, and email. In like manner, trade fraud violators may use any of these communication media in furtherance of their criminal activity. They may use them to communicate instructions to a foreign supplier for the preparation or submission of false invoices or to provide copies of documents to foreign suppliers, customs brokers, and CBP. Proof of a mail or wire fraud violation requires the U.S. Government to establish the scheme to defraud, as well as use, the mails or wire communications in furtherance of that scheme. Both 18 U.S.C. §§ 1341 and 1343 qualify as SUAs for money laundering.

Z. 18 U.S.C. § 1956

Laundering of Monetary Instruments

Knowingly concealing the proceeds of an unlawful activity through the conduct or attempted conduct of a financial transaction. (Note: See Chapter 8 for additional information.)

AA. 18 U.S.C. § 1961-1968

Racketeer Influenced and Corrupt Organizations (RICO)

Racketeering is a system of organized crime traditionally involving the extortion of money from businesses by intimidation, violence, or other illegal methods. The RICO statutes target the use of “racketeering activity” or the use of funds obtained through “racketeering activity” to engage in interstate or foreign commerce or in

acquiring or controlling any business or other “enterprise” engaged in, or affecting, interstate or foreign commerce.

4.2 References

- A. 2013 Joint Strategic Plan on Intellectual Property Enforcement Report
<https://www.whitehouse.gov/omb/intellectualproperty/sir>.
- B. DOJ, Prosecuting Intellectual Property Crimes, 2013.
http://www.justice.gov/criminal/cybercrime/docs/prosecuting_ip_crimes_manual_2013.pdf.
- C. Economic and Statistics Administration and United States Patent and Trademark Office, Intellectual Property and the U.S. Economy: Industries in Focus, March 2012, p. vii. http://www.uspto.gov/news/publications/IP_Report_March_2012.pdf.
- D. Patents, United States Patent and Trademark Office.
<http://www.uspto.gov/patents/index.jsp>
- E. Trademark, copyright or patent? United States Patent and Trademark Office.
http://www.uspto.gov/trademarks/basics/trade_defin.jsp
- F. United States Copyright Office Definitions.
<http://www.copyright.gov/help/faq/definitions.html>
- G. Office of Investigations (OI) Handbook (HB) 08-04, Undercover Operations Handbook, dated April 14, 2008, or as updated.

Chapter 5. RESPONSIBILITIES

5.1 Executive Associate Director, Homeland Security Investigations

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

5.2 Assistant Director, National Intellectual Property Rights Coordination Center

The Assistant Director, National Intellectual Property Rights Coordination Center (IPR Center), is responsible for the implementation of the provisions of this Handbook within HSI.

5.3 Special Agents in Charge and Attachés

Special Agents in Charge (SACs) and Attachés are responsible for implementing the provisions of this Handbook within their respective areas of responsibility.

5.4 Special Agents and Intelligence Research Specialists

SAs and, as applicable, IRSs are responsible for complying with the provisions of this Handbook.

Chapter 6. OVERVIEW OF THE IMPORTATION PROCESS AND INTERNATIONAL TRADE FINANCE

International trade continues to grow and is becoming an ever bigger component of the U.S. economy. Although the United States' trading relationships have evolved with various countries around the world, the traditional commercial fraud activity perpetuated by exporters, middlemen, and U.S. importers has been fairly consistent over time.

6.1 Importation Process

When importing goods from other countries, within 15 calendar days of the date that a shipment arrives at a U.S. port of entry (POE), the importer of record must electronically file entry documents with CBP using the Automated Commercial Environment (ACE) that include: 1) the Entry/Immediate Delivery data elements formerly provided on CBP Form 3461, Application and Special Permit for Immediate Delivery (Note: A paper CBP Form 3461 is no longer required.); 2) evidence of the right to make entry; 3) a commercial invoice (or a pro forma invoice when the commercial invoice cannot be produced); 4) a packing list; and 5) other documents necessary to determine merchandise admissibility. Following presentation of the entry, the shipment may be examined, or examination may be waived. The shipment is then released if no legal or regulatory violations have occurred.

An Entry Summary must then be filed along with the estimated duties deposited within 10 working days of the goods' entry. The Entry Summary documents include the Entry Summary filed in ACE (Note: A paper CBP Form 7501, Entry Summary, is no longer required.); any other invoices and documents necessary via the ACE Portal or the Document Image System (DIS) to assess duties, collect statistics, or determine that all import requirements have been satisfied; and payment of duties, taxes, and fees.

Importers of record must also post a bond with CBP to cover any potential duties, taxes, and charges that may accrue. Bonds may be secured through a U.S. surety company in the form of U.S. currency or certain U.S. Government obligations. However, customs brokers will often permit their bond to provide this coverage.

6.2 International Trade Finance

International trade is commonly financed through trade instruments such as letters of credit. Letters of credit reduce risk for exporters and importers by ensuring the delivery of merchandise and release of payment during international trade. Typically, an importer's bank will provide a letter of credit to the exporter's bank guaranteeing payment upon presentation of certain documents such as a bill of lading and commercial invoice. Understanding international trade

financing will assist SAs in conducting a comprehensive investigation not only on the fraud but also on any related money laundering violations.

Individuals involved in IP theft and Internet piracy often rely on Internet payments and money remittance services to facilitate their criminal activity. There is also a likelihood of exploiting digital or virtual currencies to finance this type of criminal activity due to their early adoption by Internet users and the increased anonymity afforded by these types of payment systems.

Chapter 7. OVERVIEW OF INTELLECTUAL PROPERTY THEFT INVESTIGATIONS

7.1 Intellectual Property Theft Background

IP theft investigations are conducted by a multitude of federal agencies, but are primarily led by HSI, the Federal Bureau of Investigation (FBI), the Food and Drug Administration (FDA), and the U.S. Postal Inspection Service (USPIS). CBP detains and seizes infringing merchandise at POEs. Other federal agencies play a role in combating IP theft, including DOJ, USPTO, the U.S. Trade Representative, the Department of State (DOS), the Department of Defense (DOD), and the Offices of Inspector General (OIGs) of a variety of agencies directly involved in the federal government and military supply chain. While the IPR Center coordinates and deconflicts interagency investigations, the Senate-appointed, White House-led Intellectual Property Enforcement Coordinator is responsible for coordinating IP policy on a government-wide scale. In addition, state and local governments routinely enforce state-enacted IP laws. Therefore, IP theft investigations will often require partnerships with other agencies at the federal, state, and local levels. (Note: The U.S. Secret Service has primary jurisdiction over counterfeit U.S. currency.)

IP theft investigations can be broadly divided into copyright, trademark, patent, and trade secret violations.

- A. Copyright law protects against the infringement of rights in original works of authorship fixed in any tangible medium of expression, including computer software; literary, musical, and dramatic works; motion pictures and sound recordings; and pictorial, sculptural, and architectural works. These exclusive rights include the rights of reproduction, public distribution, public performance, public display, and preparation of derivative works. 17 U.S.C. § 106. Legal protection exists as soon as the work is expressed in tangible form. Copyright law protects the physical expression of an idea, but not the idea itself. Although civil law protects all the copyright owner's exclusive rights, criminal law primarily focuses on the rights of distribution and reproduction. 17 U.S.C. § 506(a) and 18 U.S.C. § 2319. Those convicted of criminal copyright infringement face up to 5 years imprisonment and a \$250,000 fine.
- B. Trademarks protect a commercial identity or brand used to identify a product or service for consumers. The following marks are protected under trademark law:

- 1) *Trademarks* are used to identify and distinguish goods from those manufactured or sold by others and to indicate the source of the goods.
- 2) *Service marks* identify the source of services rendered or offered, such as athletic events, television shows, restaurant services, telecommunications services, or retail business services.
- 3) *Certification marks* are used to certify regional or other types of origin, material, mode of manufacture, quality, accuracy, or other characteristics of goods or services, or the identification of a union or other organization associated with a work or laboratory on the goods or services.
- 4) *Collective marks* are used by an association, union, or other group either to identify the group's products or services or to signify membership in the group.

(Note: Trafficking in goods or services that bear a counterfeit mark is banned by 18 U.S.C. § 2320. In 2012, this statute was amended to create new offenses and higher penalties for trafficking in counterfeit drugs and certain counterfeit military goods or services.)

- C. Patent rights are available to anyone who invents “any new and useful process, machine, manufacture, or composition of matter, or any new or useful improvement thereof.” 35 U.S.C. § 101. Unlike copyrights, trademarks, and trade secrets, there are no criminal penalties for committing a patent infringement. A patent grants an inventor the right to exclude others from making, using, offering for sale, or selling devices that embody the patented invention. *See* 35 U.S.C. § 271(a); Eldred v. Ashcroft, 537 U.S. 186, 216 (2003). The U.S. Government's authority to grant patents stems from United States Const. art. I, § 8, known as the Intellectual Property or Copyright and Patent Clause, which authorizes Congress to enact statutes that “promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.”
- D. The Economic Espionage Act of 1996 criminalizes two types of trade secret misappropriation. 18 U.S.C. § 1831 punishes the theft of a trade secret to benefit a foreign government, instrumentality, or agent, while 18 U.S.C. § 1832 punishes the commercial theft of trade secrets carried out for economic advantage, whether or not they benefit a foreign government, instrumentality, or agent.

7.2 Intellectual Property Legislation

In 1998, Congress passed the Digital Millennium Copyright Act (DMCA) in part to fulfill requirements put in place by the World Intellectual Property Organization Copyright Treaty and the Performances and Phonograms Treaty to protect copyrighted works from piracy and promote electronic commerce. The DMCA created two new statutes that are of use in IP theft

investigations: 1) 17 U.S.C. § 1201, prohibition on the circumvention of copyright protection systems; and 2) 17 U.S.C. § 1202, integrity of copyright management information. If violations of either of these statutes are willful and done for the purposes of commercial advantage or private financial gain, significant criminal penalties may be imposed. 17 U.S.C. § 1204(a).

Congress passed the Prioritizing Resources and Organization for Intellectual Property Act in 2008 (Pub. L. No. 110-403). This legislation harmonized provisions related to forfeiture and the destruction of counterfeit goods in 18 U.S.C. § 2323, allowing the forfeiture of “any property used or intended to be used” in IP infringement. It also enhanced penalties for trafficking in counterfeit goods when there is significant bodily harm or death and includes transshipment and exportation as violations of 18 U.S.C. § 2320.

Section 818 of the National Defense Authorization Act of 2012 (Pub. L. No. 112-81) amended 18 U.S.C. § 2320 to add a conspiracy provision. It also included a new violation for trafficking in goods or services with knowledge that the goods or services are counterfeit military goods or services, the use, malfunction, or failure of which is likely to cause serious bodily injury or death, the disclosure of classified information, impairment of combat operations, or other significant harm to a combat operation or a member of the Armed Forces or to national security. The new violation carries enhanced penalties for an initial offense of up to 20 years in prison and fines of \$5 million.

