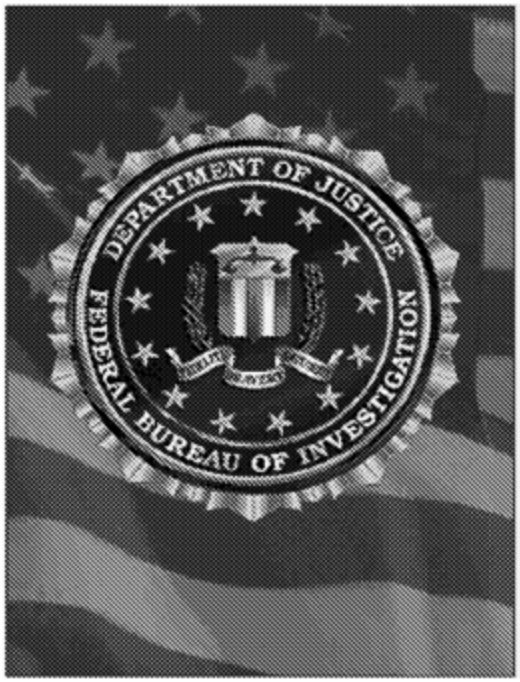
(U) Cyber Division Policy Implementation Guide



(U) Federal Bureau of Investigation

(U) Cyber Division

(U) 0395PG

(U) March 31, 2011

GENERAL INFORMATION: Questions or comments pertaining to this Policy Implementation Guide can be directed to:

Cyber Division

Division Point of Contact: Division Policy Officer

Guidance Point of Contact: Investigative Program Manager

Supersession Information:

Appendix D provides a list of policy and guidance documents superseded by this document.

This document is a new publication; no previous versions available.

Table of Contents

List of Appendices

1. (U) Scope

(U) **Purpose:** The purpose of this policy implementation guide (PG) is to provide instruction for the management and conduct of cyber investigations; to align operational guidelines with current registration and notification requirements; to articulate the basis for cyber investigations and specify the operational and procedural requirements within those investigations; and to ensure that investigations comply with any applicable laws, statutes, regulations, Attorney General's Guidelines, such as the *Attorney General's Guidelines for Domestic FBI Operations* (AGG-Dom), or any internal Federal Bureau of Investigation (FBI) policy, such as the *Domestic Investigations and Operations Guide* (DIOG) or any other applicable or successor document(s).

(U) The Cyber Division PG (CyDPG) is composed of four separate documents, three of which are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO) [redacted] b7E provisions of the CyDPG are maintained in Appendix A, and contain policy guidance regarding Cyber Division's (CyD) national security mission. Appendices B and C also exist as separate documents, and contain guidance specific to the Innocent Images National Initiative (IINI) and InfraGard® Programs, respectively.

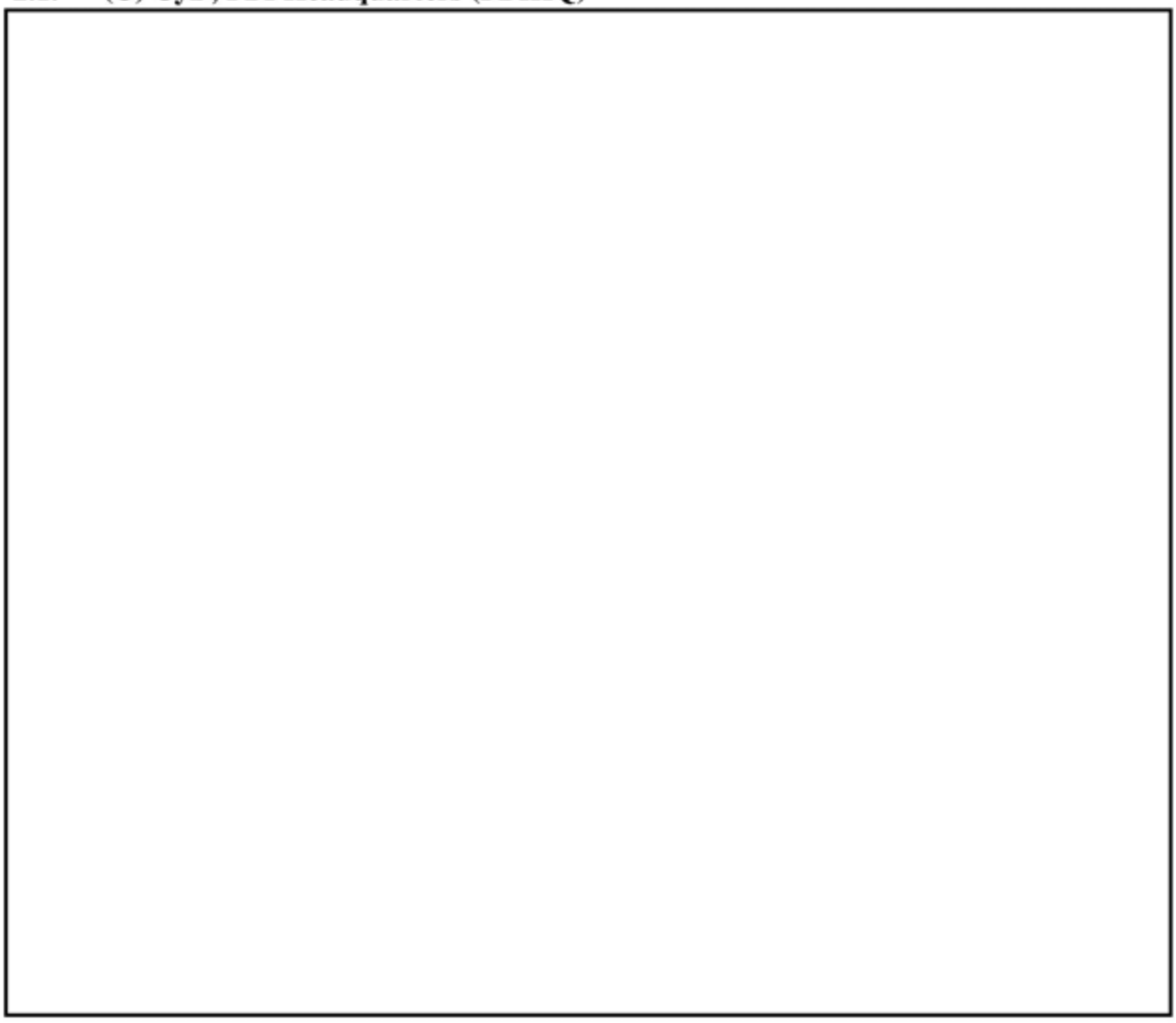
(U) **Intended Audience:** This PG is intended for FBI personnel, task force officers, and contractors involved in the management or investigation of CyD investigative matters. Refer to Section 4.3 of this PG for a list of the investigative classifications covered by this guide.

Link to Policy: Corporate Policy Directive 0395D

2. (U) Roles and Functional Responsibilities

2.1. (U) CyD, FBI Headquarters (FBIHQ)

b7E



2.2. (U) Field Offices and Task Forces

b7E

2.3. (U) Cyber Initiative and Resource Fusion Unit (CIRFU)

b7E

2.4. (U) Internet Crime Complaint Center (IC3)

b7E

3. (U) Policies

3.1. (U) General Investigative Policies

(U) All Bureau personnel supporting criminal cyber investigations are expected to follow all applicable FBI policy, to include the DIOG.

(U) Investigators must always consult the Corporate Policy Office's (CPO) Policy and Guidance Library on the [redacted] for current, program-specific policy guidance. b7E

3.2. (U) Additional Resources

(U) United States (U.S.) DOJ Online Investigative Principles for Federal Law Enforcement Agents (DOJ-OIP)

(U) The DOJ has issued guidance for all federal law enforcement agencies regarding conducting online investigations. The document, structured as "Principles" and "Commentary," uses analogies to compare online law enforcement activities to their closest physical world counterparts.

(U) DOJ Investigative and Prosecutive Guidebooks

(U) The DOJ publishes numerous guidebooks, often referred to as "DOJ Blue Books," which contain extensive guidance to assist investigators in conducting focused investigations in a manner that will lead to successful prosecution. Examples of titles relevant to the investigation of criminal cyber matters include:

- (U) Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations
- (U) Prosecuting Intellectual Property Crimes
- (U) Investigating Trademark Counterfeiting Crimes, a Field Guide
- (U) Identity Theft and Social Security Fraud

4. (U) Investigative Program Information and Guidance

4.1. (U) CyD's National Strategy

(U) CyD's strategic objective is to proactively identify and disrupt the activities of threat perpetrators while protecting the freedom, privacy, and civil liberties of Americans. The global, transcendent nature of the information infrastructure further demands that the FBI engage each of the cyber threats through coordinated partnership with government, academic, and private sector agencies, both domestically and internationally.

b7E

(U) While not all cyber investigations will fall into a currently active TFC, the FBI supervisory special agent (SSA) in a TFC acts as the program manager and primary point of contact (POC) for all FBI field investigations within the scope of that TFC. All aspects of a field investigation requiring FBIHQ, DOJ, interagency, or extraterritorial coordination must be organized through or with the knowledge of the TFC program manager. Likewise, all FBI field intelligence, analysis reporting, and intelligence products must be shared and coordinated with the FBI intelligence components in the TFC, in a manner consistent with Directorate of Intelligence (DI) program guidance and procedures.

(U) Cyber matters in field offices and Legal Attaché (Legat) offices that do not fall within the scope of an existing TFC or other initiative are managed by the CyD program manager assigned responsibility for cyber investigations in that respective field office or Legat. The current program manager assignments can be found on the

b7E

4.2. (U) CyD National Investigative Priorities

(U) The FBI's strategy to address cyber domain issues is built around a threatcentric approach: the cyber threat sets the foundation for the investigative priorities; the priorities frame the national strategy; and the strategy drives the commitment of resources.

b7E

b7E

(U) The relative scope and severity of these identified threats are the foundation of the CyD national investigative priorities. Unlike some of the threats addressed through other FBI investigative programs, the disparate, transcendent nature of the cyber threat affects our nation on a national and international scale rather than on a regional or local scale. There are few, if any, local or regional characteristics that would significantly alter the threat to any particular city or region in a manner considerably different from the effect the cyber threat has on the Nation as a whole. As a result, the following national priorities are widely applicable throughout operational field offices:

b7E

(U) All remaining classifications are the lowest priority investigative matters, absent articulable, extenuating circumstances relating to the magnitude of a subject's activity and the impact a successful investigation would have toward eliminating that criminal threat on a national scale.

b7E

(U) Refer to th for specific details regarding the national investigative priorities.

4.3. (U//FOUO) Investigative Classifications

(U//FOUO) The following tables list FBI investigative classifications that fall within the purview of this PG.

4.3.1. (U//FOUO) Computer Intrusion Matters

b7E

288A		
288B		
288C		
288D		
288E		
288F		
288G		
288H		
288I		
288J		
288K		
288L		

4.3.2. (U//FOUO) Child Pornography and Child Exploitation

b7E

305A	
305B	
305C	
305D	

4.3.3. (U//FOUO) IPR

b7E

334A	
334B	

b7E

334C		
334D		
295A		
295B		
295C		
295D		
295E		

4.3.4. (U//FOUO) Internet Fraud, Identity Theft, and Other Cybercrimes

b7E

196E		
092U		
253E		
258C		
316A		
316B		
316C		
316D		

4.3.5. (U//FOUO) InfraGard®

314		

4.3.6. (U//FOUO) Classifications Regarding Training and Enabling

b7E

001M		
001N		
305E		

308L		
163L		
163K		

b7E

4.4. (U//FOUO) 288)

4.4.1. (U//FOUO) 288B -

4.4.2. (U//FOUO) 288J -

b7E

4.4.3. (U//FOUO) 288A

4.4.4. (U//FOUO) 288K b7E

4.4.5. (U//FOUO) 288I - b7E

4.4.6. (U//FOUO) 288C-H and 288L - b7E

b7E

288C
288D
288E
288F
288G
288H
288L

4.5. (U//FOUO) (305A-D) b7E

(U//FOUO) The Innocent Images National Initiative (IINI) is a national FBI initiative that comprehensively addresses crimes related to child pornography and the sexual exploitation of children through the use of online computers. All program management of the 305 classification is incorporated into the IINI.

(U//FOUO) Information and operational policy relating to the unique investigations and operations conducted within the IINI are documented in Appendix B of this guide.

4.6. (U//FOUO) IPR

(U//FOUO) Legal constructs have created enforceable rights in certain intangibles, which have become known as intellectual property. These include copyrights, trademarks, patents, and trade secrets. While intellectual property was originally only enforceable through civil remedies, the federal government has created several criminal provisions in the interest of further enhancing the protection of intellectual property, especially where the intellectual property relates to an important economic interest. Some misuse of intellectual property, such as patent infringement, has not been criminalized.

(U//FOUO) DOJ's Computer Crime and International Property Section (CCIPS) has developed investigative and prosecution guidance to assist with intellectual property investigations. CCIPS released *Prosecuting Intellectual Property Crimes* and *Investigating Trademark Counterfeiting Crimes, a Field Guide*, to assist investigators with understanding the legal and evidentiary requirements for conducting IPR investigations.

(U//FOUO) Within the IPR program, the top priority is the investigation of counterfeit goods affecting health and safety (classification 334) and non state-sponsored theft of trade secrets (classification 295A). These classifications are followed by criminal violations related to copyrights (classifications 295B/C) and trademarks (classification 295D), which usually involve some form of the unauthorized or counterfeit use or reproduction of protected intellectual property. The statutes criminalizing signal theft (classification 295E) are part of the system that protects the dissemination of intellectual property. Program management of IPR matters at FBIHQ is fully integrated with the interagency IPR center. Requests for investigative assistance in IPR matters are addressed in Section 6.2.1.5 of this PG.

4.6.1. (U//FOUO) 295A - [redacted] b7E

(U//FOUO) A trade secret is any formula, pattern, device, or compilation of information used in a business to obtain an advantage over competitors who do not know or use it. A trade secret includes all forms and types of information – financial, business, scientific, technical, economic, or engineering – that the owner has taken reasonable measures to keep secret and that has independent economic value because it is not generally known to, or ascertainable by, the public.

(U//FOUO) The Economic Espionage Act of 1996 (EEA), 18 U.S.C. §§ 1831-1839, contains two separate provisions that criminalize the theft or misappropriation of trade secrets. The first provision, codified at 18 U.S.C. § 1831, is directed toward foreign economic espionage and requires that the theft of the trade secret be used to benefit a foreign government, instrumentality (company), or agent (individual). If the investigation may be related to a foreign power, the investigator must immediately notify the appropriate field office squad handling economic espionage matters or the appropriate FBIHQ CD-4 program manager.

(U//FOUO) The second provision of the EEA, 18 U.S.C. § 1832, centers on the criminal activity between U.S. companies and/or individuals in which the theft is purely for economic commercial advantage or revenge. The 295A classification is to be used for the investigation of the nonstate-sponsored theft of trade secrets as described in 18 U.S.C. § 1832. The statute also prohibits attempts and conspiracies to misappropriate trade secrets.

4.6.2. (U//FOUO) 295B/C – [redacted] b7E

(U//FOUO) The 295B classification is reserved for the investigation of copyright violations relating to computer software, and the 295C classification is used for the investigation of all other types of copyright violation investigations.

(U//FOUO) Copyright law protects the original expression of an idea or concept in tangible form (e.g., a novel, a song, a carpet design, or a computer source code), but does not extend to protection of the idea or concept itself. Specifically, Congress provided copyright protection to all "original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." See 17 U.S.C. § 102(a).

(U//FOUO) Note: Copyright law protects interests distinct from those protected by patent laws and trademark laws. Patent laws provide exclusive rights to inventors or their licensees of patented processes, machines, manufactures, compositions of matter, plants, and designs. Trademark laws protect the exclusive use of certain names, slogans, and symbols in connection with certain goods or services.