7.3 The Threat of Intellectual Property Crime

The impact of IP theft on the U.S. economy has been substantial. In April 2016, the Organisation for Economic Cooperation and Development (OECD) and the European Union Intellectual Property Office (EUIPO) released a comprehensive review of the impact of counterfeit and pirated goods on the global economy. Using 2013 data for the study, which took several years to complete, the OECD/EUIPO found that “counterfeit and pirated products accounted for as much as USD 461 billion in world trade in 2013... Given that total imports in world trade in 2013 amounted to USD 17 905 billion, this number implies that as much as 2.5% of total world trade in 2013 was in counterfeit and pirated products.” OECD/EUIPO (2016), *Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact*, OECD Publishing Paris. <http://dx.doi.org/10.1787/9789264252653-en>, p. 68, accessed 15 Sep 2016. The OECD/EUIPO go on to note that while they cannot directly compare this study to the ones that they conducted in 2008 and 2009, the general finding is that the results of the current study are of a “significantly higher volume than the finding of the 2008 study”. *Ibid.*

The legal protection of IP rights is intended to protect the United States’ tradition of innovation by discouraging and thwarting thieves from selling cheap imitations of products that are often far less reliable than the original products. These laws also protect public safety by preventing the proliferation of counterfeit pharmaceuticals and other materials that are potentially harmful; they also protect war fighters by preventing the procurement and spread of untested and ineffective knockoff components into the government and military supply chain. In 2012, the Senate Armed Services Committee published an assessment which cited 1,800 events and over one million counterfeit electronic components were discovered by DOD and its suppliers. 112th Congress, 2nd Session, U.S. Senate, Report 112-167, p 12.

IP theft can often be linked to other crimes, such as drugs, gang-related activities, forced child labor, and terrorism. Criminals use IP theft as part of a money laundering scheme and/or as a means to raise funds to support their other crimes.

7.4 Intellectual Property Investigative Initiatives

(b) (7)(E)



Chapter 8. APPLICABLE MONEY LAUNDERING LAWS IN SUPPORT OF INTELLECTUAL PROPERTY THEFT INVESTIGATIONS

Since criminal enterprises engaged in trade fraud and IP theft exist to make illicit profits, federal money laundering laws are appropriate and applicable to the investigation and prosecution of these types of criminal organizations. In fact, applying money laundering and asset forfeiture laws is a powerful means of attacking the IP theft threat. Enhanced penalties for violating money laundering statutes are significant and include fines of up to \$500,000 and/or imprisonment of up to 20 years.

8.1 Money Laundering Laws

Federal money laundering laws require that there be a financial transaction involving proceeds of an SUA with knowledge by the transactor that the funds are proceeds of some felony. The transaction, however, must be accomplished or undertaken for a particular purpose: (1) promote some violation which is in fact an SUA; (2) conceal some aspect (ownership, source, location, etc.) of proceeds derived from an SUA; (3) avoid a reporting requirement; or (4) engage in income tax violations prohibited by 26 U.S.C. §§ 7201 and 7206. Pertinent money laundering statutes include:

- A. 18 U.S.C. § 1956 (a)(1), Domestic Transactions
- B. 18 U.S.C. § 1956 (a)(2), International Transactions
- C. 18 U.S.C. § 1956 (a)(3), Sting Operation
- D. 18 U.S.C. § 1956 (h), Money Laundering Conspiracy
- E. 18 U.S.C. § 1957, Transactions at Financial Institutions

(Note: See the Financial Investigations Handbook (HSI HB 14-03), dated May 13, 2014, or as updated, for more information.)

8.2 Specified Unlawful Activities Related to Intellectual Property Theft

- A. 18 U.S.C. § 541, Entry of Goods Falsely Classified
- B. 18 U.S.C. § 542, Entry of Goods by Means of False Statements
- C. 18 U.S.C. § 545, Smuggling Goods into the United States
- D. 18 U.S.C. § 549, Removing Goods from Customs Custody; Breaking Seals
- E. 18 U.S.C. § 554, Smuggling Goods from the United States
- F. 18 U.S.C. § 1341, Fraud and Swindles (related to mail fraud)
- G. 18 U.S.C. § 1343, Fraud by Wire, Radio, or Television (related to wire fraud)
- H. 18 U.S.C. § 2318, Trafficking in Counterfeit Labels, Illicit Labels, or Counterfeit Documentation or Packaging
- I. 18 U.S.C. § 2319, Criminal Infringement of a Copyright
- J. 18 U.S.C. § 2319A, Unauthorized Fixation of and Trafficking in Sound Recordings and Music Videos of Live Musical Performances
- K. 18 U.S.C. § 2320, Trafficking in Counterfeit Goods or Services
- L. 18 U.S.C. §§ 2341, 2346, Trafficking in Contraband Cigarettes

8.3 Forfeiture Laws

A. 18 U.S.C. § 981, Civil Forfeiture

Any property representing proceeds of violations of 18 U.S.C. §§ 1956, 1957, or 1960, as well as real property (such as houses), is subject to administrative or judicial forfeiture under 18 U.S.C. § 981. The procedural requirements for forfeiture are described under 18 U.S.C. § 983.

B. 18 U.S.C. § 982, Criminal Forfeiture

Criminal forfeiture is available upon conviction; accordingly, to ensure that assets are forfeited to the United States should the indictment fail, SAs are strongly encouraged to pursue *in rem* civil forfeiture against the property itself. The criminal forfeiture law allows for the government to obtain a general judgment against a person and for substitution of assets if the property is not available. The procedural requirements for criminal forfeiture are described in 21 U.S.C. § 853.

C. 19 U.S.C. § 1595a(c) and (d) – Customs Forfeiture Provisions

The use of Title 19 as the procedural basis for seizure and forfeiture is exempt from the provisions of CAFRA, such as the mandatory provision of notice within 60 days of seizure and the “innocent owner defense” under 18 U.S.C. § 983. Although notice must still be given in order to not violate constitutional due process protections, it must be given within a “reasonable” period of time.

(Note: See the Asset Forfeiture Handbook (HSI HB 10-04), dated June 30, 2010, or as updated, for more information.)

8.4 Financial Investigative Methodology

(b) (7)(E)



Chapter 9. CATEGORIES OF COUNTERFEITING

While counterfeiters exploit the latest popular brands and technology in order to maximize their illicit profits, they also profit tremendously from trafficking in ordinary products that consumers rely upon every day.

9.1 Computer Hardware

An ongoing problem with counterfeiting computer chips and fake computer routers and servers passing into the U.S. Government supply chain has grown to be a significant national security threat. The integrity of the U.S. Government supply chain via DOD and General Services Administration (GSA) contracts has been threatened due to independent U.S. vendors sourcing their equipment from counterfeiters and not from original equipment manufacturers. Through (b) (7)(E) HSI works closely with industry and DOD Defense Criminal Investigative Offices (Air Force's Office of Special Investigations (AFOSI), Army Criminal Investigations Division (CID), Defense Criminal Investigative Service (DCIS), and U.S. Naval Criminal Investigative Service (NCIS)) investigators to address this vulnerability.

9.2 Computer Software

U.S. industry loses billions of dollars due to computer software piracy. The United States benefits from its strong information technology sector and advancement in IP development. Computer software piracy has evolved from the smuggling of compact disks – read-only memory (CD-ROMs) of pirated software shipped from foreign source countries – to online downloads of pirated software where consumers can instantly obtain the latest edition of highly in-demand software products.

9.3 Electrical Products

Counterfeit electrical products have also become ubiquitous around the world. This is a serious problem due to the potential for fire hazards and potential harm to sensitive electrical equipment. By counterfeiting the trademark and logo of leading safety and testing authorities in the United States, counterfeiters are able to copy the trusted trademarks and logos and sell fake electrical products where they pose major public safety issues. The trademark violations can be to the rights holder who creates the actual product or to the Underwriter's Laboratory which tests it.

9.4 Food Products

Common foodstuffs are counterfeited and potentially enter the food supply chain. This affects the health and safety of American consumers every day. Counterfeiting of foodstuffs can range from fake infant milk to condiments to beer. For example, due to the high demand of olive oil by consumers, counterfeiters started producing and trafficking fake olive oil. It is recommended that when investigating a case of this type, personnel have the counterfeits tested to determine what dangers they may pose.

9.5 Luxury Items

Luxury items, such as luxury watches and pens, are common types of products that are counterfeited due to consumers' desire to raise their standards of appearance. It is common to find poor-to-average quality counterfeit products of the latest luxury brand names. However, more and more, counterfeiters have raised the quality of these counterfeit products where they are nearly indistinguishable from the real products. As a result, this has a negative impact on the brand companies' bottom line.

9.6 Microelectronics

An integrated circuit (IC) (also known as a semiconductor, microcircuit, microchip, silicon chip, or chip) is a miniaturized electronic circuit that has been manufactured in the surface of a thin substrate of semiconductor material. IC applications can range from consumer electronics to military or space-grade products. The counterfeiting of these products can produce malfunctions, resulting in serious bodily injury or death to the consumer or the American warfighter. Additionally, there is the threat of a cyber intrusion via malware. Each of the 16 (b) (7)(E) partners works closely to combat this threat.

9.7 Movies, Films, Videos, and Streaming

Pirated movies, films, and videos constitute a major part of IP theft. Although consumers can still purchase popular Hollywood movies in the form of digital video disks (DVDs), the availability of online websites and peer-to-peer (P2P) file transfer of movies, films, and videos poses the greatest challenge to the industry and to investigators. The Internet broadband availability to consumers has made streaming of the latest movies, films, and videos ever more popular. Internet movie pirates establish rogue websites around the world, especially in

countries where Internet Service Providers (ISPs) do not respond to legal or law enforcement notices for shutting down the illicit websites.

(Note: As stated in Section 4.1 (G), SAs should be aware that federal courts have held that the unauthorized streaming of copyrighted content online constitutes an “unauthorized public performance” under the Copyright Act and, absent evidence to the contrary, involves the unlawful copying or distribution of copyrighted works. As a result, DOJ considers streaming piracy to be a misdemeanor offense under 17 U.S.C. § 506(a)(1)(A) and 18 U.S.C. § 2319(b)(3).

Additionally, SAs should be aware that content-theft sites have been linked to the intentional download of malware onto computers that visit these sites. (b) (7)(E)

(b) (7)(E)

08-04), dated April 14, 2008, or as updated. SAs should also note that the knowing distribution of malware could potentially be a federal crime and should consult with an Assistant United States Attorney (AUSA) about the specific circumstances of the case.

9.8 Pet Products

HSI and the Environmental Protection Agency (EPA) are aware of counterfeit pesticides (flea and tick prevention) designed to look like legitimately registered products. HSI and DOJ have successfully prosecuted cases in which the supply chains of major retailers have been infiltrated by counterfeit animal pesticides. When trying to identify counterfeit animal products, SAs should look for characteristics, including, but not limited to: 1) products not packaged in child-restraint packaging; 2) missing directions for use; 3) missing EPA registration number; and 4) a foreign labeled product with stickers containing some U.S. information.