(U//FOUO) Generally, copyright infringement occurs by violating one of five exclusive rights granted to a copyright owner by federal law. 17 U.S.C. § 106. The five exclusive rights are:

1. (U//FOUO) Reproduction.
2. (U//FOUO) Distribution.
3. (U//FOUO) Public display.
4. (U//FOUO) Public performance.
5. (U//FOUO) Preparation of derivative works based upon the original copyrighted work.

(U//FOUO) The Internet's inherent characteristics, such as its success as a communications medium, the large number of people worldwide who use it, and the ease with which materials may be made available for copying have contributed to an explosive growth in copyright infringement. Media products produced today, including software and music, are often in a digital format, which permits production of copies equal in quality to the original. The digital nature of today's media products also makes them much easier to distribute in large-scale to a large audience over the Internet [redacted] b7E

(U//FOUO) Internet piracy cases have characteristics distinguishing them from more traditional copyright infringement cases, including infringement without profit motive; unusual proof issues for quantity, loss, and identity; disclaimers; sympathetic defendants, including juveniles; and novel means of infringement, including file-sharing technologies and other forms of facilitating infringement. Although punishment can be harsher if the infringer is financially motivated, current law provides for prosecution of willful infringement in the absence of these monetary considerations. Even if the infringer is not profiting from such actions, that person is considered to be facilitating the theft of intellectual property from its creator (see 18 U.S.C. § 2319 and 17 U.S.C. §§ 506(a)(1)(b) and 506(a)(1)(c)).

(U//FOUO) In addition to the statutes relating to criminal infringement of copyrights, Congress has enhanced the integrity of the copyright system by specifically prohibiting trafficking in counterfeit labels designed to be affixed to phonorecords, copies of computer programs, motion

pictures, and audiovisual works, as well as trafficking in counterfeit documentation and packaging for computer programs (see 18 U.S.C. § 2318). [redacted] b7E

[redacted]

(U//FOUO) A significant number of other federal statutes are important in copyright cases. For example, most large-scale copyright cases involve the unauthorized use of a trademark in violation of 18 U.S.C. § 2320. For instance, infringing copies of movies will typically be sold with packaging bearing the trademark of the rightful owner or distributor. In addition, other criminal laws, from the familiar such as mail and wire fraud (18 U.S.C. §§ 1341 and 1343, respectively), to the obscure, such as unauthorized reception of cable service (47 U.S.C. § 553) or the unauthorized use of communications (47 U.S.C. § 605) can be applicable as well.

4.6.3. (U//FOUO) 295D [redacted] b7E

(U//FOUO) A trademark is "any word, name, symbol, or device, or any combination thereof -- (1) used by a person, or (2) which a person has a bona fide intention to use in commerce and applies to register on the principal register …, 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, even if that source is unknown" (15 U.S.C. § 1127). Service marks identify services rendered or offered and distinguish them from the services rendered or offered by another, such as restaurant or retail businesses, rather than goods (15 U.S.C. § 1127). The statute requires that the "use" of the counterfeit mark be "likely to cause confusion, to cause mistake, or to deceive" (15 U.S.C. § 1114).

(U//FOUO) Congress established a federal administrative process for registering trademarks. Federal registration is a jurisdictional prerequisite for federal criminal prosecution and is an essential element in a prosecution for trademark counterfeiting. The criminal violation associated with trademarks derives directly from the protection a trademark was intended to establish: preventing counterfeiters from using trademarked "marks" in the trafficking of their counterfeit goods. The criminal violation that can be pursued to prosecute violators is trafficking in counterfeit trademark goods or services (18 U.S.C. § 2320).

4.6.4. (U//FOUO) 295E - [redacted] b7E

[redacted]

4.6.5. (U//FOUO) 334A [redacted] b7E

(U//FOUO) Classification 334A concerns matters in which an individual knowingly falsifies or conceals a material fact concerning any aircraft or spacecraft part. The parts in question can be counterfeited, refurbished, repaired, or fabricated, but in all cases, there must be a materially fraudulent misrepresentation of the part, including any writing, entry, certification, document, record data plate, or electronic communication. Most often, this violation occurs when a company manufactures, repairs, or refurbishes parts and provides a falsified certificate with the parts. The primary statute used for this classification is 18 U.S.C. § 38 (Fraud Involving Aircraft or Space Vehicle Parts in Interstate or Foreign Commerce), but false statements (18 U.S.C. § 1001), mail fraud, wire fraud, and trademark violations may also apply. The potential penalties depend largely on the nature of the part and its effect on the aircraft or space vehicle's operation. Civil forfeiture is also included in 18 U.S.C. § 38.

4.6.6. (U//FOUO) 334B [redacted] b7E

(U//FOUO) Items covered by this classification include, but are not limited to, electrical breakers, computer chips, wiring, extension cords, switches, plugs, lighting fixtures, welding units and materials, regular and ground fault interrupt (GFI) outlets, consumer entertainment electronics, and any other item which uses, transmits, or controls electrical flow, and whose failure can result in death or injury through electrocution or fire. The most commonly utilized statute is the Trafficking in Counterfeit Goods and Services statute (18 U.S.C. § 2320). Wire and mail fraud, as well as false statements, may also be applicable.

4.6.7. (U//FOUO) 334C [redacted] b7E

(U//FOUO) The items most often targeted in this classification are counterfeit automotive parts sold in the repair and non-original equipment manufacturers (OEM) markets, including brake pads/components, windshields, suspension parts, and drivetrain components. The most commonly utilized statute is the Trafficking in Counterfeit Goods and Services statute (18 U.S.C. § 2320). Wire and mail fraud, as well as false statements, may also be applicable.

4.6.8. (U//FOUO) 334D - [redacted] b7E

(U//FOUO) Goods under this classification include, but are not be limited to, pharmaceuticals, food ingredients, manufacturing equipment, personal care items, firearms and ammunition, appliances, batteries, chemicals, and building materials. The statutes used are similar to other counterfeit goods (see 334B and 334C), but they depend on the nature of the counterfeited goods.

4.7. (U//FOUO) Internet Fraud, Identity Theft, and Other Cybercrimes

(U//FOUO) The following classifications relate to crimes which rely on the use of the Internet to perpetrate frauds, thefts, and other illegal activities when the criminal activity does not include a computer intrusion.

4.7.1. (U//FOUO [redacted] b7E

[redacted] b7E

b7E

4.7.2. (U//FOUO) 196E

(U//FOUO) Internet fraud is any fraudulent scheme that uses one or more components of the Internet - such as chat rooms, e-mail, message boards, and Web sites to present false or fraudulent solicitations or representations, to conduct fraudulent transactions, or to transmit fraudulently obtained proceeds. These cybercrimes range from simple schemes to complex fraud and are online analogues of traditional crimes such as financial institution fraud, securities and commodities fraud, telemarketing fraud, money laundering, and insurance fraud, which have victimized consumers and investors for many years. These crimes not only cause harm to consumers, investors, and organizations, but also undermine consumer confidence in legitimate transactions and the Internet.

(U//FOUO) Perpetrators of Internet fraud can operate from any location that provides Internet access, and a single fraud scheme can have numerous victims spread throughout the world.

b7E

(U//FOUO) The most direct way to prove fraud is to demonstrate that the subject was unable and disinclined to fulfill the promises made to the victim.

(U//FOUO) Obtaining subscriber and connection information, or other available identity information from Internet service providers or e-businesses (electronic businesses) is often necessary in determining the identity and location of subjects. Because of the volatility of data, particularly relating to cyber matters, investigators must issue data preservation letters as soon as practicable. If a financial transaction is involved, account information or wire transfer details can provide valuable leads

b7E

4.7.3. (U//FOUO) 092U

(U//FOUO) Significant Internet frauds committed by an organized group can be investigated and prosecuted as a racketeering enterprise investigation. Although pursuit of criminal organizations

engaging in Internet fraud through the use of the Racketeer Influenced and Corrupt Organizations (RICO) Act have been rare, there are several resources that an investigator can consult when evaluating the possibility of pursuing criminal actors through the RICO statute. See *Racketeer Influenced and Corrupt Organizations (RICO): A Manual for Federal Prosecutors* (DOJ Organized Crime and Racketeering Section (OCRS)), which is available on the [redacted] It is critical that any consideration of pursuing a RICO investigation be closely coordinated with CyD. Specific procedures regarding the conduct of enterprise investigations, including RICO, are located in section 8 of the DIOG. b7E

4.7.4. (U//FOUO) 253E - [redacted]

(U//FOUO) Investigations of criminal activity involving identity theft with a substantial Internet connection may also involve other cybercrime violations or criminal computer intrusions. In those instances, investigations will be pursued with the goal of disrupting the threat to the information infrastructure, rather than the fraudulent activity relating to identity theft.

(U//FOUO) The statute criminalizing activity in the 253E classification is the Fraud and Related Activity In Connection With Identification Documents (FRAID) statute, 18 U.S.C. § 1028. The DOJ-CCIPS has developed investigative and prosecution guidance to assist with identity theft investigations. CCIPS released the *Identity Theft and Social Security Fraud Manual* to assist investigators with understanding the legal and evidentiary requirements for conducting identity theft investigations. b7E

4.7.5. (U//FOUO) 258C - [redacted]

(U//FOUO) Investigations of criminal activity involving credit/debit card fraud with a substantial Internet connection may also involve cybercrime violations or criminal computer intrusions. These investigations are pursued with the goal of disrupting the threat to the information infrastructure rather than the fraudulent activity relating to identity theft.

(U//FOUO) The statute criminalizing activity in the 258C classification is the Fraud and Related Activity In Connection With Access Devices statute, 18 U.S.C. § 1029.

4.7.6. (U//FOUO) 316A [redacted] b7E

(U//FOUO) Many subjects use the Internet to extort money, power, and status over their victims. Utilizing the Internet allows the subjects to quickly direct the extortion attempt. Subjects can more efficiently initiate and coordinate their schemes from overseas by threatening individuals and/or companies for monetary gain and requesting the funds be wired into overseas bank accounts. These extortion threats can also be run more efficiently over the Internet between regions, states, or even locally. Significant, threatening e-mail messages and other significant Internet or online threats, without extortion demands, must also be worked under this classification.

(U//FOUO) In many computer intrusion cases, the leverage used by the subjects is the loss of control by the victims, and the threat of remote damage by the subjects compels the victims to comply with the extortionate demands. In these cases, an investigation will be pursued as a 288 matter with a focus on disrupting the threat to the information infrastructure, as opposed to as a 316A - [redacted]

4.7.7. (U//FOUO) 316B [redacted] b7E

(U//FOUO) Internet gambling and advertising for other illegal activities have rapidly increased since 2002. Overseas gambling sites have opened whereby money is placed into online accounts, and individuals may increase the monetary amount in their account through credit cards. Sports betting is now available around the world through the Internet. Advertisements for Internet gambling have proliferated through various sites such as PayPal, eBay, and the like. If there is a nexus to organized crime or a criminal enterprise, contact the appropriate CyD program manager for coordination with the Criminal Investigative Division (CID).

4.7.8. (U//FOUO) 316C - [redacted]

(U//FOUO) Financial transactions utilizing the Internet typically involve cyber payments, digital currency, e-money (electronic money), or similar means to facilitate the transfer of financial value. These means provide the transacting parties with an immediate, convenient, secure, and potentially anonymous means by which to transfer financial value. Although these means provide benefits for legitimate commerce, they also can be used to facilitate the transfer of illicit funds.

4.7.9. (U//FOUO) 316D - [redacted]

(U//FOUO) Modern purveyors of pornography utilize the Internet to advertise, distribute, and receive payment for their services and products. Adult obscenity is often depicted and described on Web sites that offer still images or video or facilitate the mailing of movies on video tapes or DVDs (digital video discs). These Web sites are easily located and provide services to any users who describe themselves as being at least 18 years old. Although images of adult pornography are not legally declared obscene until deemed so by a judge or jury based on community standards, certain recordkeeping requirements are mandated for all sexually explicit material that is distributed. Any sexually explicit material, legal or otherwise, cannot be knowingly distributed to minors under the age of 16. In addition, records must be maintained by producers of such material as proof that all actors in the production are at least 18 years old. The material, whether on video tape, DVD, or on Web site, must identify the custodian of records regarding the production of the material and must include a physical address of that custodian.

(U//FOUO) For material to be deemed obscene, it must be presented to a jury or judge who must decide whether the average person, applying contemporary community standards, would determine that the work, taken as a whole: (1) appeals to a prurient interest in sex; (2) depicts or describes sexual conduct in a patently offensive way; and (3) lacks serious literary, artistic, political, or scientific value. As a result, searches or other investigative methods employed in adult obscenity matters must be sensitive to the First Amendment protections afforded all such material prior to it being deemed obscene. In addition, a person's right to possess obscene material in his or her home, for his or her own personal use, has been upheld by the Supreme Court.

4.8. (U//FOUO) 314 - [redacted] b7E

(U//FOUO) The 314 classification is used for operational and administrative matters associated with the InfraGard® Program. This program is not mandated by any U.S. laws. Additional information regarding the InfraGard® Program and guidance regarding querying InfraGard® Program resources is located in Sections 4.9.4 and 6.2.1.4 of this PG and in the *InfraGard® Policy Implementation Guide*, CyDPG Appendix C.

4.9. (U) CyD Strategic Outreach and Initiatives

(U) CyD has many outreach and initiatives resources that advance various CyD missions and provide investigative support, including:

4.9.1. (U) IC3

(U) As a partner in the IC3, the FBI maintains a unit containing a number of ICSs and other personnel at the IC3 facility in West Virginia. While the FBI is a full partner in the IC3, the [redacted] is the designated owner of the data contained within the IC3 database. b7E

(U) IC3 does not conduct predicated investigations; rather, they obtain and disseminate information (as appropriate) from the IC3 database, conduct assessments of Internet crime complaints, and provide investigative assistance and access to the resources of the [redacted] and IC3 database and to the resources of other partner agencies and private entities. Since any interaction with the IC3 database or with any of the other partners by IC3 entails interaction with members of public and private entities, FBI personnel must ensure that any such interactions must be within the scope of a current assessment or predicated investigation.

4.9.1.1. (U) IC3 Investigative Procedures and Processes

(U) IC3 FBI personnel are reminded to follow the requirements in and obtain authorizations associated with the FBI's domestic investigative methods as identified in the DIOG. Many of the activities that are central to IC3's mission involve activities that can only be conducted pursuant to an authorized assessment or predicated investigation. While this can often be accomplished derivatively through the ongoing field investigation to which the investigation pertains, IC3 may also initiate an assessment (as authorized in the DIOG), as necessary, to accomplish investigative objectives and facilitate the exchange and development of information with IC3 partners and contacts.

4.9.1.2. (U) Authorized Investigative Methods in IC3 Assessments

b7E

- [redacted]

Note: See DIOG for applicable guidance regarding these methods.

4.9.1.3. (U) Field Office Requests to the IC3

b7E

(U) Field office requests to the IC3 must be transmitted using an EC, by e-mail to [redacted] or by telephone. An FBI EC may also be used to memorialize a request after the initial contact with IC3 to ensure that the request is made in a timely fashion.

(U) The IC3 can query the field office's request through the IC3 complaint database [redacted] b7E
[redacted] Responses are forwarded to field offices and appropriate FBIHQ operational units via EC.