9.9 Pharmaceuticals and Personal Health Care and Beauty Products

Pharmaceuticals and personal health care and beauty products are counterfeited and pose a significant health and safety risk to consumers. Consumers purchase pharmaceuticals and personal health care and beauty products with the belief that the products advertised and sold are legitimate products, but in fact they are often purchasing a counterfeit or unapproved version of the product that may have been manufactured in unsanitary conditions and/or may not have been subjected to any safeguards or quality control regimes. It is recommended that, when investigating a case of this type, SAs have the counterfeit items tested to determine what dangers they may pose.

Counterfeiters have leveraged the Internet to effectively sell and distribute counterfeit pharmaceuticals and personal health care and beauty products, including selling medicine without a valid prescription from a doctor. HSI prioritizes its IP investigations to combat the counterfeiting of pharmaceutical drugs and personal health care and beauty products by partnering closely with CBP, FDA, and private industry.

FDA has primary jurisdiction over the FD&C Act. This authority extends to drugs and devices that may be adulterated, misbranded, banned, unapproved, or mislabeled. The sections related to

prohibited acts in the FD&C Act are 21 U.S.C. §§ 331, 352, 353, and 355. This authority is not delegated to CBP.

9.10 Toys and Household Goods

Counterfeit toys and household goods have been known to contain substandard/dangerous contents and are typically not made to the same specifications as the legitimate product. Because of this, they could contain sharp or loose pieces and could be made with toxic materials. It is recommended that when investigating a case of this type, SAs have the counterfeits tested to determine what dangers they may pose.

9.11 Transportation and Heavy Industry Products

Counterfeit automotive, aerospace, rail, and heavy industry products represent a grave public safety threat to people and a potential economic impact to industry. These counterfeit items are often made of substandard materials that can fail at critical times when the genuine item is designed to work. This category can include items such as airbags, brake pads, steering rods, and bearings, as well as the diagnostic equipment used to test them.

9.12 Wearing Apparel and Footwear

While counterfeit branded clothing continues to be a common problem, the quality of such clothing is generally inferior. Additionally, the trafficking of counterfeit sports merchandise and apparel is extremely lucrative and becomes more profitable in markets involving successful and popular teams. The tremendous draw of major sports has paid major dividends by the sale of sports jerseys and apparel to consumers around the world. Counterfeit athletic shoes are a common category for counterfeiters.

Chapter 10. VERIFICATION OF INTELLECTUAL PROPERTY

10.1 U.S. Copyright Office

Copyrights are registered with the U.S. Copyright Office. Although the U.S. Government often proves the existence of a valid copyright by introducing a certificate of registration from the Copyright Office, such registration is not a prerequisite to a criminal prosecution for copyright infringement.

The U.S. Copyright Office's Records Research and Certification Section provides copies of completed and in-process registration records (applications, certificates of registration, and related correspondence), completed and in-process recordation records (recorded documents, certificates of recordation, and related correspondence), search reports, and registration deposit materials. Such requests can include certain documents needed in potential or actual copyright litigation, here or abroad. From the Copyright Office's homepage (www.copyright.gov), there is a link under the "Other Services" column on the far right, entitled "Records Research and Certification Section – Litigation Services." This page is located at <http://copyright.gov/rrc/>.

10.2 U.S. Patent and Trademark Office

Trademarks are registered with the USPTO. Having a registered trademark with the USPTO is required as an element of trafficking in counterfeit goods. The USPTO's website at www.uspto.gov has a considerable amount of information regarding patents and trademarks, including an overview of the process and information on applicable laws, regulations, and policies.

To search the USPTO database for patent information, go to:
<http://www.uspto.gov/patents-application-process/search-patents>.

To search the USPTO data base for registered marks, go to:
<http://tess2.uspto.gov/bin/gate.exe?f=tess&state=4806:5nlwg0.1.1>. To view and download trademark application and registration files, SAs should go to the following:
<http://tsdr.uspto.gov/>.

The USPTO will provide certified copies of trademark registration certificates and certain other documents free of charge to prosecutors and investigators for use in criminal counterfeit court proceedings. They require 3 weeks to process the request. Guidance on this process can be found at: <http://www.uspto.gov/trademark/trademark-documents-prosecutors-official-government-use-only>.

10.3 U.S. Customs and Border Protection

Once copyrights and trademarks are registered, they may be recorded with CBP. Recorded trademarks and copyrights are afforded protection by CBP. For purposes of a criminal investigation into trafficking in counterfeit goods or copyright infringement, CBP recordation is useful, but not a required element of either offense. For information on CBP's recordation of a trademark, HSI personnel can search over 34,000 CBP recordations at CBP's IPR database located at: (b) (7)(E)

Additionally, CBP employs Import Specialists who are responsible for classifying and appraising commercially imported merchandise entering the United States. Import Specialists can provide assistance during the course of an investigation. However, it should be noted that Import Specialists will typically not make a determination on a product that HSI seizes during the course of an investigation, outside of the importation process.

10.4 Brand Holders

SAs should also consider working with brand holders, as they can promptly provide information pertaining to the verification of trademarks and copyrights. This coordination with brand holders will help to legally uphold the seizure and subsequent forfeiture due to counterfeiting or piracy. Brand holders often have experts on staff at their head office or nearby so that SAs can verify the authenticity of any seized goods (b) (7)(E) for trademark and

copyright determination. The IPR Center may be able to connect personnel to a brand holder representative.

Chapter 11. SOURCE AND TRANSSHIPMENT COUNTRIES

While the United States is not immune from counterfeit merchandise production, there are many foreign source and transshipment countries associated with counterfeit merchandise that is shipped around the world. (b) (7)(E)

[REDACTED]

(b) (7)(E)
[REDACTED]

(b) (7)(E)
[REDACTED]

(b) (7)(E)
[REDACTED]

(b) (7)(E)
[REDACTED]

Chapter 12. DISTRIBUTION CHANNELS AND MARKETPLACES OF COUNTERFEIT MERCHANDISE

12.1 Retail Outlets

Counterfeit merchandise is sold in retail outlets throughout the United States. From individual peddlers on the street corner and flea market vendors opened on the weekend to retail shops set up in a strip mall, counterfeit merchandise can be found almost everywhere. Individuals involved in retail counterfeit sales are important because they may possess important information

about their sources of supply and reveal the supply chain that leads to wholesalers and ultimately to the importer that is smuggling the counterfeit merchandise from foreign sources.

Retail outlets may have concealed rooms where counterfeit merchandise is displayed and held as inventory. The bulk of the inventory may be housed in another storage location separate from the retail outlet. There will be code words or a foreign language to denote the counterfeit merchandise. However, the retail vendors will maintain sales records, shipping records, phone logs, and payment records to help identify their illegal trafficking activity and their wholesale sources.

12.2 Wholesale Outlets

Wholesale outlets are typically located in cities close to major U.S. POEs because they deal in larger volumes of merchandise and have ready access to large inventories of counterfeit merchandise. (b) (7)(E)

[REDACTED]

(b) (7)(E)

[REDACTED]

12.3 Business-to-Business (B2B) Online Marketplaces

B2B websites provide buyers and sellers access to the global wholesale market. While trade shows hosted around the world are still very popular, B2B e-commerce technology connects wholesale sellers and buyers for popular consumer products. At the same time, these online marketplaces are also rife with traffickers in counterfeit merchandise. (b) (7)(E)

[REDACTED]

12.4 Business-to-Consumer (B2C) Online Marketplaces

B2C websites connect online buyers and sellers in retail transactions. Websites like eBay, Amazon, Craigslist, and Alibaba are popular examples of B2C marketplaces. While B2C e-commerce businesses are primarily engaged in the sale of consumer merchandise, they are also vulnerable to counterfeiters. This is due primarily to the fact that the size of the marketplace allows counterfeiters to hide among the legitimate sellers. Additionally, counterfeiters know that the marketplace's name adds credibility to the counterfeiter's sales. Further, the payment processing provided by the marketplace makes it easier for the counterfeiter to sell goods online.

(b) (7)(E)




(b) (7)(E)



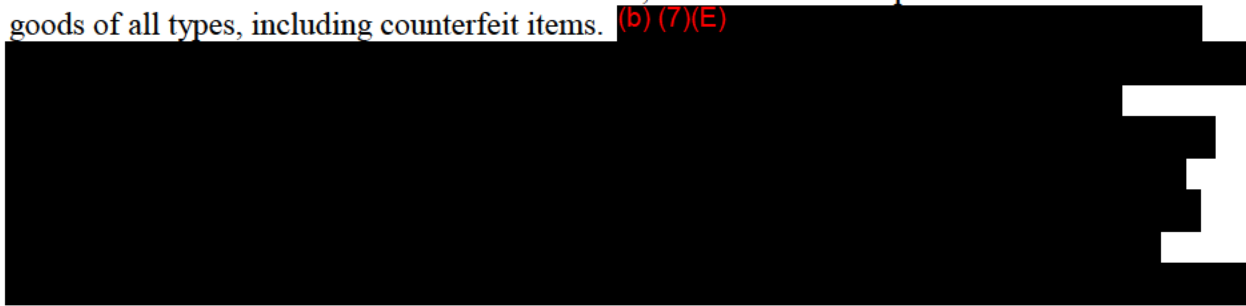
12.5 Virtual Currency

Although not legal tender, the use of virtual currency is growing. (b) (7)(E)



12.6 The Dark Web

Because it can obscure transactions and identities, the Dark Web is ripe for the sale of illicit goods of all types, including counterfeit items. (b) (7)(E)



(b) (7)(E)

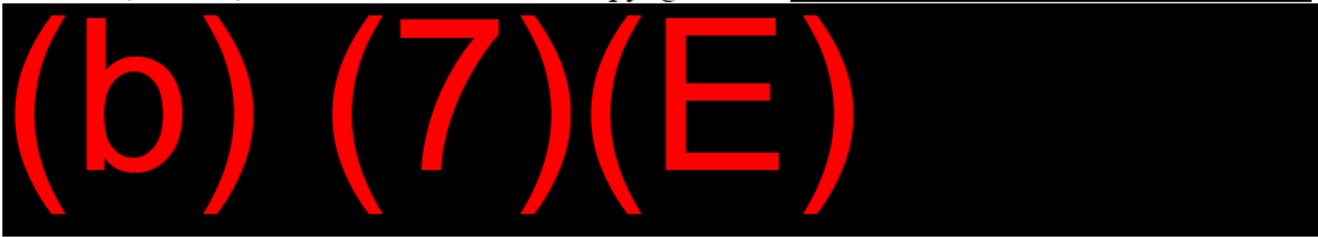


12.7 Express Consignment

The use of express consignment is quickly replacing the shipment of counterfeit goods in large containers. It enables a counterfeiter to ship small discreet packages directly to the consumer; the cost of one or two packages being seized is simply the cost of doing business.

12.8 Warez Groups

Warez Groups are underground, organized piracy groups involved in stealing copyrighted software, movies, and music in violation of copyright laws. (b) (7)(E)




12.9 File Sharing

12.9.1 Peer-to-Peer (P2P) File Sharing Technology

P2P file sharing technology is a popular means of distribution of pirated copyright works. A counterfeiter can store great numbers of pirated songs, software, and movies on a computer and provide access to anyone on the Internet to download the copyrighted works onto their computer. P2P technology has also been associated with data breaches of corporations and organizations through inadvertent file sharing.

File sharing websites have also proliferated on the Internet where users can share photos, videos, music, documents, and copyrighted works using private P2P networks. (b) (7)(E)



12.9.2 Cloud Computing Websites

(b) (7)(E)



12.9.3 Downloads vs. Streaming Content

(b) (7)(E)



Chapter 13. INTELLECTUAL PROPERTY THEFT INVESTIGATIONS

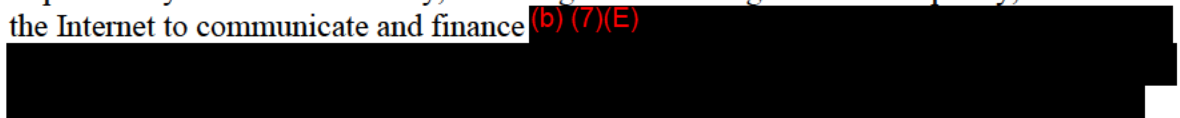
13.1 Investigative Tools

SAs can apply many traditional investigative techniques and tools, including, but not limited to, issuing 19 U.S.C. § 1509 Summonses as implemented in 19 C.F.R. § 163.7 (Summons), as well as grand jury subpoenas, to examine the records, persons, and merchandise at the border or at the premises of an importer/customs broker; conducting the controlled delivery of counterfeit merchandise; (b) (7)(E) conducting consensual electronic recordings, surveillance, and trash runs; interviewing witnesses and suspects; examining financial records; and executing search warrants.

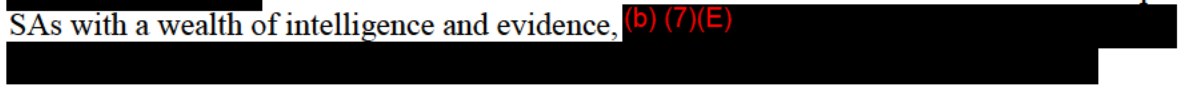
(b) (7)(E)



In practically all criminal activity, including counterfeiting and Internet piracy, criminals' use of the Internet to communicate and finance (b) (7)(E)



Various communication and business channels on the Internet will provide SAs with a wealth of intelligence and evidence, (b) (7)(E)



(b) (7)(E) [Redacted]

13.1.1 ICE (b) (7)(E) [Redacted]

(b) (7)(E) [Redacted] provides a suite of tools to facilitate investigative, analytical, and operational workflows. (b) (7) [Redacted] tools provide an intuitive unified interface to search the (b) (7)(E) [Redacted], (b) (7)(E) [Redacted]. (b) (7)(E) [Redacted]

(b) (7)(E) [Redacted] anchors the (b) (7) [Redacted] program by providing a single interface for searching data sources, creating investigations, and collaborating on analytics. The (b) (7)(E) [Redacted] integrates tools for network analysis, geospatial analysis, and temporal analysis into a single, unified workspace backed by simple powerful search capabilities across various datasets (b) (7) [Redacted] and an intuitive interface for importing end user (E) [Redacted] intelligence from structured (spreadsheet) and unstructured (documents) sources.

(b) (7)(E) [Redacted]

(b) (7)(E) [Redacted]

[Redacted]

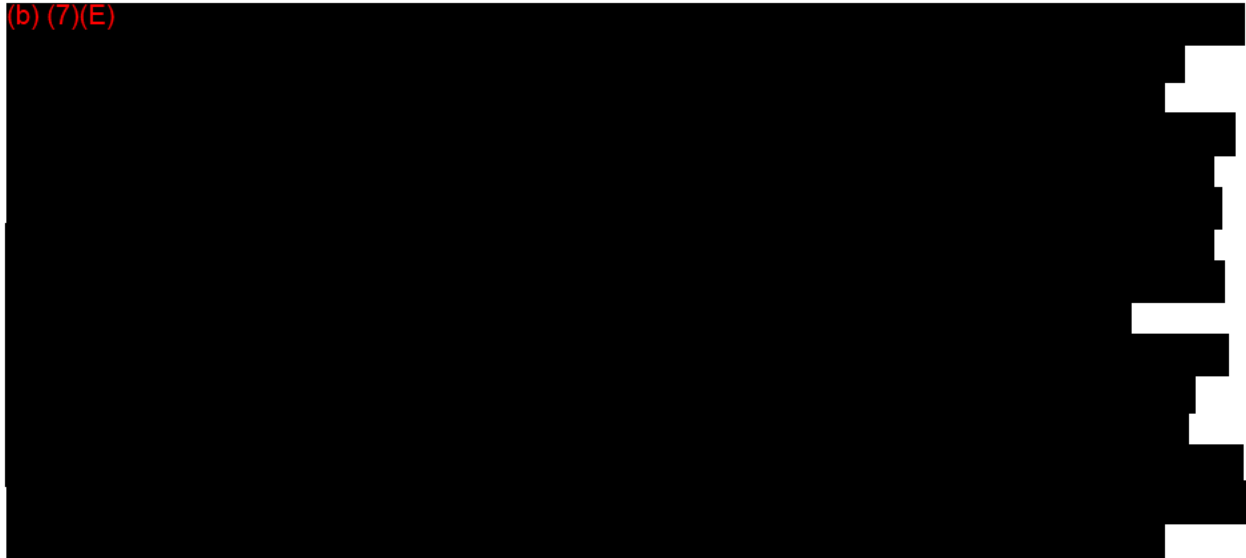
13.1.2 Open Source Internet Research

Traffickers advertise extensively on the Internet. They may have registered domain names, independent stores on online marketplaces, and established websites offering an inventory of

merchandise. It is also common for traffickers, as well as their customers, to actively blog on the Internet. The traffickers may actually host a blogspot where customers provide feedback and advice on their experience as well as on how to evade customs and law enforcement scrutiny.

13.1.3 Websites

(b) (7)(E)



13.1.4 Google Analytics

(b) (7)(E)



(b) (7)(E)



13.1.5 Preservation Letter

Upon discovery of Internet communications such as an email account, social media account, or instant messaging account, SAs should consider seeking the contents of those accounts in order to further their investigations. Under 18 U.S.C. § 2703(f), Requirement to Preserve Evidence, SAs can request the preservation of records and data maintained by an ISP for a period of (b) (7). This legal obligation by ISPs provides SAs with an immediate ability to protect any (b) (7) potential evidence from deletion by a trafficker, and it also provides a window of time to obtain a subpoena, summons, or search warrant for the records and data.

13.1.6 Subpoena, Disclosure by Internet Service Providers, and Notification to Users

SAs may use a summons, a subpoena (including a grand jury subpoena), or a warrant to obtain subscriber, account, and Internet Protocol history information from an ISP or email provider.

(b) (7)(E)




13.1.7 Internet Pen Register/Trap and Trace

(b) (7)(E)



13.1.8 Internet Search Warrants

SAs should seek communications content and other Internet data as mentioned above with respect to Internet Protocol addresses, because they provide a wealth of information about the trafficking activities in IP investigations. (b) (7)(E)

[REDACTED]

[REDACTED]

13.1.9 Online Marketplaces

Traffickers utilize online marketplaces to leverage and advertise their counterfeit merchandise. Some counterfeit sellers offer retail sales while many traffickers also use online marketplaces to drive potential customers to their websites. (b) (7)(E)

[REDACTED]

(b) (7)(E)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(b) (7)(E) [Redacted]

13.1.10 Financial Data Exploitation

Counterfeit traffickers use a full range of financial services from traditional banking and money remittances to online financial services. (b) (7)(E)

[Redacted]

13.1.11 Money Service Businesses

MSBs are online and mobile payment systems that are popular with e-commerce. (b) (7)(E)

[Redacted] (b) (7)(E)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

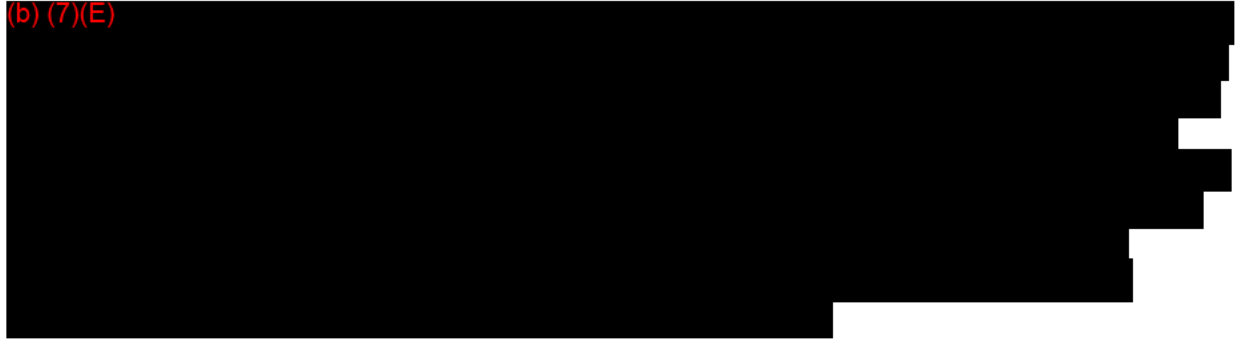
SAs can easily build a case based on the counterfeit sales and financial activity by analyzing this information. (b) (7)(E)

[Redacted]

It should be noted that some MSBs are not subject to the Right to Financial Privacy Act. SAs may use a summons and/or a subpoena for information requests.