4.9.2. (U) CIRFU

[redacted] b7E

[redacted] b7E

[redacted] b7E

4.9.2.1. (U) CIRFU Core Activities

- [redacted] b7E

4.9.2.2. (U) CIRFU Interface with NCFTA

[redacted] b7E

b7E

4.9.2.3. **(U) Field Office Requests to CIRFU**

b7E

4.9.3. (U) IINI

(U) The IINI is an intelligence-driven, proactive, multi-agency investigative initiative to combat the proliferation of child pornography/child sexual exploitation facilitated by online computers.

b7E

(U) The objective of the IINI is to reduce the vulnerability of children to acts of sexual exploitation and abuse that are facilitated through the use of computers; to support divisions in their efforts to identify and rescue child victims; to support divisions in their efforts to investigate and prosecute sexual predators who use the Internet and other online services to sexually exploit children for personal or financial gain; and to strengthen the capabilities of federal, state, local, law enforcement through programs and investigative assistance. The classification was created to consolidate all investigations of child pornography and sexual exploitation of children facilitated by the use of online computers. The IINI is an FBIHQ-led initiative, and the CyD provides program management functions for field office investigations within the initiative, as well as an investigative component.

b7E

(U) Information for investigators regarding querying IINI resources and contacts is located in Section 6.2.1.3 of this PG. Operational policy and guidance for investigations falling within the IINI Program are documented in the CyDPG Appendix B.

4.9.3.1. **(U**

b7E

[redacted] b7E

4.9.3.2. **(U) National Center for Missing & Exploited Children (NCMEC)**

(U) The NCMEC is a private, nonprofit organization established in 1984 in Alexandria, Virginia, that operates under a Congressional mandate and works in cooperation with the DOJ's Office of Juvenile Justice and Delinquency Prevention (OJJDP). As the nation's resource center for child protection, NCMEC spearheads national efforts to locate and recover missing children and raises public awareness about ways to prevent child abduction, molestation, sexual exploitation, and the victimization of children by coordinating the efforts of law enforcement, social service agencies, elected officials, judges, prosecutors, educators, and the public and private sectors.

(U) [redacted] b7E

[redacted]

4.9.4. (U) The InfraGard® Program

(U) The InfraGard® Program was created by the FBI to support the nation's critical infrastructure by promoting ongoing dialogue and timely communication between all stakeholders regarding critical infrastructure protection. The mission of the InfraGard® Program is to support an information-sharing partnership between members from private, local, state, federal, and international entities for the purpose of protecting the nation's critical infrastructures against attack or failure caused by either foreign or domestic threats and to support all FBI investigative programs, including the Counterterrorism (CTD) Program, the Counterintelligence (CD) Program, the Criminal Program, and the Cybercrime Program. The InfraGard® Program is not mandated by any U.S. laws.

(U) The InfraGard® Program provides assistance to the field by providing access to individual InfraGard® Program members or through canvasses of the InfraGard® Program membership, which can only be conducted within the scope of a current assessment or predicated investigation.

[redacted] b7E

(U) Information for investigators regarding canvassing InfraGard® Program membership and contacts for information is located in Section 6.2.1.4 of this PG. Policy and guidance regarding the InfraGard® Program field office coordinators are documented in the *InfraGard® Policy Implementation Guide*, CyDPG Appendix C.

4.9.5. [redacted] b7E

[redacted] b7E

[redacted] b7E

4.9.6. [redacted] b7E

[redacted] b7E

[redacted] b7E

4.9.7. (U) Cyber Task Forces

(U) There are more than 50 cyber task forces throughout FBI field offices. A cyber task force is defined as two or more agencies that agree to work together to primarily address cybercrimes. There must be a memorandum of understanding (MOU) or memorandum of agreement (MOA) in place for a group to be considered a task force. If there is no MOU or MOA in place, the organization is considered to be a working group. Task forces work FBI cyber investigations consistent with program priorities, as established by the CyD. Through the Asset Forfeiture Program, only full-time officers receive overtime funding, leased vehicles/gas, cyber training, and BlackBerry® cellular phones.

(U) Information regarding the task force program can be found on the FBI Intranet site under Cyber Criminal Unit Three (CCU-3).

4.10. (U) CyD Investigator Education and Development Requirements

(U) The Cyber Education and Development Unit (CEDU) identifies, develops, and delivers core and continuing education and training for cyber investigators. The Cyber Special Agent Career Path Developmental Plan sets forth required and elective training courses and experiential milestones for each stage of the career path. The plan assures the development and continuing education of cyber investigators and may be reviewed at any time on the CEDU Intranet SharePoint site.

4.10.1. (U) Core Curriculum

(U) CEDU has developed a series of courses considered to be "core" training. These core courses are required for all special agents assigned to the cyber career path and are intended to provide investigators with the skill set needed to successfully work cases in support of the priorities of the CyD. The core training sequence includes basic, intermediate, and advanced training requirements, along with required developmental activities and is taken on a timetable established by the division in the Cyber Special Agent Career Path Developmental Plan. Meeting the multiyear timetable can be challenging and requires a commitment by agents and by field management to ensure successful completion.

4.10.2. (U) Elective Curriculum

(U) The core courses are complimented by a number of elective courses and recommended developmental activities that allow investigators to explore and develop expertise with specific operating systems and technologies. These courses are also directed toward specific cyber investigative programs, including computer intrusions, online child exploitation, intellectual property rights violations, and Internet fraud. Elective courses are offered at various levels and each course has established attendance prerequisites.

4.10.3. (U) "Test-out" Options for Investigators with Technical Expertise

(U) The majority of training classes offered by CEDU are technical in nature. Recognizing that CyD personnel bring varying levels of technical expertise with them into the FBI, CEDU has developed test-out options for personnel who already possess significant technical skills. These personnel may avail themselves of the test-out options in order to meet the prerequisites of more advanced and challenging coursework.

4.11. (U//FOUO) Liaison to Other Federal Agencies - The Department of Homeland Security (DHS)/United States Computer Emergency Readiness Team (US-CERT), the Central Intelligence Agency (CIA), and the National Security Agency (NSA)

	b7E
	b7E

b7E

4.12. (U//FOUO) Regional Cyber Action Team (RCAT)

b7E

4.12.1. (U//FOUO) RCAT Team Composition and Capabilities

b7E

b7E

4.12.2. (U//FOUO) Requesting RCAT Assistance

b7E

4.12.3. (U//FOUO) Approval for RCAT Deployment

b7E

b7E

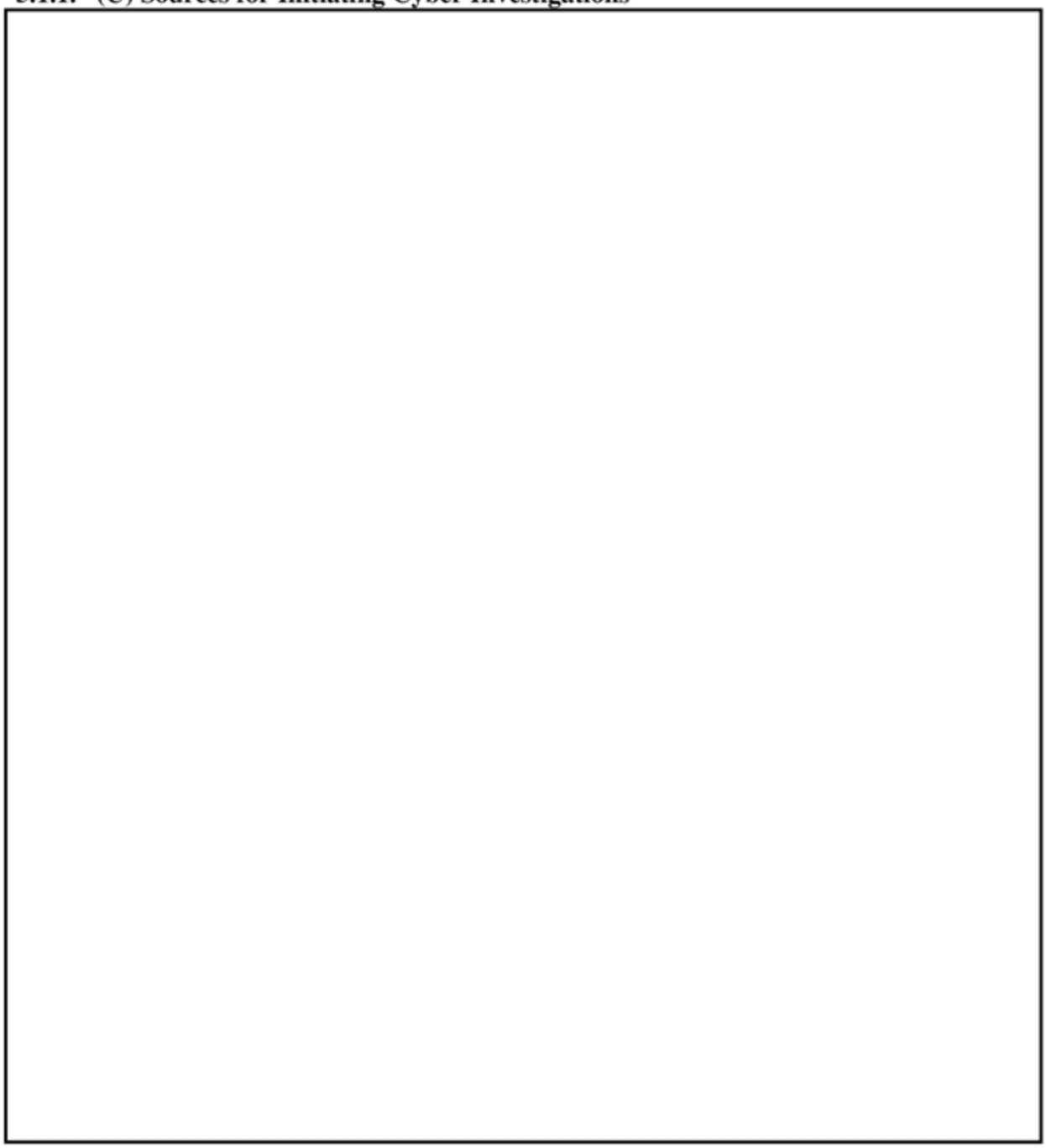
5. (U) Investigative Procedures and Processes

5.1. (U) Authorized Investigative Activity

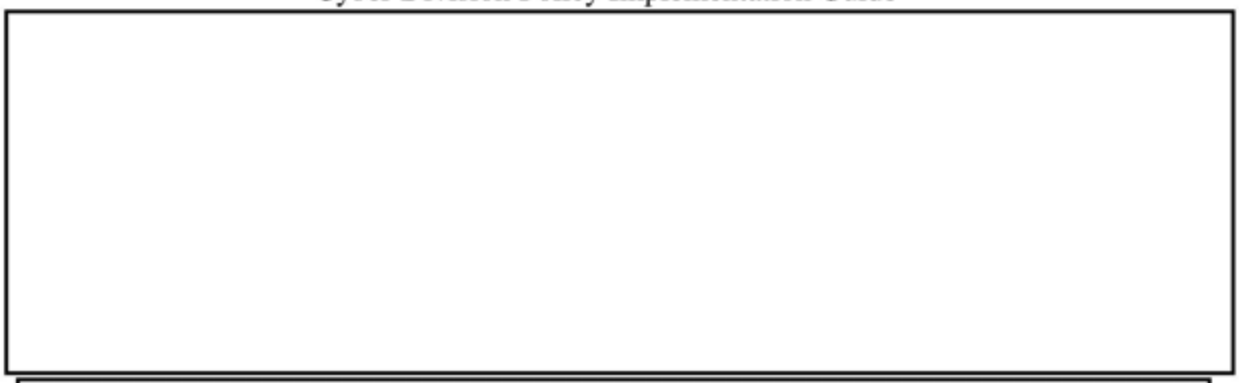
(U) Investigations and operations conducted in furtherance of Cyber Program classifications must use the full authorities and methods implemented in the DIOG, subject only to the limitations and qualifications set forth below.

5.1.1. (U) Sources for Initiating Cyber Investigations

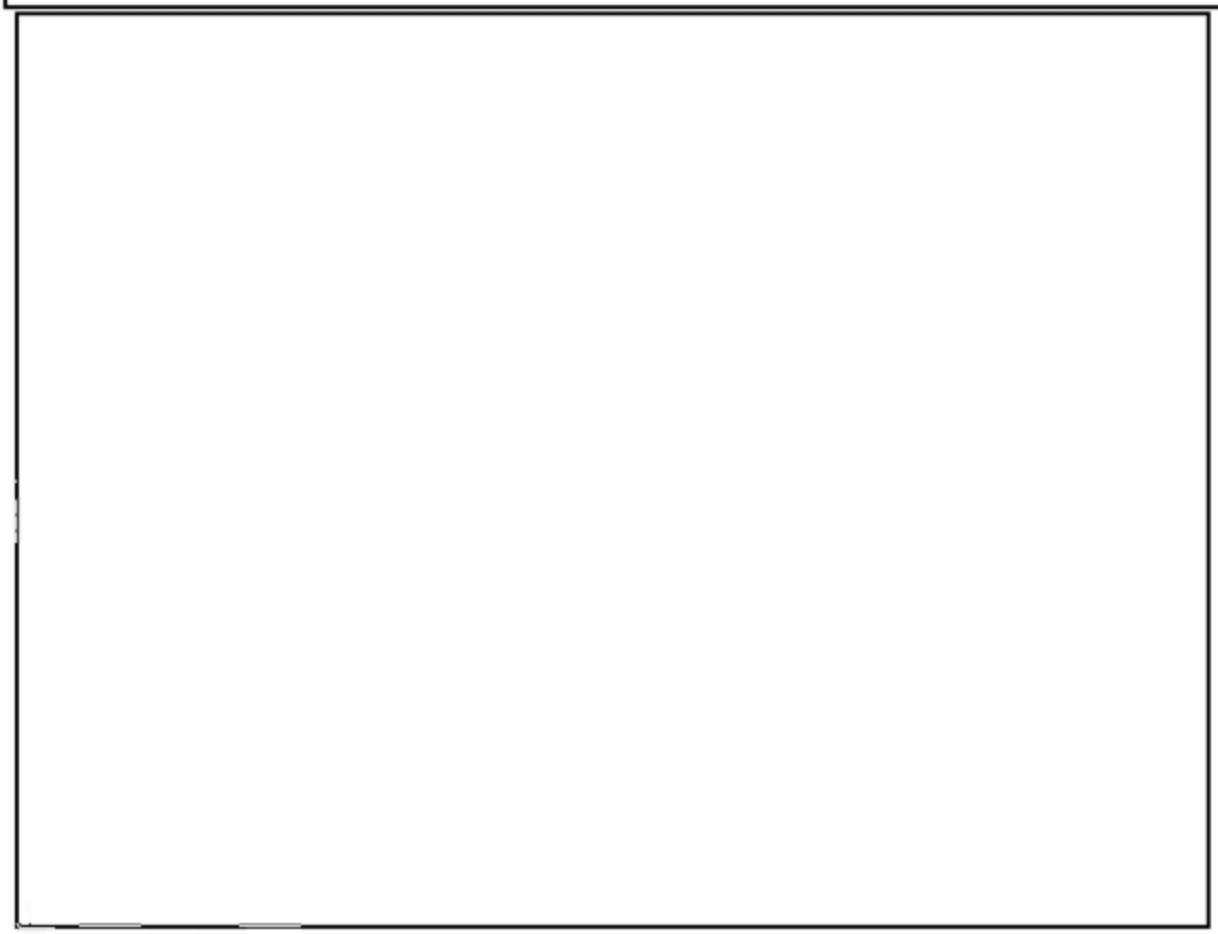
b7E



b7E



b7E



5.2. (U) Documentation

(U) The DIOG sets forth general documentation and notification requirements associated with authorization and execution of investigative and operational activities. Investigative activities within the scope of this PG must comply with all documentation and notification requirements set forth in the DIOG, as well as with any additional documentation and notification set forth in this PG.

5.3. (U) Victim Notification in Computer Intrusion Matters

(U) The CyD's top priority is the protection of our national security, economy, and information infrastructure from intrusions, malicious code, and nefarious computer network operations. This includes the sharing of investigative information with intrusion

victims and the computer network defense (CND) community to protect compromised systems, mitigate economic loss and damage, and prevent future attacks. Victim notification is a compelling way for the CyD to contribute to network defense for the protection of individual, commercial, and government users of the Internet, as well as for the protection of the infrastructure itself. It is the policy of the CyD to notify and disseminate meaningful information to victims and the CND community in a timely manner to the extent it does not interfere with ongoing law enforcement or U.S. Intelligence Community (USIC) investigations, operations, methods, sources, or technologies.

(U//FOUO) Cyber victims are generally individuals or organizations subjected to cyberbased operations, including computer network attack (CNA) and computer network exploitation (CNE) in furtherance of criminal activity or threats to the national security. These CNA/CNE operations often result in the compromise of electronic systems, resulting in the alteration, loss, exfiltration, or denial of access to data that the victim maintains or controls. Victims may be identified, to the extent possible, by the FBI or its partner agencies in the course of investigative activities of suspected cybercrimes and cyber-related threats.

b7E

(U//FOUO) Because timely victim notification has the potential to completely mitigate ongoing and future intrusions and can mitigate the damage of past attacks while increasing the potential for the collection of actionable intelligence, the CyD's policy regarding victim notification is designed to strongly favor victim notification. Even when it may interfere with another investigation or USIC operation, notification should still be considered in coordination with the operational stakeholders when the equities of victim notification will serve to protect U.S. persons or a national infrastructure or other U.S. interests from significant harm.

5.3.1. (U) Victim Notification Test

(U//FOUO) The Attorney General (AG) has issued guidelines that create a mandatory victim notification paradigm which requires, under certain circumstances, that federal investigators and prosecutors identify victims of crime, and, among other things, notify them, except where such notification would interfere with an ongoing investigation (*Attorney General Guidelines for Victim and Witness Assistance*, Article IV, Section A).

b7E

(U//FOUO) To ensure decisions relating to providing notice to a victim in a cyber investigation are consistent, the following analysis must be conducted prior to providing notice to a victim:

b7E

b7E

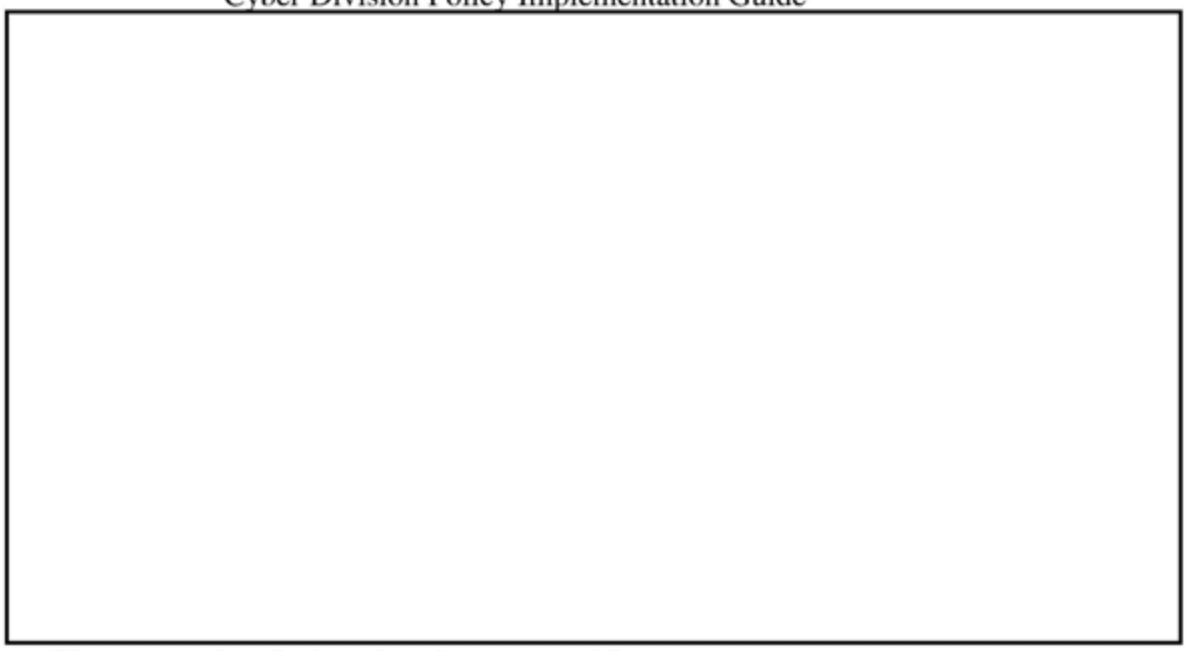
2.

b7E

3.

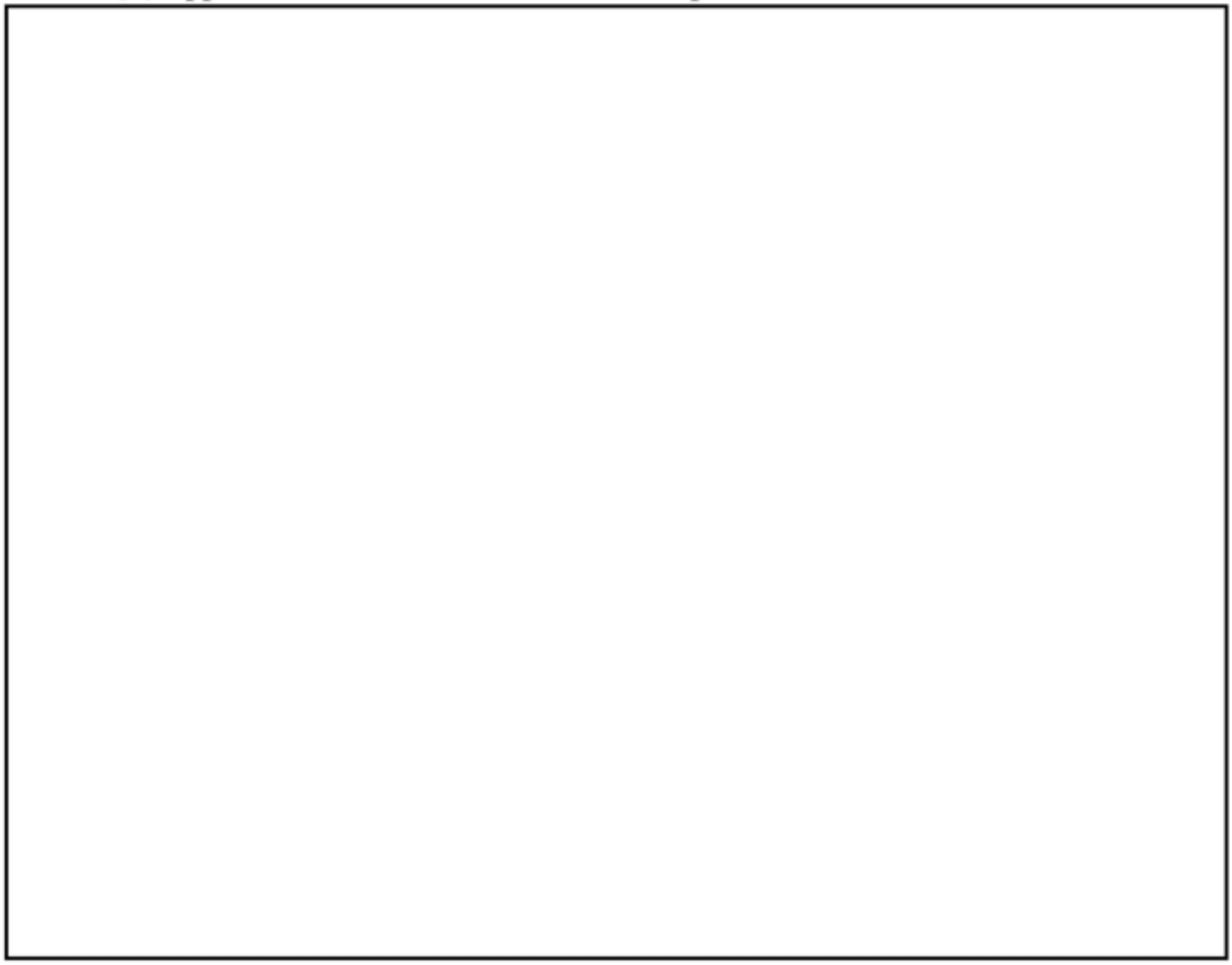
b7E

b7E



5.3.2. (U) Approval or Deferral and Associated Requirements

b7E



b7E

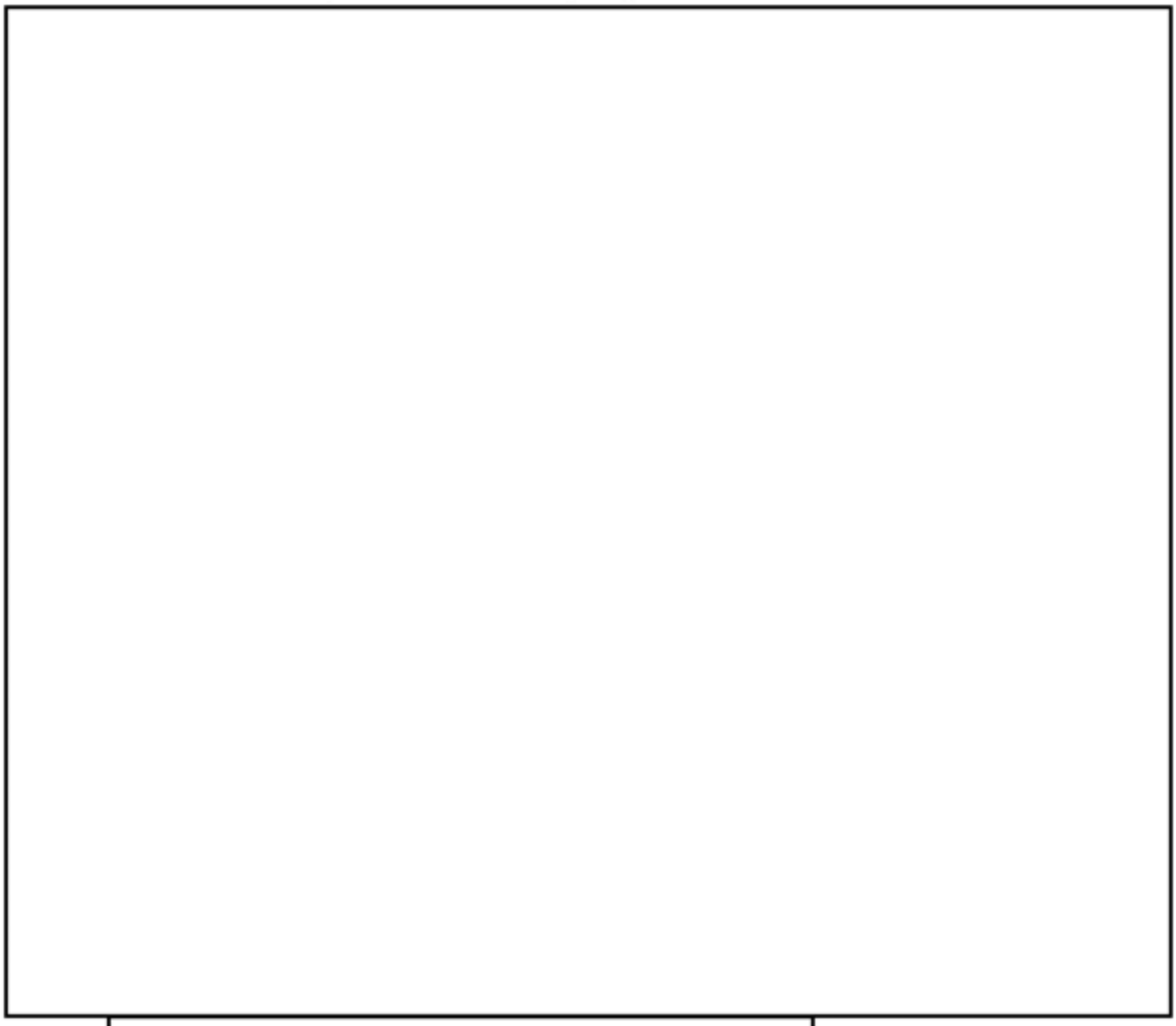
5.3.3. (U) Timing of Notification

b7E

5.3.4. (U) Method of Notification

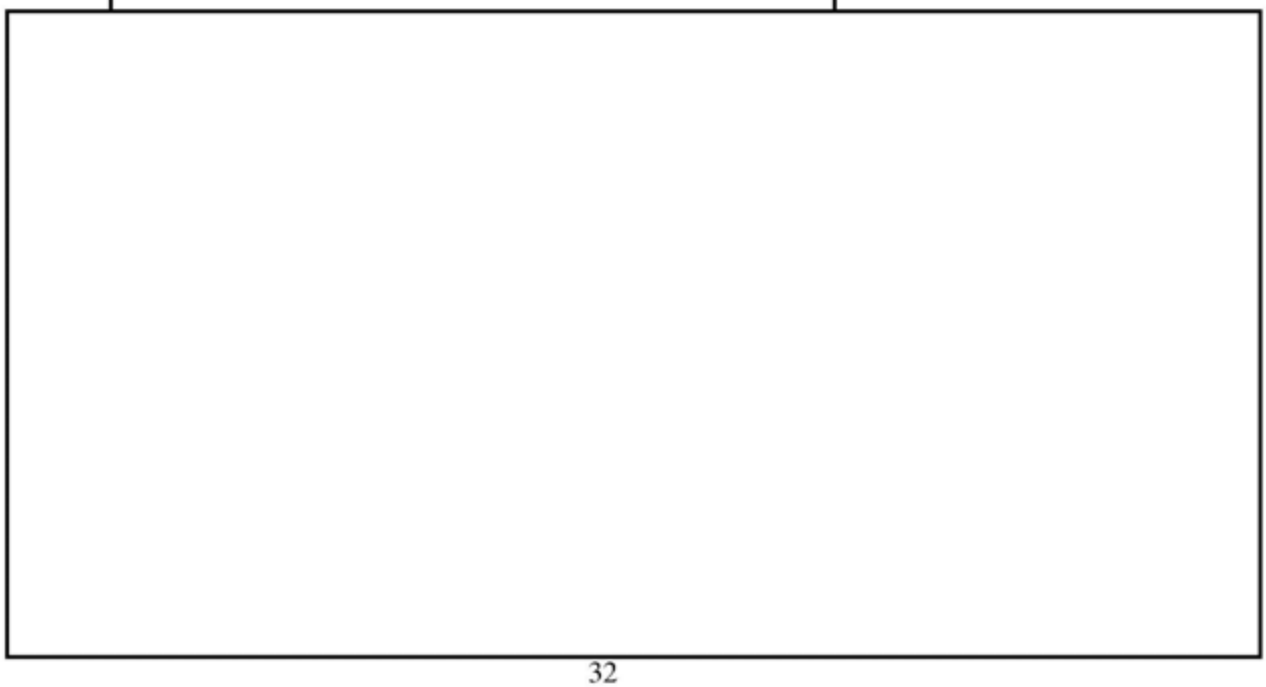
b7E

b7E



5.3.5.

b7E



[redacted] b7E

5.4. (U) Initiation of Assessments

[redacted] b7E

5.5. (U) Initiation of Predicated Investigations

[redacted] b7E

5.5.1. (U) FBIHQ Notification Requirements for Criminal Cyber Subprograms

[redacted] b7E

5.5.2. (U//FOUO) Coordination Requirements

(U//FOUO) Whenever there may be overlap between a cyber investigation and other operational divisions (e.g., CTD, CD, or CID), the investigator must notify the field office operational squad with whom there is overlap and the respective CyD program manager. The program manager can assist in coordinating with the appropriate division as needed. These cases will generally be resolved by one squad taking the lead, or they may be jointly worked with dual caption requirements.

(U//FOUO) Refer to Appendix A for coordination requirements in international terrorism and counterintelligence matters, and below for domestic terrorism matters.