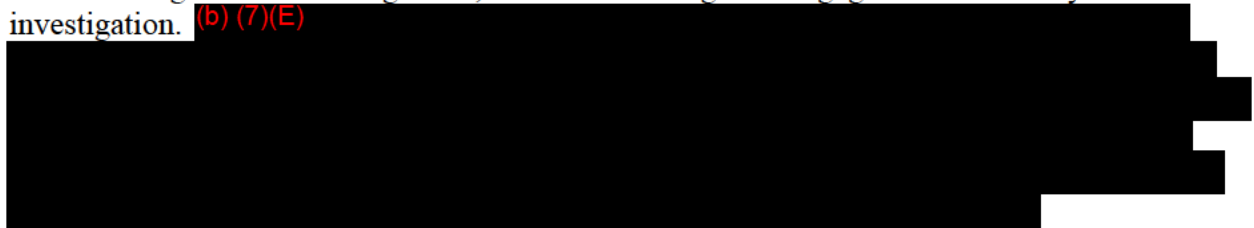
13.1.12 Financial Wire Transfers

(b) (7)(E)



13.2 Coordination with a Prosecutor

In conducting IP theft investigations, SAs are encouraged to engage an AUSA early in the investigation. (b) (7)(E)




(b) (7)(E)



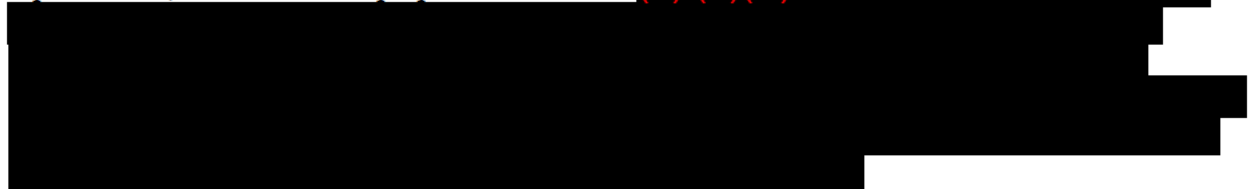
Finally, CCIPS sponsors IP crime related training at DOJ's National Advocacy Center, and there are usually spaces reserved for SAs. Interested SAs should have an AUSA nominate them to attend or reach out to CCIPS directly.

With respect to international IP issues, DOJ's IP Law Enforcement Coordinator (IPLC) program places experienced prosecutors in high-impact regions to enhance individual countries' capacity to investigate and prosecute IP crimes and to develop regional networks to more effectively deter and detect IP crimes. IPLCs accomplish these goals by developing contacts in the region with appropriate IP law enforcement officials and assisting in the regional and bilateral training of prosecutors and investigators in the area of IP crimes. (b) (7)(E)



SAs are also encouraged to maintain contact with the local prosecutors, as many states and local jurisdictions have IP laws that they can enforce. Collaboration with state and local authorities is particularly important as there are numerous times when IP crimes do not rise to the level of a federal prosecution. It should be noted that there will be instances where a case starts at the local level and grows in scope and size to be subsequently adopted by a federal prosecutor.

Regardless of whether a prosecutor works on the federal, state, or local level, when meeting with a prosecutor, SAs should be prepared to discuss: (b) (7)(E)




13.3 Joint Investigations

The IPR Center encourages field personnel to engage their federal, state, and local counterparts when conducting an IP theft investigation. Often, state and local law enforcement are the first to encounter a counterfeiting crime in the community, and many other federal agencies have jurisdiction and expertise that can enhance and broaden an investigation. Some of the larger offices have an Intellectual Property Theft Enforcement Team (IPTET), an informal task force that builds cooperation and enhances coordination between law enforcement partners in an area of responsibility. Offices that have IPTETs place the (b) (7)(E) program code on those cases.

13.4 Working with Brand Holders

As brand holders, companies closely guard their IP, brand, and reputation in the highly competitive marketplace. Companies often proactively scour the marketplace, whether it is the brick and mortar arena or the Internet, to determine IP threats to their company. Companies have established brand managers or hired outside consultants to conduct due-diligence checks of the marketplace for counterfeits and pirated goods. (b) (7)(E)



(b) (7)(E)

Brand holders frequently provide intelligence leads for potential investigation. Combined with CBP seizures and additional financial analysis of suspected individuals and companies, SAs can develop strong cases in fighting counterfeiting. Brand holder representatives are typically enthusiastic about their jobs and can be very helpful. (b) (7)(E)

13.5 HSI Cyber Crimes Center

C3 maintains expertise in the latest computer forensics and cybercrimes trends. SAs who are investigating IP crimes should be aware of the criminal exploitation of computers, smartphones, and remote storage devices, like cloud accounts, by individuals and businesses when carrying out criminal acts. SAs can leverage their local computer forensic agents or contact the Computer Forensics Unit at C3 for additional support in obtaining digital evidence from the aforementioned electronic devices. SAs can also obtain assistance and guidance from the Cyber Crimes Unit with respect to the unique methods of how criminal suspects leverage the Internet and digital devices and accounts. (b) (7)(E)

13.6 ICE Suspension and Debarment

The HSI memorandum entitled, “Expansion of Referrals for Suspension and Debarment,” dated February 24, 2011, or as updated, provides that HSI investigations based on crimes involving egregious offenders, sentences of extreme duration, crimes related to counterproliferation, IPR, commerce regulations, customs violations, and cases involving federal contractors and subcontractors may also be referred for suspension and debarment.

The purpose of suspension and debarment is to protect the U.S. Government and limit future harm by ensuring that the government is conducting business with responsible participants (people or businesses). Suspension and debarment are administrative tools; they are not a punishment and should not be referred to as such or used as leverage during the course of a criminal case. Once debarred, a person and/or company are prohibited from doing business with the U.S. Government. This can include receiving federally funded contracts or benefiting from things such as loans that are insured by the U.S. Government.

When there is a clear nexus that the defendant is a business risk to the U.S. Government and there is an immediate need to protect the U.S. Government, SAs are encouraged to contact the HSI Suspension and Debarment Coordinator as early in the investigation as possible to submit a referral for suspension pending any legal proceedings. SAs should coordinate suspension referrals with their first-line supervisor, the local Office of Chief Counsel, the assigned AUSA, and the Suspension and Debarment Coordinator. SAs may also submit referrals for debarment upon the conviction of a defendant.

SAs must submit all formal referrals for suspension and/or debarment to HSI's Suspension and Debarment Program through their chain of command and signed by their SAC or designee.

Chapter 14. COORDINATING INTELLECTUAL PROPERTY CASES

14.1 National Intellectual Property Rights Coordination Center

The HSI IP investigations program is based at the IPR Center. Utilizing a task force concept, the IPR Center uses the expertise of its member agencies to share information, develop initiatives, coordinate enforcement actions, and conduct investigations related to IP theft. The IPR Center brings together the key U.S. and international agencies involved in the federal administration and enforcement of IP laws which the IPR Center leverages to provide a comprehensive response to IP theft.

14.1.1 National Cyber-Forensics and Training Alliance

The National Cyber-Forensics and Training Alliance (NCFTA) is a non-profit corporation that focuses on identifying, mitigating, and neutralizing cyber-crime threats. The NCFTA operates by conducting real time information sharing and analysis with SMEs in the public, private, and academic sectors. By merging a wide range of cyber expertise in one location, the NCFTA provides a conduit for information sharing. (b) (7)(E)

collect, analyze, deconflict, and share information with IPR Center partners and field offices. Because they regularly coordinate with industry, they are an invaluable resource and, at the request of SAs, they will deconflict, vet, and further develop case information.

14.2 IPR Center Partner Agencies

The IPR Center consists of U.S. federal agencies along with several international partners that have jurisdiction over IP theft or are affected by IP crimes. The IPR Center partner agencies are as follows:

14.2.1 U.S. Customs and Border Protection

CBP brings a whole host of assets to support its IP enforcement. SAs should be familiar with expertise offered by CBP Officers focused on imported merchandise inspections and

enforcement at air, land, and seaports; Import Specialists focused on IP infringement; CBP Laboratories throughout the country, including the Los Angeles laboratory which specializes in supporting IP enforcement; and the CBP Office of the Chief Counsel attorneys who are familiar with customs laws. CBP established the Centers of Excellence and Expertise (CEEs), which bring all of CBP's trade expertise to bear on a single industry in a strategic location. CEEs are staffed with numerous trade positions using account management principles and operational skills to authoritatively facilitate trade. CEEs also serve as resources to the broader trade community and to CBP's U.S. Government partners. CEE personnel answer questions, provide information, and develop comprehensive trade facilitation strategies to address uniformity and compliance concerns. The IPR Center can provide information on how to contact the CEEs. Alternatively, information about contacting a CEE can be found on CBP's website.

The Regulatory Audit (RA) Field Offices are responsible for auditing major importers and other entities involved in international trade compliance with laws and regulations governing the importation and exportation of merchandise. RA conducts hundreds of audits each fiscal year, and these audits provide a means by which to collect and analyze data to determine a likelihood of noncompliance. RA maintains a strong partnership with HSI and can provide invaluable assistance to HSI during the course of a criminal or civil investigation. While this assistance is primarily designed to aid Trade Enforcement investigations, it can also be an important tool in IP investigations. SAs who would like RA's assistance should fill out and submit an HSI referral questionnaire to their local RA office to request assistance at any time. HSI can also refer individuals and entities that are suspected of violating U.S. trade laws, but which do not meet HSI thresholds for opening a case, to RA for an audit. (b) (7)(E)

RA may use this form to obtain further information about referrals from HSI in order to further define the work and resources required. HSI referrals to RA can also be made by sending an email (b) (7)(E). The referral will then be forwarded to the appropriate RA field office.

14.2.2 Department of Commerce

The Department of Commerce, through its Office of Intellectual Property Rights (OIPR), is housed within the agency's International Trade Administration. This office helps U.S. rights holders protect and enforce their IPR in foreign markets. OIPR participates in multilateral and bilateral dialogues to promote U.S. IPR trade policy internationally and monitors countries' compliance with IPR-related trade agreement obligations. This ensures that U.S. companies enjoy access to foreign markets and adequate IPR protection and enforcement abroad. If individuals experience difficulties protecting or enforcing abroad, OIPR experts can help them by suggesting strategies to evaluate the problem and collaborating with Washington, D.C.-based agencies and U.S. embassies around the world to pursue resolution. OIPR also has worked with U.S. Government and private sector partners to develop a number of tools and resources to assist U.S. rights holders, including an educational training module on IPR, country-specific toolkits, and access to volunteer attorneys for a free one-hour consultation.

14.2.3 Consumer Product and Safety Commission

The Consumer Product and Safety Commission (CPSC) is charged with protecting the public from unreasonable risks of injury or death from products that pose a fire, electrical, chemical, or mechanical hazard or can injure children. <http://www.cpsc.gov/>

14.2.4 Federal Bureau of Investigation

The FBI focuses on the theft of trade secrets and infringements on products that can impact consumers' health and safety, such as counterfeit aircraft, car, and electronic parts. <http://www.fbi.gov/about-us/investigate/cyber/ipr/>

14.2.5 Food and Drug Administration's Office of Criminal Investigations

FDA's Office of Criminal Investigations (OCI) employs law enforcement methods and techniques in the investigation of suspected criminal violations of the FD&C Act, the Federal Anti-Tampering Act, and other related federal statutes. OCI investigations concentrate on significant violations of these laws, with a priority on conduct that may present a danger to the public health. <http://www.fda.gov/ICECI/CriminalInvestigations/default.htm>

14.2.6 General Services Administration's Office of Inspector General

The GSA OIG manages a nationwide program to prevent and detect illegal and/or improper activities involving GSA programs, operations, and personnel. The GSA OIG oversees the integrity of the U.S. Government supply chain and any threats to the U.S. Government from counterfeit goods, such as computers, servers, and network devices that may be surreptitiously introduced into the supply chain system. <http://www.gsa.gov/portal/category/21413>

14.2.7 DOS' Office of International Intellectual Property Enforcement

DOS' Office of International Intellectual Property Enforcement (IPE) engages in IPR negotiations in the world's international organizations, oversees the distribution of training and technical assistance funds to help developing countries build IPR law enforcement capacity, and undertakes public diplomacy programs to generate awareness of the importance of IPR protection. <http://www.state.gov/e/eb/tpp/ipe/>

14.2.8 National Aeronautics and Space Administration's Office of Inspector General

The National Aeronautics and Space Administration (NASA) OIG investigates allegations of crime, cybercrime, fraud, abuse, and misconduct having an impact on NASA programs, personnel, and resources. The NASA OIG refers its findings to either DOJ for prosecution or to NASA management for action. Through its investigations, the NASA OIG identifies crime indicators and recommends effective measures for NASA management designed to reduce NASA's vulnerability to criminal activity, including counterfeit equipment entering its supply chain. <https://oig.nasa.gov/>

14.2.9 Nuclear Regulatory Commission

The Nuclear Regulatory Commission (NRC) was created to ensure the safe use of radioactive materials for beneficial civilian purposes while protecting people and the environment. NRC regulates commercial nuclear power plants and other uses of nuclear materials, such as in nuclear medicine, through licensing, inspection, and enforcement of its requirements.