5.5.3. (U//FOUO) Domestic Terrorism Notification and Coordination Requirements

(U//FOUO) For computer intrusion cases where the facts or circumstances surrounding the intrusion incident suggest that the intrusion may have been in furtherance of a domestic political or social change, the investigator must coordinate with the domestic terrorism squad in his or her field office and the Counterterrorism Division, Domestic Terrorism Operations Unit (DTOU), following these guidelines:

- [redacted] b7E

b7E

-
-

5.5.4. (U//FOUO) Sensitive Investigative Matter (SIM) Notification Requirements

b7E

b7E

5.5.5.

b7E

5.5.5.1.

b7E

5.5.5.2.

b7E

5.5.6. (U) Office of Origin (OO) Determination

(U) The office of origin in any given investigation is usually determined by the residence, location, or destination of the subject of the investigation. With prior CyD concurrence, origin may be assumed by the field office that can establish venue. The OO is often in the same location as a victim or a compromised computer or network device controlled or used by the subject. In some circumstances, CyD identifies overlapping investigations being conducted by multiple field offices and consolidates these cases into a combined case, with the OO determined by CyD. In all circumstances, final determination of the OO for cyber investigations is made by CyD.

(U) No office may conduct any investigation that could reasonably be expected to impact the OO of any investigation, without prior coordination with CyD.

(U) With the concurrence of the OO, a field office with current investigative interest in a subject may initiate investigative methods, as deemed appropriate, without opening a separate investigation.

(U) In certain circumstances, parallel full investigations may be run by separate OOs with CyD approval. Individual offices are responsible for adhering to the applicable requirements throughout the AGG-Dom, the DIOG, and this PG. In furtherance of mutual or national investigative objectives, individual offices must ensure successful investigative coordination with CyD program managers and any other field offices that may be involved.

5.5.7. (U) Investigative Methods

b7E

5.5.8. (U) Notice Regarding Significant Investigative Events

(U) Notice of major investigative events (e.g., indictments, arrests, convictions, and significant operations) must be provided to the appropriate CyD program manager by the case agent through an EC or an email submitted to the investigative case file, regardless of other reporting requirements.

5.5.9. (U) Legats

b7E

[redacted]

5.6. (U) Preliminary Investigation Extensions

(U//FOUO) It is the responsibility of the OO to advise lead offices and obtain necessary extensions (in compliance with the DIOG). Lead offices must cease investigation upon expiration of the authorized period until advised by the OO of an extension. When an extension is granted, the date must be noted on subsequent file communications as well as the revised date of the PI's expiration.

5.7. (U) Evidence Procedures

b7E

[redacted]

5.8. (U) United States Attorney's Office

(U) The USAO must be consulted on criminal cases to determine prosecution viability. For guidance in counterterrorism and counterintelligence cases, see Appendix A. Legal guidance and verification of compliance with respective federal district standards must be ascertained by the investigating agent. AUSAs will evaluate cases and coordinate prosecution with respective divisions. Each USAO has, at a minimum, a computer hacking and intellectual property (CHIP) attorney or a CHIP unit with several AUSAs coordinating the prosecution of cybercrime and criminal intrusion efforts. The USAO may further coordinate investigations and prosecutions with the DOJ CCIPS when appropriate.

5.9. (U) Retention and Sharing of Information

(U) All agents and managers must ensure compliance with the DIOG regarding guidance on retaining and sharing information collected during an investigation. However, as is articulated in the DIOG, when the FBI collects information relating to the exercise of a First Amendment right, or related to rights pursuant to the Equal Protection Clause, the FBI may only collect and retain that information so long as it is associated with an authorized law enforcement purpose.

5.10. (U) Closing Predicated Investigations

(U) Upon conclusion of a predicated investigation, a closing EC drafted by the investigating field office must be submitted to the appropriate CyD program manager. The closing communication and notifications must be in accord with the DIOG, including notification to the CyD program manager associated with the investigation.

6. (U) Investigative Methods in Cyber Matters

b7E

6.1. (U) Least Intrusive Method, Protection of Civil Liberties, and Privacy Rights

(U) Cyber investigators must adhere to the principle requiring that the "least intrusive" method that will achieve the investigative objective be employed to protect civil liberties and privacy rights. This principle is described in full in the DIOG. As set forth extensively in the DIOG, investigators must utilize the least intrusive, most efficient methods, but not be inhibited from prudently using any authorized investigative method to address the criminal activity and eliminate the threat. Cyber investigators should utilize methods with the intention of expeditiously moving from network-based investigation to attribution of the activity and the identification and investigation of the individual(s) executing the cyber criminal activity.

6.2. (U) Authorized Investigative Methods in Assessments and Predicated Investigations

(U) The CyD encourages investigators to avail themselves of the full spectrum of methods authorized by the DIOG. In addition to the guidance and requirements set forth in the DIOG, CyD offers the following qualifications:

6.2.1. (U) Querying Strategic Outreach and Initiative Resources

b7E

6.2.1.1. (U

b7E

6.2.1.2. (U

b7E

6.2.1.3. (U

b7E

6.2.1.4. (U

b7E

6.2.1.5. (U) b7E

6.2.1.6. (U) b7E

6.2.2. (U) b7E

6.2.3. (U) Obtaining Publicly Available Information

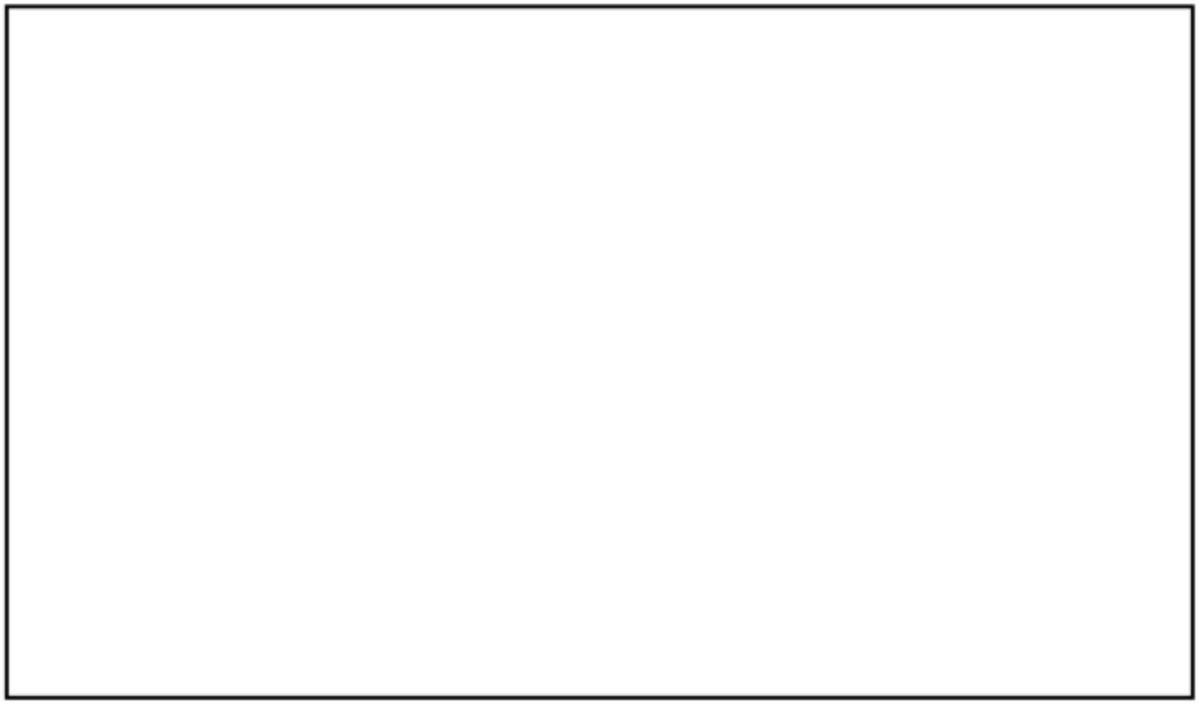
(U) Investigators may obtain information from publicly accessible online sources and facilities under the same conditions as they obtain information from other sources generally open to the public. b7E

(U) Individuals do not have a reasonable expectation of privacy on personal information that is generally made publicly available by themselves or by others (such as publicly available Internet telephone directories); therefore, obtaining information from online facilities configured for unrestricted public access is a minimally intrusive law enforcement activity.

(U) However, as is articulated in the DIOG, when the FBI collects information relating to the exercise of a First Amendment right or related to rights pursuant to the Equal Protection Clause, the FBI may only collect and retain that information so long as it is associated with an authorized law enforcement purpose.

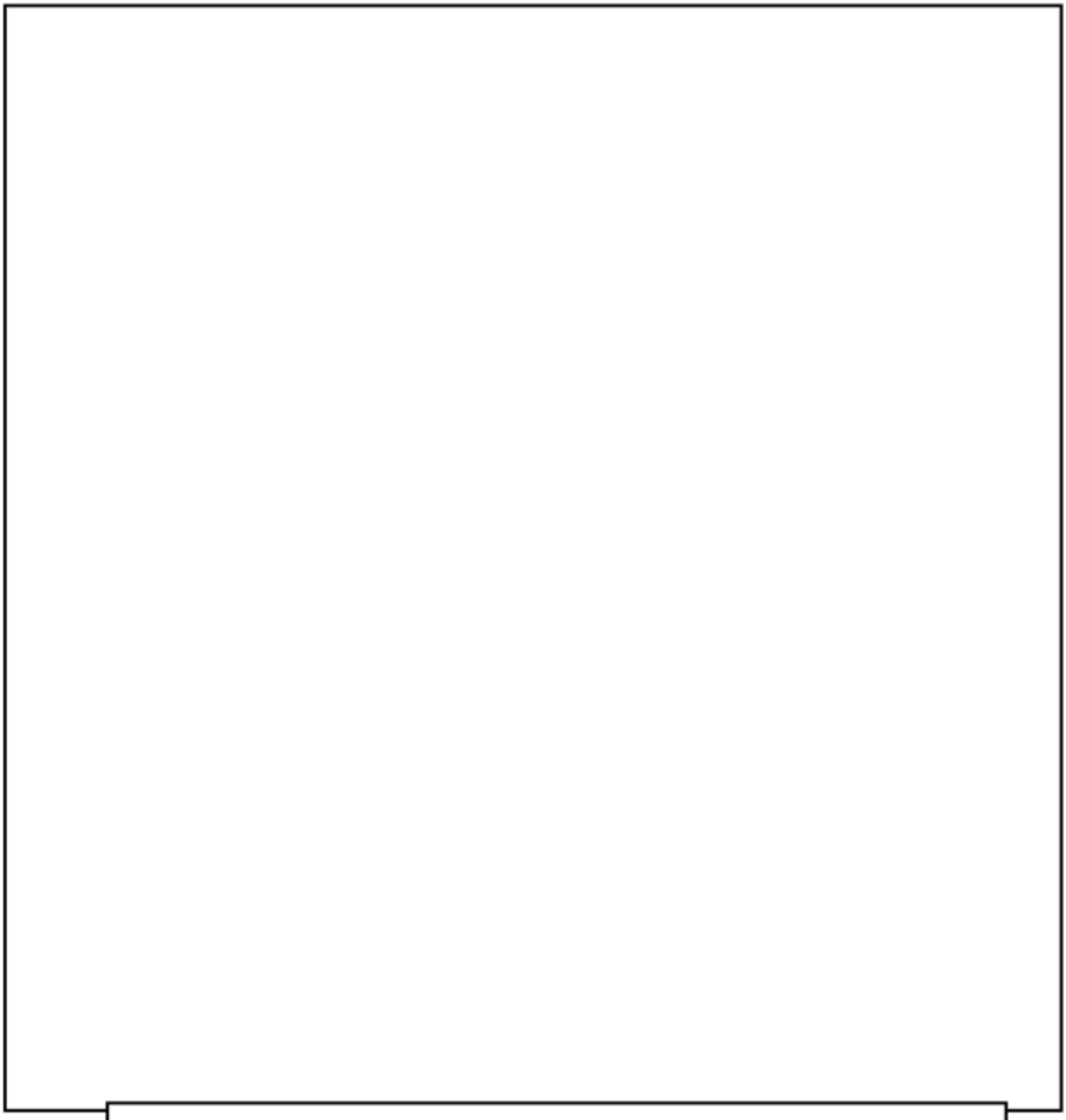
b7E

6.2.4. (U) Attend and Obtain Online Real Time Public Communications

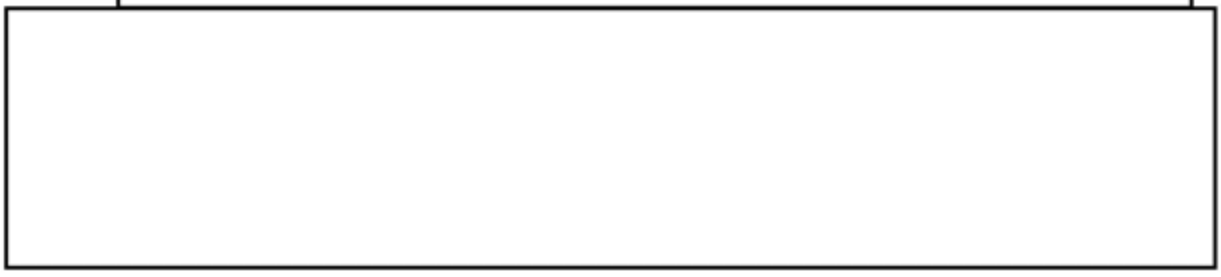


b7E

b7E



6.2.5. b7E



b7E

b7E

b7E

6.2.7. (U) Online Activity on Personal Time

(U) While not on duty, an investigator is free to engage in personal online pursuits. If, however, an investigator's off duty online activities are undertaken for the purpose of developing investigative leads, an investigator is bound by the same investigative conduct restrictions as would apply when that investigator is on duty, regardless of whether or not an investigative activity is occurring during working hours or from a workplace.

6.3. (U) Mail Covers

b7E

6.4. (U) Trash Covers

b7E

(U//FOUO) CyD investigations may use trash covers in accordance with the policy set forth in the DIOG.

6.5. (U) Monitoring of Electronic Communications

(U) In addition to the policy and requirements set forth in the DIOG, CyD offers the following guidance.

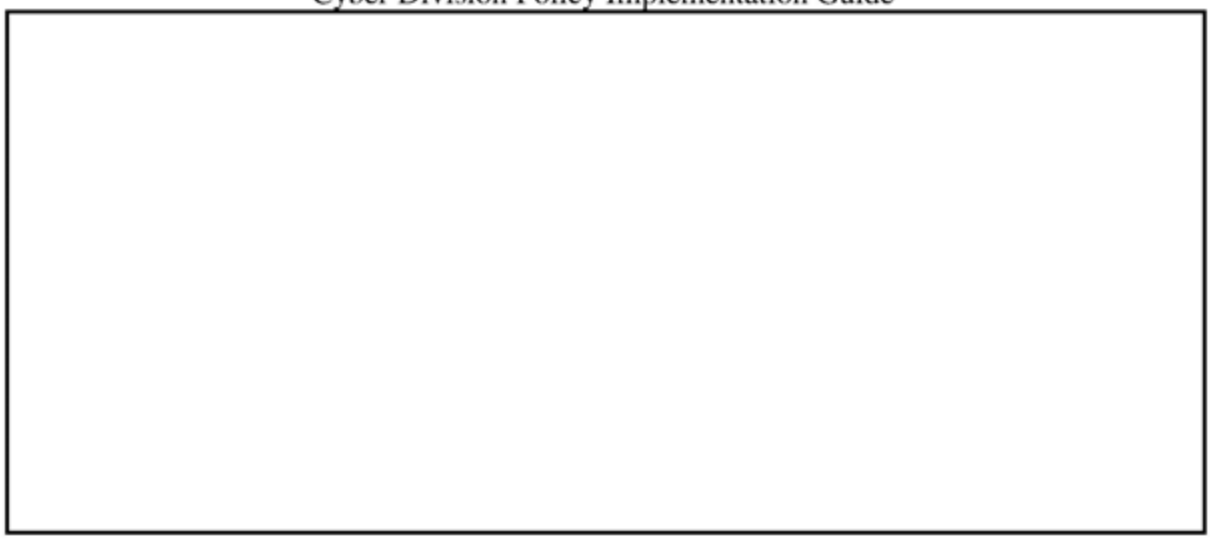
6.5.1.

b7E

6.5.2. (U) Consensual Computer Monitoring

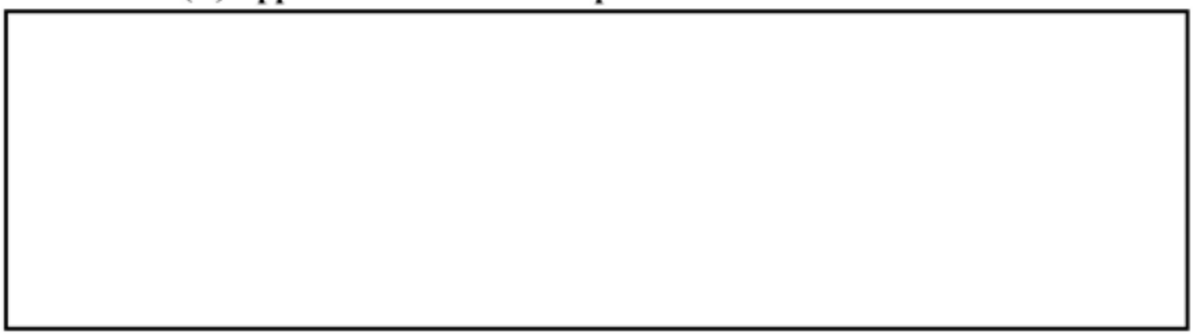
b7E

b7E



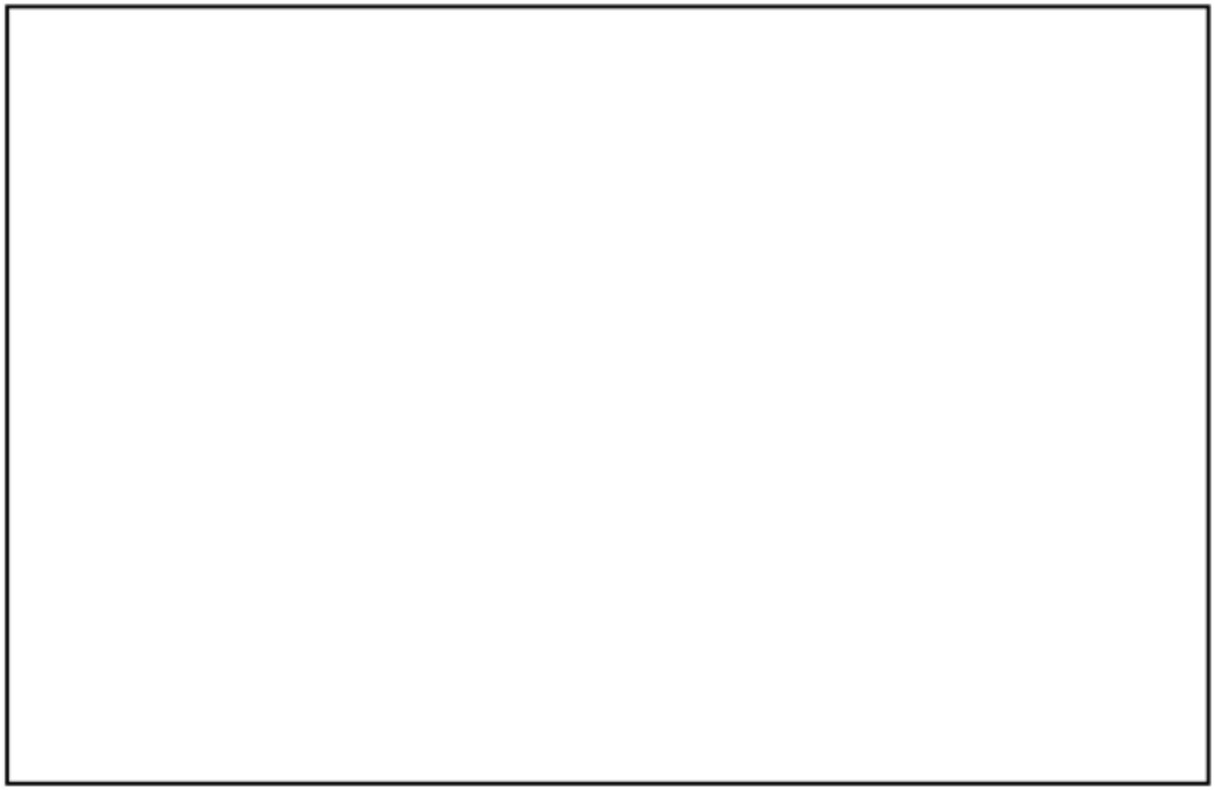
b7E

6.5.2.1. **(U) Approval to Monitor Computer Communications**



b7E

6.5.2.2. **(U) Documenting Consent to Monitor Computer Communications**



b7E

b7E

6.5.2.3. (U) Consent and Warning Banners

b7E

[redacted]

b7E

6.5.3. (U) [redacted]

[redacted]

b7E

6.5.3.1. **(U)** [redacted]

[redacted]

b7E

b7E

b7E

b7E

b7E

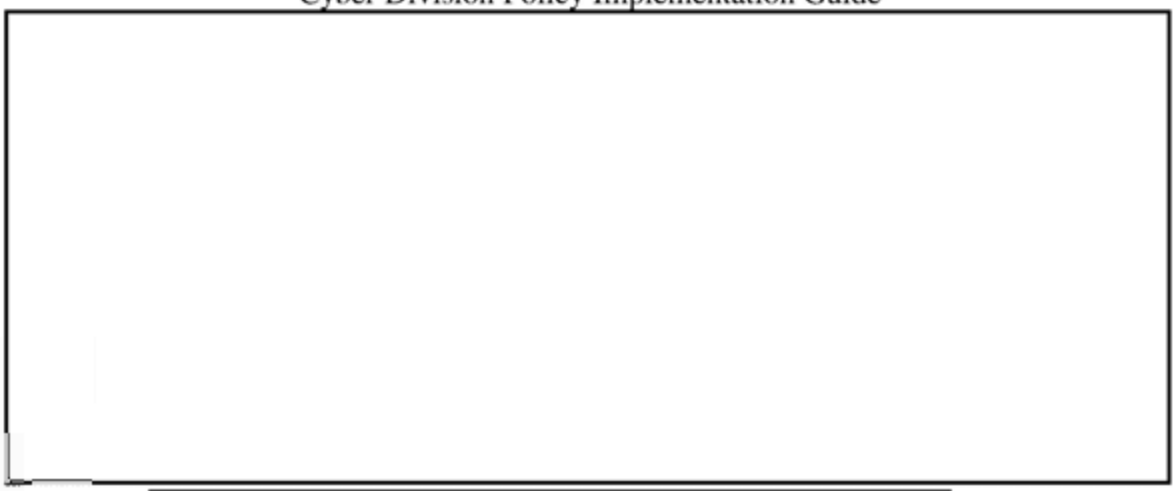
[redacted]

b7E

6.5.4. (U) Use of Surveillance Authorities Concurrently

[redacted]

b7E



6.6. (U

b7E

6.7. (U) Polygraph

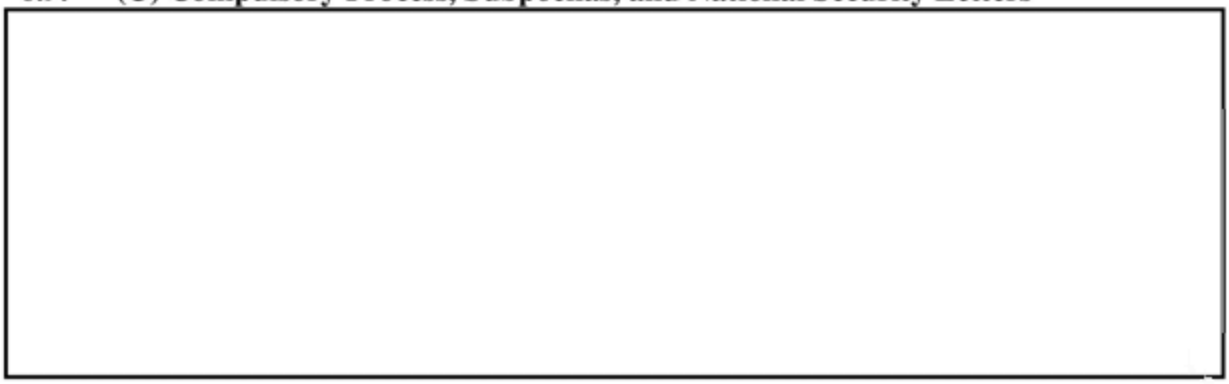
(U) CyD investigators may use polygraphs in accordance with the policy set forth in the DIOG.

6.8. (U

b7E

6.9. (U) Compulsory Process, Subpoenas, and National Security Letters

b7E



6.9.1. (U) Limitations of Federal Grand Jury Subpoenas

(U) FGJ subpoenas are typically used in criminal computer investigations to obtain

b7E

A major limitation associated with FGJ subpoenas is Rule 6(e) of the Federal Rules of Criminal Procedure (FRCP), which restricts access to the results to the personnel on the Grand Jury 6(e) list maintained by the USAO.

6.9.2. (U) Administrative Subpoenas

(U//FOUO) Agents investigating child pornography and sexual exploitation over the Internet (i.e., 305 investigative matters) have been granted the authority to use administrative subpoenas with proper approval (see 18 U.S.C. § 3486 and the DIOG). This authority does not extend to other cyber matters. The records that may be obtained via administrative subpoena in 305 matters are limited to basic subscriber and customer information that is otherwise subject to ECPA. Additional information regarding the use of administrative subpoenas is discussed in CyDPG, Appendix B.

6.9.3. (U)

b7E

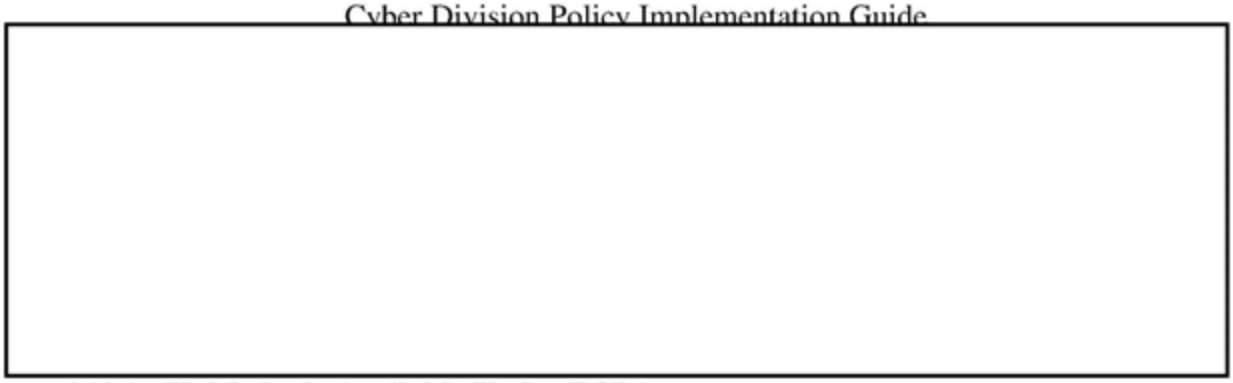
6.10. (U) Accessing Stored Electronic Communications

b7E

6.10.1. (U) Scope and Application

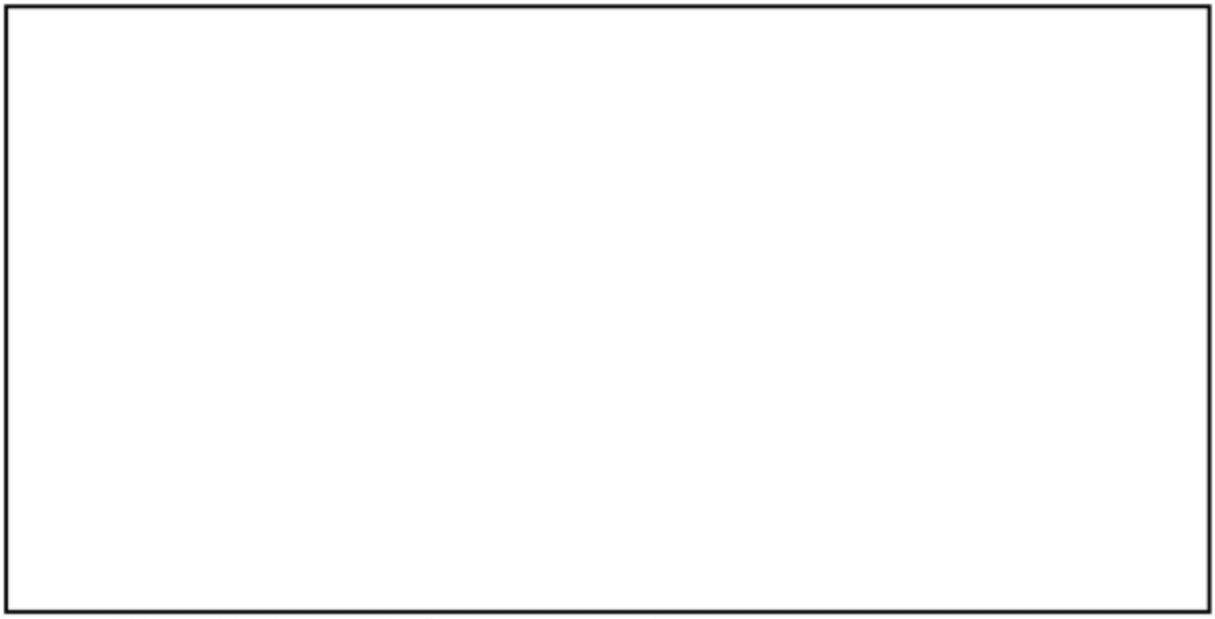
b7E

b7E



6.10.2. (U) Methods Available Under ECPA

b7E

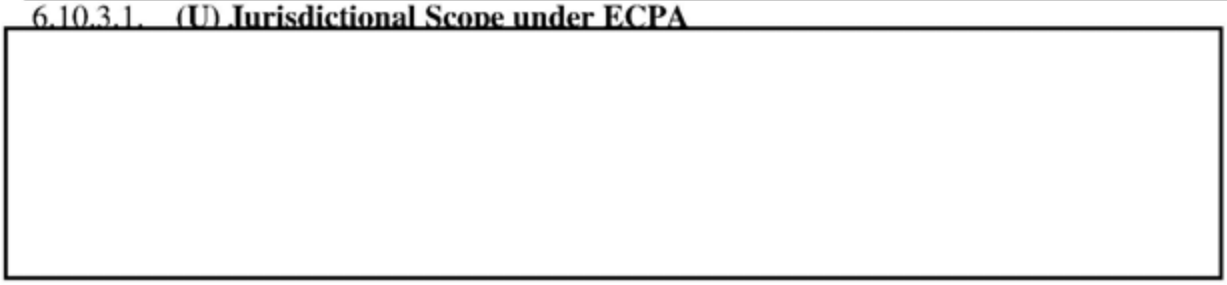


6.10.3. (U) ECPA Compelled Disclosure Provisions

b7E

6.10.3.1. (U) Jurisdictional Scope under ECPA

b7E



b7E

6.10.3.2. **(U) Notice Requirements Regarding ECPA Compelled Process**

b7E

6.10.3.3. **(U) Requirements for and Access Provided by Legal Process**

b7E

b7E

4

5

b7E

6.10.3.4. **(U) 18 U.S.C. § 2703(f) Preservation Letters**

b7E

6.10.4. (U) ECPA Voluntary Disclosure Provisions

b7E

6.10.4.1. (U) Disclosure of Contents under 18 U.S.C. § 2702(b)

b7E

6.10.4.2. (U) Disclosure of Customer Records under 18 U.S.C. § 2702(c)

b7E

b7E

6.10.4.3. **(U) Reporting ECPA Emergency Disclosures**

b7E

6.11. (U) Pen Register/Trap-and-Trace Device (PR/TT), Title III, and Searches Requiring Judicial Order or Warrant

(U) In addition to the guidance and requirements set forth in the DIOG, the following qualifications apply.