<http://www.nrc.gov/>

14.2.10 Defense Criminal Investigative Service

DCIS is the criminal investigative arm of the DOD OIG. Its main objective is to investigate criminal activities involving terrorism, procurement fraud, computer crimes, illegal technology transfers, and public corruption within DOD. (b) (7)(E)

14.2.11 Defense Logistics Agency's Office of Inspector General

The Defense Logistics Agency (DLA) OIG provides worldwide support to warfighters; detects, identifies, and documents fraud, waste, and abuse; develops and implements actions to correct weaknesses; and ensures that corrective actions are in place and working. The DLA OIG protects the integrity of its supply chain from counterfeit goods, such as counterfeit computer equipment entering its supply chain system. <http://www.dla.mil/HQ/InspectorGeneral.aspx>

14.2.12 U.S. Army Criminal Investigative Command's Major Procurement Fraud Unit

Through six subordinate field offices and 26 resident agencies, the U.S. Army CID's Major Procurement Fraud Unit (MPFU) conducts investigations into allegations of fraud associated with the Army's major acquisition programs. Each year, MPFU recoveries have exceeded the entire U.S. Army CID's operating budget. MPFU protects the integrity of its supply chain from counterfeit goods, such as counterfeit computer equipment entering its supply chain system.

<http://www.cid.army.mil/701st.html>

14.2.13 U.S. Air Force's Office of Special Investigations

A significant amount of AFOSI's investigative resources are assigned to fraud (or economic crime) investigations. These include violations of the public trust involving Air Force contracting matters, appropriated and non-appropriated funds activities, computer systems, pay and allowance matters, environmental matters, acquiring and disposing of Air Force property, and major administrative irregularities. AFOSI uses fraud surveys to determine the existence, location, and extent of fraud in Air Force operations or programs. It also provides briefings to base and command-level resource managers to help identify and prevent fraud involving Air Force or DOD resources. AFOSI oversees the integrity of its supply chain from counterfeit computer equipment entering its supply chain system. <http://www.minot.af.mil/Units/OSI>

14.2.14 U.S. Naval Criminal Investigative Service

NCIS is the federal law enforcement agency charged with conducting investigations of felony-level offenses affecting the U.S. Navy and the U.S. Marine Corps. NCIS also performs investigations and operations aimed at identifying and neutralizing foreign intelligence, international terrorist, and cyber threats to the Department of the Navy. NCIS protects the integrity of its supply chain from counterfeit goods, such as counterfeit computer equipment entering its supply chain system. <http://www.navy.mil/local/ncis/>

14.2.15 U.S. Postal Inspection Service


USPIS investigates crimes related to counterfeit stamps and money orders, fraud schemes, and other crimes that may occur online and which involve the misuse of mail or the postal service, mail fraud, and/or money laundering. <https://postalinspectors.uspis.gov/>

14.2.16 U.S. Postal Service Office of Inspector General

The USPS OIG helps maintain confidence in the postal system and improves USPS' bottom line through independent audits and investigations. Audits of postal programs and operations help to determine whether the programs and operations are efficient and cost effective. Investigations help prevent and detect fraud, waste, and misconduct and have a deterrent effect on postal crimes. The USPS OIG protects the integrity of USPS' supply chain from counterfeit goods, such as counterfeit computer equipment entering USPS' supply chain system. <https://uspsig.gov/>

14.2.17 U.S. Patent and Trademark Office

USPTO is the Federal agency that grants U.S. patents and registers trademarks. USPTO advises U.S. Government agencies on IP policy, protection, and enforcement, and promotes stronger and more effective IP protection around the world. USPTO works with other agencies to secure strong IP provisions in free trade and other international agreements. It also provides training, education, and capacity building programs. USPTO has an Overseas Intellectual Property Rights Attaché program that was designed to promote IP protection and enforcement internationally for the benefit of U.S. stakeholders. They have individuals stationed in the following countries:

 The USPTO Attaché can be a great source of assistance to an IP theft investigation and should be contacted by working through the HSI Attaché in the respective region. <http://www.uspto.gov/>

14.2.18 International Criminal Police Organization

The International Criminal Police Organization (INTERPOL) supports regional and global operations to break up the networks behind IP crime and remove dangerous and sub-standard goods from circulation; delivers specialized IP crime training programs under the umbrella of the International Intellectual Property Crime Investigators College; and facilitates the sharing of intelligence on IP crime via a secure police communications system and specialized database on

International IP Crime. <http://www.interpol.int/Crime-areas/Intellectual-property-crime-and-counterfeiting/Intellectual-property-crime-and-counterfeiting>

14.2.19 Europol

Europol is the European law enforcement agency whose mission is to support the European Union Member States in preventing and combatting all forms of serious transnational crime and terrorism. Europol received the mandate to work on IP-related crime in 2002.

<https://www.europol.europa.eu/>

14.2.20 Government of Mexico, Tax Administration Service (Servicio de Administración y Tributario)

The Government of Mexico's Tax Administration Service (Servicio de Administración y Tributario (SAT) is responsible for enforcing IP and customs laws in Mexico. Through its representative at the IPR Center, SAT has participated in several joint initiatives with HSI.

<http://www.sat.gob.mx/>

14.2.21 Royal Canadian Mounted Police

The Royal Canadian Mounted Police (RCMP) is particularly interested in situations where criminal organizations are believed to be linked to the illegal distribution of counterfeit goods, or if the goods pose a serious threat to public health or safety.

<http://www.rcmp-grc.gc.ca/fep-pelf/ipr-dpi/index-eng.htm>

14.2.22 Federal Maritime Commission

The Federal Maritime Commission is the independent federal agency responsible for regulating the U.S. international ocean transportation system for the benefit of U.S. exporters, importers, and the U.S. consumer.

14.3 DOJ Computer Crimes and Intellectual Property Section

The IPR Center works closely with CCIPS even though it is not an IPR Center partner. CCIPS implements DOJ's national strategies in combating computer and IP crimes worldwide, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts. CCIPS attorneys work to improve the domestic and international infrastructure – legal, technological, and operational – and pursue network criminals most effectively. CCIPS attorneys regularly resolve legal and investigative issues raised by emerging computer and telecommunications technologies; litigate cases; provide litigation support to other prosecutors; train federal, state, and local law enforcement personnel; comment on and propose legislation; and initiate and participate in international efforts to combat computer and IP crime.

14.4 Investigative Support

The IPR Center provides support and analysis to ongoing IP theft investigations. The IPR Center can provide subject matter expertise and intelligence analysis to assist in complex, long-term, Internet-based, or multijurisdictional investigations. (Note: For information on how to obtain assistance, contact the IPR Center’s Trade Enforcement Unit or the Intellectual Property Unit.)

14.5 Outreach and Training

The IPR Center provides outreach to industry, domestic and foreign counterparts, and the public. Training for state and local IP Enforcement Teams is accomplished on a rotating basis. (Note: For more information on how to obtain IPR Center support or additional training, contact the IPR Center’s Outreach and Training Section.)

14.6 International Operation Coordination

The IPR Center manages large scale, international IP operations, such as those conducted under the auspices of the World Customs Organization or INTERPOL. (Note: SAs interested in learning more about future international operations should contact the IPR Center’s Trade Enforcement Unit or the Intellectual Property Unit.)

14.7 Case Deconfliction

The IPR Center receives, analyzes, and deconflicts leads from the public, industry, and other IPR Center participating agencies; coordinates investigative overlap; and notifies rights holders of final enforcement actions.

14.8 IPR Center Deconfliction and Vetting Process

A. New Lead Vetting

- 1) All new incoming unclassified leads received by the IPR Center are forwarded to IPRIS to conduct analysis to identify additional information associated with the targets for inclusion in an unclassified criminal intelligence report.
- 2) IPR Center partners query the target data to identify any investigative, intelligence, and/or regulatory information available. DOJ’s CCIPS will also receive the intelligence report to assist in determining the viability of the lead for a successful criminal investigation and prosecution.
- 3) If there are no active investigations or information, IPR Center partners will determine which, if any, partner will receive the lead based on its merits and the commodity involved.

- 4) If the lead vetting process identifies investigative overlap, the IPR Center will work with IPR Center members to determine the best avenue of coordination and dissemination.
- 5) IPRIS at the IPR Center will forward viable ICE leads to the appropriate HSI office via an (b) (7)(E) [REDACTED]. The IPR Center will track and monitor the progress of the field investigation while continuing to provide investigative, deconfliction, and coordination assistance, as appropriate.

B. Lead Deconfliction

- 1) IPR Center partners query their respective case management systems each week and provide target identification information on newly initiated cases to IPRIS for consolidation and dissemination to IPR Center partners.
- 2) SAs who have requested assistance from the IPR Center will also have their cases deconflicted with IPR Center partners as part of the support process.
- 3) All information provided during the case deconfliction process is the exclusive property of the submitting agency. No further dissemination of the submitted case information will be authorized without prior approval from the originating agency.
- 4) If the lead deconfliction process identifies investigative overlap, the IPR Center will coordinate with IPR Center members to determine the best avenue of coordination and dissemination, with particular emphasis on existing acceptance for prosecution, established undercover activity, and significant seizure activity.
- 5) When overlap is identified and it warrants multiple agency involvement, the lead information will be disseminated to all partners involved and joint investigations will be encouraged.
- 6) If the case vetting process identifies investigative overlap in a matter involving FDA-regulated products, or if there is only one investigative agency with no overlap and the matter involves an FDA-regulated product, FDA OCI may conduct the investigation jointly with the other participating investigative agencies in order to fulfill its public health mission. If FDA OCI determines that a joint investigation involving an FDA-regulated product has potential public health risk, the mitigation of the potential public health risk will take precedence over the investigation.
- 7) Conflicts on case-related matters should be resolved at the field level. If a resolution cannot be agreed upon by field office management, the matter will be forwarded for review and decision by the IPR Center partner agency principals. If partner agency principals do not reach a final determination, the matter will be referred to the executive leadership level of the involved partner agencies.

Chapter 15. DOMAIN NAME SEIZURE PROTOCOLS

15.1 Initial Lead Research

- 1) Upon selecting a website to target, HSI SAs will query open source indices and conduct (b) (7)(E) checks to locate additional information and determine whether HSI is already conducting an investigation related to the lead.
- 2) SAs will assess the site (b) (7)(E) [REDACTED] SAs will also research online complaints against the site and determine whether the site also contains non-criminal content. Additionally, SAs will reach out to rights holders to obtain any derogatory information they may have on the site.
- 3) SAs will conduct further analysis to include checking import/export activity and any related information, including past seizures or impending shipments.
- 4) If SAs determine that the lead could be a viable criminal investigation and that the website is actively being used to violate U.S. laws, has a U.S. nexus, or has potential U.S.-based targets, they can contact the National Program Manager (NPM) for (b) (7)(E) at the IPR Center for guidance on domain name vetting and deconfliction.
- 5) (b) (7)(E) [REDACTED]

15.2 Targeting a Subdomain or Subdirectory

- 1) (b) (7)(E) [REDACTED]
- 2) Sites that merit action must not present any issues with potential cascading takedowns of non-violative sites. (Note: Some domain owners operate primarily to provide retail subdomain registration and domain name services at free or low cost. Each subdomain can have access to a broad range of Internet services arranged through the provider, including email addresses, web space, and file storage and retrieval space.)

- 3) (b) (7)(E) [REDACTED]
- 4) To avoid the seizure of non-violative subdomains, seizure orders for subdomain names should not be served on TLD registries such as VeriSign (the registry for .com, net, .cc, and .tv domains) absent exceptional circumstances. Exceptional circumstances may exist if:
- a) There are no other subdomains associated with the domain name for which seizure is sought; or
 - b) *All* other subdomains associated with that domain name have been identified as facilitating criminal conduct.
- 5) If there are no legitimate subdomains connected to the violative domain name, the seizure order should be directed to the registry of the TLD name.
- 6) However, if the registrant or second level domain is a hosting service that provides subdomains (e.g., MYDOMAIN.FREEHOST.COM) with its registered domain names (e.g., FREEHOST.COM), the seizure order should be directed to the entity providing the DNS service for the subdomain. (b) (7)(E) [REDACTED]
- 7) (b) (7)(E) [REDACTED]
- 8) (b) (7)(E) [REDACTED]

- 9) If the website is foreign-based with no U.S. targets but has a U.S. nexus such as the generic TLD or country code TLD (.com, .net, org, .us, .biz, etc.) that is controlled by a U.S. based registrar, (b) (7)(E)

[REDACTED]

- 10) If the registrar does not respond to the request or refuses to investigate the report of abuse, (b) (7)(E)

[REDACTED]

- 11) SAs can check for the existence of any associated subdomain names using the (b) (7)(E)

[REDACTED]

- 12) Special attention should be given to requests for seizure of domain names for ad-revenue supported sites in which the ads link to illegal content or for domain names of sites that serve as search engines leading to illegal content. Although a linked ad or search may take the user to illegal content, domain name seizure may not be advisable if the site also provides significant legitimate uses. Some ads are dynamic, user-specific, or may be delivered by ad brokers without the input of the site operator. Similarly, sites may have automatic feeds from outside sources. The SA should determine what content is automatically “fed” to the site and what is not. That information may help inform prosecutorial discretion regarding whether to seek *in rem* forfeiture of the site’s domain name.

- 13) (b) (7)(E)
- [REDACTED]

15.3 Targeting Violative Sites for Domain Name Seizure

- 1) (b) (7)(E) [REDACTED]
- 2) (b) (7)(E) [REDACTED]
- 3) Past purchases by the rights holder may be used only to strengthen an affidavit. SAs must independently obtain evidence of Intellectual Property violations. (b) (7)(E) [REDACTED]
- 4) (b) (7)(E) [REDACTED]
- 5) SAs will generate (b) (7)(E) [REDACTED] and a draft affidavit for a seizure warrant. As part of the affidavit, SAs will also complete an attachment that will be labeled “Attachment A,” which will provide instructions to the registry on redirecting the seized website. These documents will be forwarded through the case agent’s chain of command for a complete and comprehensive review. (Note: For IPR Center cases, the chain of command is the Operations Section Chief and the Intellectual Property Unit Chief. In field offices, approval levels will be determined by the SAC.) Once the comprehensive review is complete, the draft affidavit can be sent to the (b) (7)(E) [REDACTED] NPM to ensure that it contains the appropriate procedural language for the redirect of Internet users to the seizure banner. A sample affidavit for a seizure warrant and two sample “Attachment A’s” (one for domestic and one for foreign websites are located in Appendix B. Additional samples can be obtained from the CCIPS Online website. (Note: See Section 13.2 for directions on how to access CCIPS Online.)
- 6) After HSI approval, the draft affidavit will be presented to the AUSAs, both in the criminal division and the civil division, assigned to the case. The decision as to whether the criminal, civil, or both divisions get involved is determined by the

USAO. An in-depth legal review will be conducted by the AUSAs and their respective chains of command before a final affidavit for seizure warrant is created.

- 7) Once a Magistrate Judge reviews and signs the seizure warrant, SAs will serve the seizure warrant on the applicable registry and/or registrar with instructions on when to initiate the seizure and a copy of the seizure warrant provided to the (b) (7)(E) NPM.

15.4 Creating (b) (7)(E), Arrest, or Seizure Reports for Domain Name Seizures

- 1) A subject record must be input in the (b) (7)(E) for each domain name seizure:
- 2) A (b) (7)(E) should also be created for the domain name. This record should include only the domain name without the “www.” prefix. For example: FREEHOST.com, NOT www.FREEHOST.com. This subject record will become the primary violator in the (b) (7)(E) Search, Arrest, or Seizure Reports (SAS) report and that information will populate the violator business name on screen 1 of the SAS report. This record will be linked to the Incident Report.
- 3) If SAs are able to obtain and verify the registrant (operator) of the domain name through the (b) (7)(E), they should create a person or business subject record using that information. (b) (7)(E)
If the domain name uses a proxy/privacy service to hide the registrant’s identity and reflects a U.S.-based registrar, (b) (7)(E)

(b) (7)(E) following information into the specific (b) (7)(E) fields:

- a) Necessary Project Codes: (b) (7)(E)
- b) The place of discovery: (b) (7)(E)
- c) The place of seizure: (b) (7)(E)
- d) (b) (7)(E)
- e) (b) (7)(E)
- f) (b) (7)(E)
- g) (b) (7)(E)

h) Appraised value for all domain name seizures should be \$7.00 (cost as of the date of issuance of this Handbook to obtain the site from the registry for 1 year). This amount was determined in coordination with CBP's Seized and Forfeited Property Division (SFPD) at CBP Headquarters. CBP Fines, Penalties and Forfeitures (FP&F) Officers (FPFOs) have been notified of this value.

i) (b) (7)(E)

j)

k)

l)

m)

n) (b) (7)(E)

(b) (7)(E)

- 6) Since there is no tangible property being turned over to SFPD, there will be no chain of custody (Department of Homeland Security (DHS) Form 6051S, Custody Receipt for Seized Property and Evidence).
- 7) The following items must be provided to SFPD:
 - a) A copy of the seizure warrant signed and dated by the judge.
 - b) A signed copy of the "Return and Certification" form indicating that the warrant was executed and sworn before a judicial officer.
 - c) Any attachments that are made a part of the seizure warrant describing seizure procedures, etc.

15.5 Transferring Custody of a Forfeited Domain Name

- 1) Domain name seizures, unless otherwise requested by the seizing office, will be forfeited administratively by FPFOs under the CAFRA of 2000 and are therefore subject to all CAFRA timelines.

- 2) The case agent should request two copies of the declaration of forfeiture from the FPFO. One of those copies should be provided by the case agent to the registry of the TLD. The other should be placed in the case file.
- 3) After completing the forfeiture process, the FPFO will update (b) (7)(E) by adding the disposition of the line item and updating the case status. A new case status code (b) (7) has been created for the purpose of updating the case when the Disposition Order (CBP Form 7605) is issued. A new code (b) (7) has been created for the closing disposition.
- 4) The case agent must complete the Disposition Order (CBP Form 7605) and return it to the FPFO.
 - a) In Block #7, the Property should be released to the Director, Network Engineering and Design Branch in the ICE Office of the Chief Information Officer (OCIO). SAs will use ICE, 801 I Street, NW, Suite 700, Washington, D.C., 20536, as the address and 202-732-2000 as the telephone number.
 - b) In Block #8, the disposition accomplished date is the date the entry was completed in (b) (7)(E). The person receiving the property is the Director, Network Engineering and Design Branch in ICE OCIO. The Seizing Agency Representative is the case agent.
 - c) The Seized Property Custodian for the case agent's office signs Block #9.
- 5) The Disposition Order (CBP Form 7605) will be forwarded to the appropriate HSI case agent to accomplish the line item disposition in (b) (7)(E). When the HSI case agent accomplishes the disposition to the physical status of the line item through PMPM, Option 7, this will trigger a change from the physical status "HE" to the physical status (b) (7) and the (b) (7) disposition will close the line item in (b) (7)(E). The HSI case agent must return CBP Form 7605 to the FPFO within 30 days and send a copy of the completed form to the (b) (7)(E) NPM.

SAs should contact the (b) (7)(E) NPM at the IPR Center for additional information on seizing domain names or to redirect a seized or forfeited domain name to a seizure banner.