6.11.1. (U) Pen Register/Trap and Trace Device Orders

b7E

b7E

6.11.1.1. **(U) Nationwide Effect**

b7E

6.11.1.2. **(U) Certification**

b7E

6.11.2. (U) Reporting Requirement for

b7E

6.12. (U) Court-Ordered Electronic Surveillance, Title III

(U) In addition to the guidance and requirements set forth in the DIOG, the following guidance applies.

6.12.1. (U) Title III

(U) Title III intercepts, intrusive by their nature, are not undertaken lightly. Although real time data and voice intercepts are highly technical and require a great amount of specific justification and oversight, this method has been successfully utilized in cyber investigations. Agents considering implementation of a Title III intercept in a cyber investigation must notify the program manager in the operational unit as soon as possible in order to coordinate and facilitate implementation.

6.13. (U) Searches Requiring Judicial Order or Warrant

(U) In addition to the guidance and requirements set forth in the DIOG, CyD offers the following guidance.

6.13.1. (U) Express Consent

(U) A victim or subject of an investigation will sometimes consent to the FBI conducting a complete search of his or her computer. However, the consenting party's authority to consent is limited to the information they have authority to access. For example, a party does not have authority to provide consent to material that is password protected when they do not have the password. In all circumstances, agents must have any individuals with authority provide written consent, which must be documented using the FD-941 "Consent to Search Computer(s)" form. Agents must check with their CDC if there is any doubt as to the scope of a person's consent (i.e., the extent to which the FBI is authorized to retrieve information stored on the machine) or the legal ability of that person to provide consent for the search to take place. This issue often arises when a roommate, friend, parent, or other third party is providing consent to search.

6.13.2. (U) Search Warrants

(U) Search warrants, Rule 41 warrants and 18 U.S.C. § 2703(a) warrants are some of the most intrusive, but also some of the most effective, methods of obtaining evidence in criminal cyber matters. Once probable cause has been established to show a crime has been committed and evidence or fruits of that crime are believed to be at a specific physical location at a specific time, an application for a search warrant can be prepared and presented to a U.S. magistrate judge (see the DIOG for more guidance). Search warrants can be used to seize the subject's computer equipment and all storage media, as well as offline documentation, manuals, notes, and memoranda that may be relevant to the investigation. All computer-related search warrants must take into account the advanced nature of cybercrimes, and coordination with Computer Analysis and Response Team (CART) members is required.

7. (U) Summary of Legal Authorities

(U) Criminal cyber investigations often involve multiple violations by the same subjects. Therefore, all applicable statutes must be considered. This not only includes those statutes covering computer intrusions and cybercrime, but also statutes that are traditionally used for white collar crime, extortion, RICO, and money laundering. Several of the applicable statutes that should be considered for criminal cyber investigations are summarized and referenced below.

Statute	Violation
17 U.S.C. § 506	Copyright Infringement [1]
17 U.S.C. § 506 (c-d)	Fraudulent Notice/Removal of a Copyright Notice
17 U.S.C. §§ 1201, 1204	Digital Millennium Copyright Act
17 U.S.C. § 1201 (a)(1)	Circumvention of Copyright Infringement
17 U.S.C. § 1201 (a)(2)	Trafficking in Circumvention Tools and Services
17 U.S.C. § 1202	Falsifying, Altering or Removing Copyright Management Information
18 U.S.C. § 38	Fraud Involving Aircraft or Space Vehicle Parts in Interstate or Foreign Commerce
18 U.S.C. § 223	Obscene or Harassing Domestic or Foreign Telephone Calls or Other Communications
18 U.S.C. § 371	Conspiracy to Commit a Federal Offense
18 U.S.C. § 844(e)	Threats made in Interstate or Foreign Commerce to Fire or Explosives
18 U.S.C. § 875	Interstate Communications Related to Kidnapping, Ransoms, Extortion, Threats to Injure
18 U.S.C. § 1028	Fraud-Related with Identification Documents and Information
18 U.S.C. § 1029	Fraud Related to Connection with Access Devices

[1](U) Copyright protection is principally statutory. Federal copyright statutes are found primarily in Title 17 of the U.S. Code, of which §§ 101 and 1101 are called the "Copyright Act." The penalties for criminal infringement are set forth in 18 U.S.C. § 2319.

Statute	Violation
18 U.S.C. § 1030	Fraud Related to Computers
18 U.S.C. § 1037	Fraud and Related Activity in Connection with Electronic Mail
18 U.S.C. § 1084	Gambling
18 U.S.C. § 1341	Mail Fraud
18 U.S.C. § 1343	Wire Fraud [2,3,4]
18 U.S.C. § 1356	Tampering with Consumer Products
18 U.S.C. § 1361	Injury to Government Property
18 U.S.C. § 1466A	Obscene Visual Representations of the Sexual Abuse of Children
18 U.S.C. § 1832	Theft of Trade Secrets
18 U.S.C. § 1834	Forfeiture of Property under 18 U.S.C. § 1832
18 U.S.C. § 1951	Hobbs Act Extortion
18 U.S.C. § 1952	Racketeering
18 U.S.C. § 1953	Gambling: Interstate Transportation of Wagering Paraphernalia
18 U.S.C. § 1955	Prohibition of Illegal Gambling Businesses
18 U.S.C. §§ 1956 and 1957	Money Laundering [5]

[2] (U) Since the Fraud by Wire Statute, enacted July 16, 1952, was patterned after the Mail Fraud Statute (18 U.S.C. § 1341), mail fraud principles have been applied to fraud by wire prosecutions. As in the former, it is not necessary that the victim of the scheme be actually deceived or suffer a loss. Moreover, while it is necessary to show that a subject caused the use of a wire, it is not necessary to establish that a subject directly participated in the use of the wire; it is sufficient if some communications were a foreseeable result of a subject's act.

[3] (U) Conspiracy to violate 18 U.S.C. § 1343 must be prosecuted under the general conspiracy section (18 U.S.C. § 371).

[4] (U) 18 U.S.C. § 1343 is a specified unlawful act violation that can be utilized in the prosecution of 18 U.S.C. §§ 1956 and 1957, money laundering.

Statute	Violation
18 U.S.C. §§ 1961-1968	RICO[6]
18 U.S.C. § 2251	Sexual Exploitation of Children
18 U.S.C. § 2252	Activities Relating to Material Involving the Sexual Exploitation of Children
18 U.S.C. § 2252A	Activities Relating to Material Constituting or Containing Child Pornography
18 U.S.C. § 2252B	Misleading Domain Names on the Internet (re: Obscenity)
18 U.S.C. § 2260	Production of Sexually Explicit Depictions of a Minor for Importation into the United States
18 U.S.C. § 2261A	Interstate Stalking
18 U.S.C. §§ 2314 and 2315	Interstate Transportation of Stolen Property, including Trade Secrets
18 U.S.C. § 2318	Trafficking in Counterfeit Labels for Records; CDs; Computer Software; Computer Software Packaging, Movies; Gaming Software; Audio Visual Works
18 U.S.C. § 2319	Copyright Infringement Material – Punishments
18 U.S.C. § 2319A	Unauthorized Fixation and Trafficking in Sound Recordings and Music Videos of Live Performances
18 U.S.C. § 2319B	Unauthorized Recording of Motion Pictures in a Movie Theater (Camcording)
18 U.S.C. § 2320	Trafficking in Counterfeit Goods or Services
18 U.S.C. § 2423	Transportation of Minors
18 U.S.C. § 2511	Illegal Wiretap/Disclosure of Wiretap in Order to Obstruct

[5] (U) Money Laundering - In 1994, copyright infringement under 18 U.S.C. § 2319 was added to the list of violations that constitute "specified unlawful activity" under the money laundering statute, 18 U.S.C. § 1956. Thus, the proceeds earned by a defendant from copyright infringement can form the basis for a charge of money laundering.

[6] (U) RICO – In addition to the inclusion of several child exploitation violations such as "racketeering activity," the Anticounterfeiting Consumer Protection Act of 1996 amended 18 U.S.C. § 1961 to include Section 2319 within the definition of "racketeering activity."

Statute	Violation
	Justice
18 U.S.C. § 2701	Unlawful Access to Stored Communications
18 U.S.C. § 2702	Voluntary Disclosure of Customer Communications or Records
18 U.S.C. § 2703	Required Disclosure of Customer Communications or Records
47 U.S.C. § 223	Harassment (with telecommunication device)

(U) The following Acts of Congress provide the historical and legal foundation of the FBI's authority to investigate computer intrusion matters.

7.1. (U) Comprehensive Crime Control Act of 1984

(U) On October 12, 1984, President Reagan signed into law the "Comprehensive Crime Control Act of 1984." Included in the passage of this act was "Fraud and Related Activity in Connection with Computers," 18 U.S.C. § 1030. The creation of this statute was an attempt by Congress to address unauthorized access or use of computers. Jurisdiction for investigating violations of this statute is governed by memoranda of understanding (MOU) between the Department of Treasury and the DOJ.

7.2. (U) Computer Fraud and Abuse Act of 1986

(U) This Computer Fraud and Abuse Act of 1986 expanded 18 U.S.C. § 1030, which contains provisions against the unauthorized access or use of "federal interest" computers with intent to harm the U.S. government by obtaining classified or private financial information; modifying, destroying, or disclosing information; preventing use of the computer by others; or affecting computer operations by adding fraudulent access to obtain property of value, trafficking in passwords with intent to defraud, and damage to certain stored information.

7.3. (U) Electronic Communications Privacy Act of 1986

(U) The ECPA enhances individual and corporate protection against computer crime. Title II of this act amended Title 18 of the U.S.C. by adding Section 2701. This statute makes it a federal offense to access or disclose, without authorization, the contents of a "wire or electronic communication while it is in electronic storage."

7.4. (U) USA PATRIOT Act

(U) The USA PATRIOT Act contains several antiterrorism provisions, including changes to surveillance authorities under ECPA and changes to the Computer Fraud and Abuse Act. Among the changes to 18 U.S.C. § 1030 are: (1) increased penalties for hackers who damage protected computers (from a maximum of ten years to a maximum of 20 years); (2) clarification of the *mens rea* required for such offenses to make explicit that a hacker

need only intend damage, not a particular type of damage; (3) the addition of a new offense for damaging computers used for national security or criminal justice; (4) expanded coverage to include computers in foreign countries so long as there is an effect on U.S. interstate or foreign commerce; (5) state convictions may now count as prior offenses for recidivist sentencing enhancements; and (6) the $5,000 jurisdictional threshold may be calculated by aggregating losses to several computers from a hacker's course of conduct.

(U) Some additional highlights related to cybercrime are outlined below:

- (U) The USA PATRIOT Act also amended 18 U.S.C. § 2516(1), the subsection that lists those crimes for which investigators may obtain a wiretap order for wire and oral communications. Felony violations of 18 U.S.C. § 1030 have been added to the list of predicate offenses.
- (U) A new exception to Title III was added to allow victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer systems.
- (U) A number of other changes to ECPA are relevant to 288 investigations, including the expansion of the list of items subject to a subpoena to include the means and source of payment for the service; the records of session times and durations; and any temporarily assigned network address.
- (U) 18 U.S.C. § 2702 was amended to clarify that service providers may voluntarily disclose records and the content of communications under certain circumstances, including to a governmental entity if the provider reasonably believes that an emergency involving serious injury justifies the disclosure.
- (U) Significant changes were also made to 18 U.S.C. § 3121 (the pen register/trap and trace device statute) that clarify its applicability to communications on the Internet and other computer networks and allow for nationwide service of a single order without the necessity of returning to the court for each new carrier involved in transmitting the communication.

7.5. (U) PATRIOT Reauthorization Acts of 2005 and 2006

(U) USA PATRIOT Improvement and Reauthorization Act of 2005 (USPA IRA) and USA PATRIOT Act Additional Reauthorization Amendments of 2006.

(U) Both laws make changes to many national security legal authorities, including NSLs, FISA durations, reporting requirements, and several criminal statutes. The changes related to NSLs and FISA are discussed in more detail in the *Cyber Division PG National Security Appendix*.

(U) The duration was extended for both initiations and renewals of ELSUR (FISA Section 105(e)), physical searches (FISA Section 304(d)), and pen register/trap and trace surveillance (FISA Section 402(e)) for agents of a foreign power who are non-U.S. persons (USPER). Orders for ELSUR surveillance are provided for a period of time not to exceed: 90 days for USPERs; 120 days for non-USPERs; and one year for a foreign power. Renewal of FISA orders may be requested for the same period of time originally

authorized, based upon a continued showing of probable cause. For non-USPERs, renewals can be for a period not to exceed one year. National Security Division, DOJ, requests that all renewal requests be submitted by the requesting field office to DOJ at least 45 days prior to the expiration of the existing order.

(U) Congress modified the FISA pen register/trap and trace device authority to give the FBI access to more customer information, eliminating the need to secure a FISA business record order in conjunction with a pen register/trap and trace device order to obtain customers or subscribers who use the service covered by the pen register/trap and trace order. Under a pen register/trap and trace device order, agents are now able to obtain the name and address of the customer and the subscriber; the telephone instrument number or other subscriber number or identifier of the customer or subscriber, including any temporarily assigned network address or associated routing or transmission information; the length of the provision of service by the provider and the types of services utilized by the customer or subscriber; any local or long distance telephone records, if applicable; any records reflecting periods of usage or sessions; and mechanisms and sources of payment including account numbers for banks or credit cards.

(U) In order to activate the nondisclosure requirement of an NSL, the NSL must now contain a certification from either the Director of the FBI, the special agent in charge (SAC) of a field office, if so designated by the Director (each field office will have received a communication from FBIHQ on their designation), or an AD or deputy assistant director (DAD).

(U) The EC requesting an NSL must set forth the reason why nondisclosure is necessary, and the NSL itself must contain a certification paragraph that disclosure would result in danger to the national security of the United States. Agents must now advise recipients that they may disclose the contents of the NSL to persons necessary to comply with the NSL or provide legal advice. Recipients must be informed of the requirement to pass on the nondisclosure requirement to whomever recipients disclose the NSL. If requested by the FBI, recipients must disclose to the FBI the identities of those to whom the NSL was disclosed, except for the names of their legal counsel. Title 18 U.S.C. § 1510 makes it a federal crime for an individual to knowingly, and with the intent to obstruct an investigation, violate the nondisclosure provision of an NSL.

(U) USPA IRA also mandates enhanced oversight of ECPA's good faith emergency disclosure of communication contents. 18 U.S.C. § 2702(b)(8) allows a provider of a remote computing service or electronic communication service to the public to voluntarily divulge the contents of a communication to a governmental entity when the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency. The USPA IRA added 18 U.S.C. § 2702(d) to provide congressional oversight when DOJ receives information under this provision. Specifically, 18 U.S.C. § 2702(d) requires that the AG, on an annual basis, submit a report to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate containing the number of accounts from which the DOJ has received voluntary disclosures under 18 U.S.C. § 2702(b)(8), and a summary of the basis

for disclosure in those instances where the investigation pertaining to those disclosures was closed without the filing of criminal charges.