(b) (7)(E)



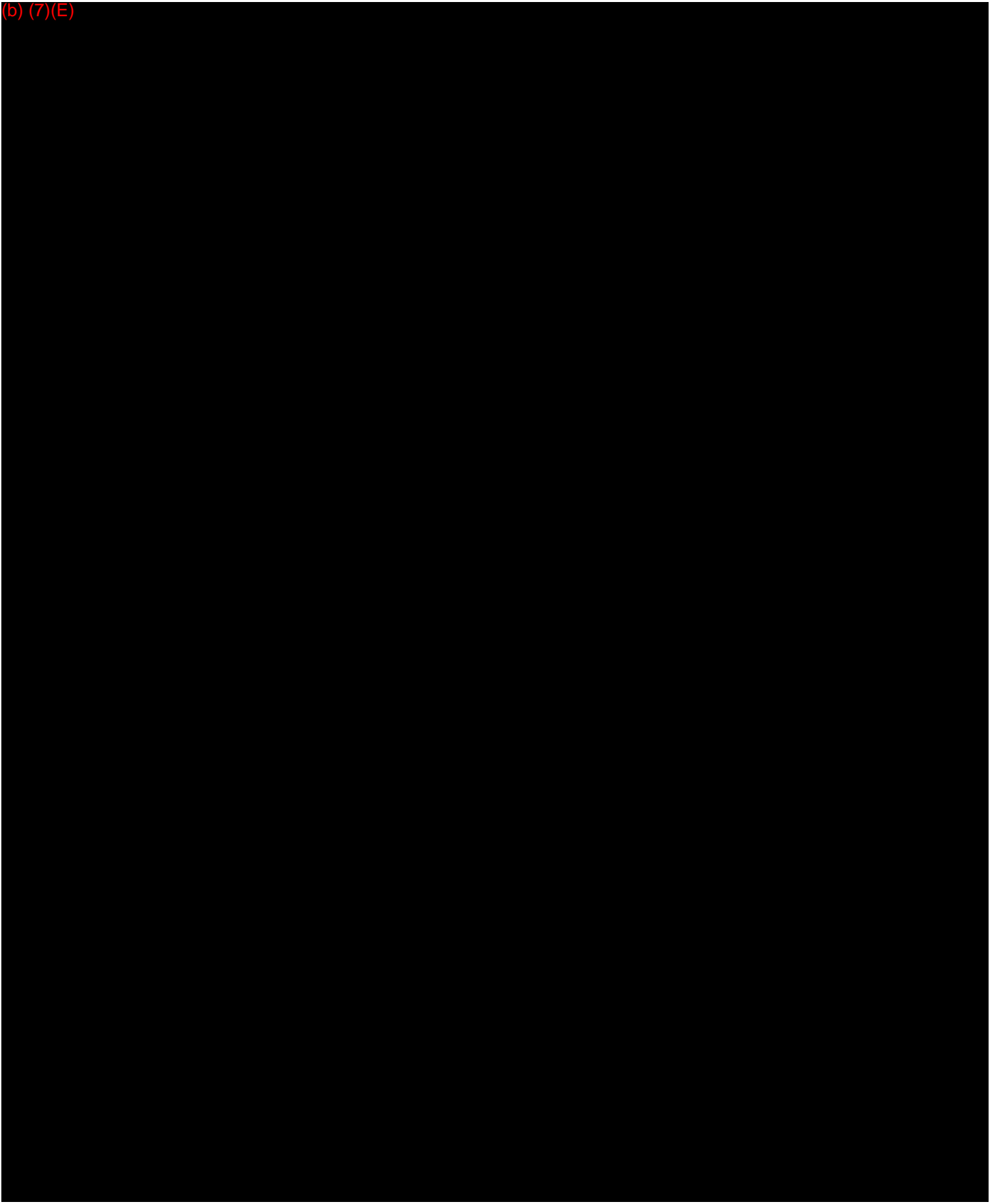
(b) (7)(E)



(b) (7)(E)



(b) (7)(E)



(b) (7)(E)



(b) (7)(E)



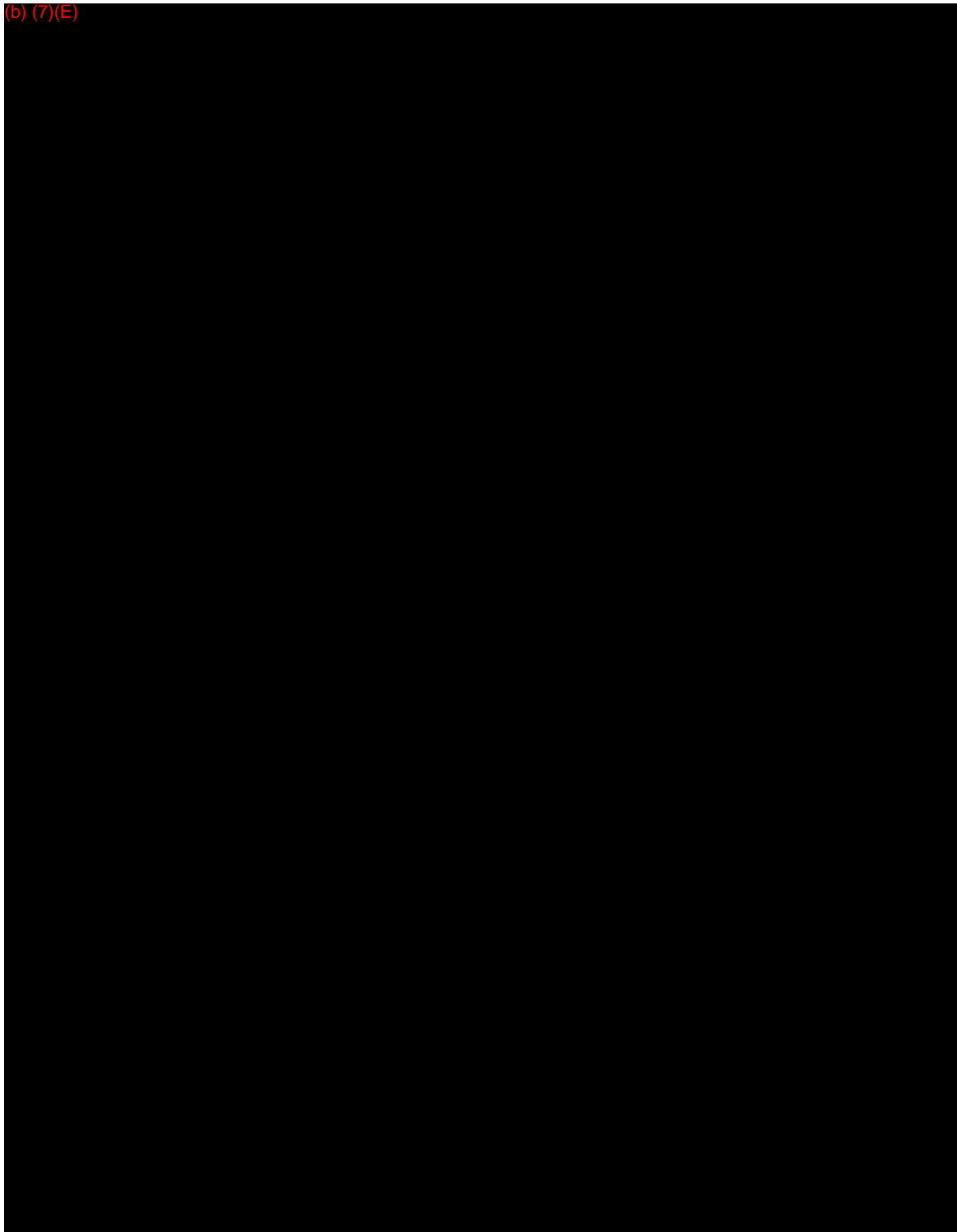
(b) (7)(E)



(b) (7)(E)



(b) (7)(E)



(b) (7)(E)



(b) (7)(E)



ACRONYMS

ACE	Automated Commercial Environment
AFOSI	U.S. Air Force Office of Special Investigations
AFRINIC	African Internet Registry
APNIC	Asia Pacific Internet Registry
ARIN	American Registry for Internet Numbers
AUSA	Assistant United States Attorney
B2B	Business-to-Business
B2C	Business-to-Consumer
BTC	Bitcoin
C3	Cyber Crimes Center
CAFRA	Civil Asset Forfeiture Reform Act
CBP	U.S. Customs and Border Protection
CCIPS	Computer Crimes and Intellectual Property Section
CD-ROM	Compact Disk – Read-Only Memory
CEE	Center of Excellence and Expertise
C.F.R.	Code of Federal Regulations
CHIP	Computer Hacking and Intellectual Property
CHIPS	Clearing House International Payments System
CID	Criminal Investigations Division
CLEAR	Consolidated Lead Evaluation and Reporting
CPSC	Consumer Product Safety Commission
(b) (7)(E)	
DCIS	Defense Criminal Investigative Service
DHS	Department of Homeland Secretary
DIS	Document Image System
DLA	Defense Logistics Agency
DMCA	Digital Millennium Copyright Act
DNS	Domain Name System
DOD	Department of Defense
DOJ	Department of Justice
DOS	Department of State
DVD	Digital Video Disk
(b) (7)(E)	
EDTD	Enforcement and Removal Operations Detention Telephone Data
EID	Enforcement Integrated Database
EPA	Environmental Protection Agency
EUIPO	European Union Intellectual Property Office
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FD&C Act	Food and Drug Cosmetic Act

FOUO	For Official Use Only
FP&F	Fines, Penalties and Forfeitures
FPFO	Fines, Penalties and Forfeitures Officer
GSA	General Services Administration
HB	Handbook
HSI	Homeland Security Investigations
IC	Integrated Circuit
(b) (7)	
ICC	Illicit Cyber Commerce
ICE	U.S. Immigration and Customs Enforcement
ICM	Investigative Case Management
ID	Identification
INTERPOL	International Criminal Police Organization
IOS	In Our Sites
IP	Intellectual Property
IPE	Office of International Intellectual Property Enforcement
IPLEC	Intellectual Property Law Enforcement Coordinator
IPR	Intellectual Property Rights
IPR Center	National Intellectual Property Rights Coordination Center
IPRIS	IPR Intelligence Section
IPTET	Intellectual Property Theft Enforcement Team
ISP	Internet Service Provider
IRS	Intelligence Research Specialist
LACNIC	Latin American and Caribbean Internet Address Registry
MPFU	Major Procurement Fraud Unit
MSB	Money Services Business
NASA	National Aeronautics and Space Administration
NCFTA	National Cyber-Forensics and Training Alliance
NCIS	Naval Criminal Investigative Service
NPM	National Program Manager
NRC	Nuclear Regulatory Commission
OCI	Office of Criminal Investigations
OCIO	Office of the Chief Information Officer
(b) (7)(E)	
OECD	Organization of Economic Cooperation and Development
OEN	Operation Engine Newity
OI	Office of Investigations
OIG	Office of Inspector General
OIPR	Office of Intellectual Property Rights
OTP	Operation Team Player
P2P	Peer to Peer
POE	Port of Entry
RA	Regulatory Audit
RAA	Registrar Accreditation Agreement
RCMP	Royal Canadian Mounted Police

RICO	Racketeer Influenced and Corrupt Organization
RIPE	Regional Internet Registry for Europe, the Middle East, and parts of Central Asia
SA	Special Agent
SAC	Special Agent in Charge
SAS	Search, Arrest or Seizure
SAT	Servicio de Administración y Tributario
(b) (7)(E)	
SEN	Significant Enforcement Notification
SFPD	Seized and Forfeited Property Division
SME	Subject Matter Expert
SUA	Specified Unlawful Activity
TLD	Top Level Domain
TLS	Telecommunications Linking System
UA	Universal Analytics
UC	Undercover
URL	Uniform Resource Location
USAO	U.S. Attorney's Office
U.S.C.	United States Code
USPIS	U.S. Postal Inspection Service
USPS	U.S. Postal Service
USPTO	U.S. Patent and Trademark Office