(U) The USPA IRA also amended ECPA so that the same standard now applies under 18 U.S.C. § 2702(b)(8) and 18 U.S.C. § 2702(c)(4) when a provider decides to voluntarily disclose subscriber noncontent records and subscriber communication contents under emergency circumstances. Disclosure is permitted under either provision "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency." The USPA IRA also added a new definition to ECPA, stating at 18 U.S.C. § 2711(4) that the term "governmental entity" means "a department or agency of the United States or any State or political subdivision thereof." Foreign government agencies are not included within the definition.

8. (U) Appendices

(U) The following appendices address cyber investigative matters and other information that is either classified above the level of the CyDPG or addresses the operations of a specific unit or initiative. None of these appendices constitutes a standalone PG and each must be considered as a supplement to the information found in this guide. Unless specifically excepted, the guidance in the appendices must be read only to impose further qualifications and limitations on the investigative activity found in the DIOG and in Sections 1 through 6 of this PG, and must not be interpreted to provide authorization not provided for elsewhere in the DIOG.

(U) Appendix A: Classified Investigations

(U//FOUO) Appendix A, *National Security*, is maintained as a separate document to keep the classification of the rest of the CyDPG unclassified.

(U) Appendix B: Innocent Images National Initiative (IINI)

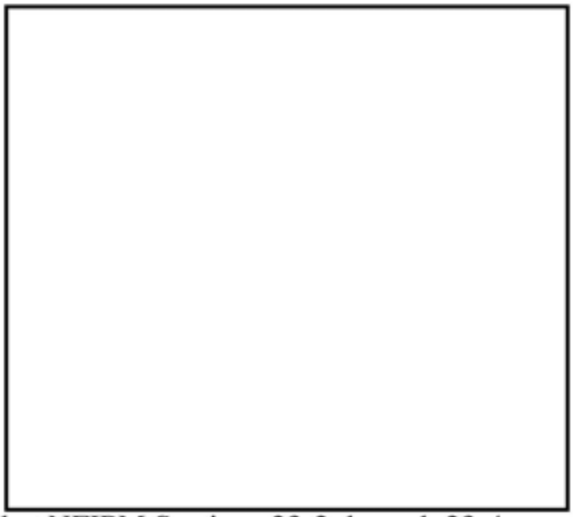
(U) Appendix B, *Innocent Images National Initiative Policy Implementation Guide*, provides additional policy and guidance specifically applicable to investigations within the IINI, which includes all investigations regarding child sexual exploitation and child pornography facilitated by the use of online computers. It is incorporated into the CyD PG by reference.

(U) Appendix C: InfraGard® Program Policy Implementation Guide

(U) The *InfraGard® Program Policy Appendix* is maintained as a separate guide primarily for use by InfraGard® Program coordinators and program managers. It is incorporated into the CyD PG by reference.

(U) Appendix D: Superseded *National Foreign Intelligence Program Manual* (NFIPM) Sections, *Manual of Investigative Operations and Guidelines* (MIOG) Sections, and Documents

(U) The following NFIPM sections, MIOG sections, and other documents are superseded by the CyD PG:

- NFIPM 23 1-15
- MIOG Part 1-264
- MIOG Part 1-288
- MIOG Part 2-295
- MIOG Part 2-316
- MIOG Part 2-196
- MIOG Part 2-163
- MIOG Part 2-139
- MIOG Part 1-92
- MIOG Part 2-253
- MIOG Part 2-258
- MIOG Part 1-305
- *305 Innocent Images National Initiative (IINI) Manual*, dated August 03, 2005 b7E
- 

(U) Note that NFIPM Sections 23-2 through 23-4 were no longer valid following the creation of the DHS in Fiscal Year (FY) 2003.

(U) Note that there was no previous policy regarding 334 IPR, health and safety matters.

(U) Note that MIOG Sections 145-1.8, 145-4.7, and 145-4.8 discuss sexual exploitation of children (i.e., child pornography), which is also in the purview of the CyD PG and former MIOG, Part 1, Section 305.

(U) Appendix E: Key Words

(U) **Academic nexus:** As a matter of FBI policy, an investigative activity having an academic nexus is considered a sensitive investigative matter if: (1) the investigative activity involves matters related to the responsibilities of an administrator or faculty member employed by any college or university, provided the matter under a predicated investigation is related to the individual's position at the institution or (2) the matter involves any student association recognized and approved by that institution. See Appendix A, for additional information.

(U) **Actionable intelligence:** intelligence sufficiently developed for a field office or other investigative entity, where basic questions regarding scope, potential impact, venue and physical location of threat/actors or key components of the scheme (e.g., command and control, dump sites, and so on) have been answered.

(U) **Attribution:** the identification of the specific person, place, group, organization, or foreign power responsible for a computer intrusion or other malicious cyber activity.

(U) **Botnet**: short for “robot network.” A collection of compromised computers running malicious software under a common command–and-control infrastructure.

(U) **Camcording:** the use of an audiovisual recording device (e.g., a hand-held video camera) to capture and copy a motion picture or other audiovisual work while it is being displayed in a movie theater or other exhibition facility.

(U) **Computer trespasser:** a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer. This does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer. (18 U.S.C. 2510(21).

(U) **Consensual monitoring:** monitoring of communications for which a court order or warrant is not legally required because of the consent of a party to the communication.

(U) **Copyright:** Copyright law protects the original expression of an idea or concept in tangible form (i.e., a novel, a song, a carpet design, or computer source code), but does not extend to protection of the idea or concept itself. Thus, copyright law protects interests distinct from those protected by patent laws, which provide exclusive rights to inventors of new methods or processes and trademark laws, which protect the exclusive use of certain names and slogans in connection with certain goods or services. Congress provided copyright protection to all "original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device," (17 U.S.C. § 102(a)).

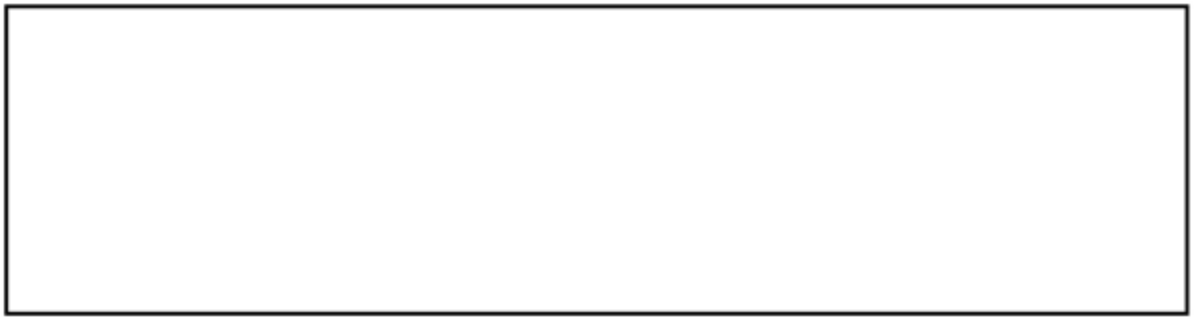
(U) **Copyright infringement:** Generally, infringement is the violation of one of five exclusive rights granted to a copyright owner by federal law. The five exclusive rights are: (1) reproduction, (2) distribution, (3) public display, (4) public performance of the copyrighted work, and (5) preparation of derivative works based upon the original copyrighted work (17 U.S.C. § 106(1)-(5)). Title 18 U.S.C. § 2318 prohibits the

counterfeit labeling of copyrighted works. Title 18 U.S.C. § 2319A expressly covers the unauthorized "fixation" of and trafficking in recordings and musical videos of live musical performances.

(U) **Counterfeit/trafficking in counterfeit goods:** The Copyright Act, 18 U.S.C. § 2318, enhanced the integrity of the copyright system by specifically prohibiting trafficking in counterfeit labels designed to be affixed to phonorecords, copies of computer programs, motion pictures and audiovisual works, and counterfeit documentation or packaging for computer programs. Many copyright infringement crimes make use of counterfeit labels, and in some cases, it can be easier for the government to prove the counterfeit labeling count than the copyright infringement count. For example, the counterfeit labeling crime does not require proof of infringement (i.e., actual copying or distribution). It is enough to show that the subject was "trafficking." In addition, a counterfeit labeling case requires proof of only a "knowing" mental state, rather than a "willful" mental state.

(U) **Criminal computer intrusion:** intrusions or attempted intrusions into any computer or information system that may adversely impact the confidentiality, integrity, or availability of critical infrastructure data, components, or systems (cyber threats or incidents involving the national information infrastructure) by, or on behalf of, individuals or groups who are not international terrorists or other foreign powers. Often, criminal computer intrusions are motivated by potential monetary gains, such as intent to defraud, extort, or steal. Criminal intrusions also include intrusions conducted with the intent to cause damage or deprive computer owners of the use of their systems or networks, which would include intrusions for the purpose of retaliation, defamation, vandalism, hate, or other purposes.

b7E



(U) **Digital forensics:** Digital forensics is the science of identifying, collecting, preserving, documenting, examining, analyzing, and presenting evidence from computers, networks, and other electronic devices. In addition to computer forensics, some professional organizations recognize forensic audio, video, and image analysis as sub disciplines of digital forensics.

(U) **Electronic communication service:** any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, telephone companies and electronic mail companies generally act as providers of electronic communication services.

(U) **Electronic communications system**: any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications,

and any computer facilities or related electronic equipment for the electronic storage of such communications.

(U) **Electronic storage:** any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof, or any storage of such communication by an electronic communication service for purposes of backup protection of such communication. In short, electronic storage refers only to temporary storage made in the course of transmission by a provider of an electronic communication service.

b7E

(U) **Employee:** an FBI employee or an employee of another agency working under the direction and control of the FBI.

(U) **Enterprise investigation:** Enterprise investigations are a type of full investigation and are subject to the same requirements that apply to full investigations as described in the DIOG. An enterprise investigation as defined in the DIOG is distinct from a full investigation pursuant to prosecution under Title 18 U.S.C. section 2252A(g) (Child Exploitation Enterprises statute).

(U) **FISA:** The Foreign Intelligence Surveillance Act of 1978, as amended, establishes a process for obtaining judicial approval of electronic surveillance and physical searches for the purposes of collecting foreign intelligence. Orders for ELSUR surveillance are provided for a period of time not to exceed 90 days for United States Persons; 120 days for non-United States Persons; and one year for a foreign power. Renewal of FISA orders may be requested for the same period of time originally authorized, based upon a continued showing of probable cause. For non-United States Persons, renewals can be for a period not to exceed one year. National Security Division, DOJ requests that all renewal requests be submitted by the requesting field office to DOJ at least 45 days prior to the expiration of the existing order.

b7E

b7E

b7E

b7E

b7E

(U) **Identity theft:** Identity theft occurs when someone appropriates another individual's personal information without his or her knowledge in order to commit theft or fraud. Identify theft is a vehicle for perpetrating other types of fraud schemes. In its classic form, also referred to as "social engineering," victims are led to believe they are divulging sensitive personal information to a legitimate business, sometimes as a response to an e-mail solicitation to update billing or membership information, or as an application to a fraudulent Internet job posting. This can be done through "spoofing" and "phishing." More recently, identity theft occurs directly through computer intrusion activity or a combination intrusion and social engineering activity.

(U) **Intellectual property rights:** Legal constructs have created enforceable rights in certain intangibles which have become familiar as intellectual property, including copyrights, trademarks, patents, and trade secrets. Although civil remedies, which may provide compensation to wronged intellectual property rights holders, are available, criminal sanctions are often warranted to ensure sufficient punishment and deterrence of wrongful activity. However, some misuse of intellectual property has not been criminalized. For example, infringement of a patent is not generally a criminal violation.

(U) **Intelligence activities:** any activity conducted for intelligence purposes or to affect political or governmental processes by, for, or on behalf of a foreign power.

(U) **International terrorism:** activities that involve violent acts or acts dangerous to human life that violate federal, state, local, or tribal criminal law or would violate such law if committed within the United States or a state, local, or tribal jurisdiction; appear to be intended to intimidate or coerce a civilian population; influence the policy of a government by intimidation or coercion; affect the conduct of a government by assassination or kidnapping; and occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons

they appear to be intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

(U) **Internet Crime Complaint Center (IC3):** The IC3 is a clearinghouse and repository for complaints from industry and private citizens regarding cybercrime. The IC3 is in partnership with the National White Collar Crime Center, a nonprofit organization funded by Congress. The IC3 database links the victim complaints together through its "Automatch" system. The complaint information is combined in an internal IC3-related case. The IC3 Internet crime specialist (ICS) will conduct an open and closed source check on the identifying information. The referral is provided to the appropriate law enforcement agency, FBI field offices, and/or Legats for investigative purposes. The IC3 will provide analytical support for active cyber investigations. A search query of the IC3 database can be requested through FBI Intranet e-mail at HQ-DIV16-IC3-DATABASE-SEARCH. The request should include the case file number and all pertinent information the requestor would want searched through the IC3 database.

(U) **Internet fraud:** Internet fraud is any fraudulent scheme that uses one or more components of the Internet, such as chat rooms, e-mail, message boards, Web sites, etc., to present false or fraudulent solicitations or representations, conduct fraudulent transactions, or transmit fraudulently obtained proceeds.

(U) **Internet piracy:** The ability to duplicate and distribute with near perfect quality has increased not only the amount of copyright infringement which occurs online, but the frequency of infringement. Web sites that are dedicated, either entirely or in part, to providing widespread access to copyrighted materials are commonly known as "warez" (pronounced "wares") sites. Title 17 U.S.C. § 506(a) (2) allows for prosecution in cases involving large-scale illegal reproduction or distribution of copyrighted works where the infringers act willfully, but without a discernible profit motive.

(U) **Investigator:** The term "investigator," as used in this guide, is intended to be inclusive of FBI special agents (SA), intelligence analysts (IA), online covert employees (OCE), UCEs, and any other FBI employees engaged in activities authorized by the AGG-Dom and the DIOG, as well as any task force officers, assignees, or detailees to the FBI who are expected to follow FBI operational policy when working on behalf of the FBI, as delineated by the cooperative agreement, memorandum, or other contract under which they are operating.

(U) **Money laundering (cyber money laundering):** Cyber money laundering is the digital transfer of assets to conceal the existence, illegal source, or illegal application of income to make it appear legitimate.

(U) **National Security Letters:** An administrative demand for documents or records that can be made by the FBI during a predicated investigation relevant to a threat to national security. The standard for issuing an NSL, except under 15 U.S.C. § 1681v, is relevance to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigations of USPERS are not predicated solely on activities protected by the First Amendment of the Constitution of the United States. Information is relevant if it tends to make a fact more or less probable. There must

be a reasonable belief that the information sought through the NSL either supports or weakens the case being investigated.

b7E

(U) **Phishing:** A technique whereby the perpetrator impersonates another individual or business through the use of e-mail or Web sites that copy (or mimic) legitimate e-mail or Web site characteristics. Phishing refers to the scheme whereby the perpetrators use "spoofed" e-mail/Web sites in an attempt to dupe victims into divulging sensitive information, including passwords, credit card numbers, and bank account numbers. Victims are provided with a hyperlink, usually by e-mail, which is directed to a fraudulent Web site whose URL (uniform resource locator) closely resembles the true name of a legitimate business. Victims arrive at the fraudulent Web site, and convinced by the site's content that they are visiting the company's legitimate Web site, are tricked into divulging sensitive personal information. Spoofing and phishing are done to further perpetrate other schemes, including identity theft, credit/debit card fraud, and auction fraud. Phishing is a form of social engineering.

(U) **Physical surveillance:** the deliberate observation by an FBI employee of persons, places, or events, on either a limited or continuous basis, in a public or a semipublic (e.g., commercial business open to the public) setting.

(U) **Preliminary investigation:** Preliminary investigations may be carried out to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security. However, a preliminary investigation cannot be used solely for the purpose of collecting against foreign intelligence requirements or FBI national or field office collection requirements, or for conducting enterprise investigations (see the "Preliminary Investigations" section of the DIOG). Intelligence responsive to foreign intelligence requirements or FBI national or field office collection requirements must be collected incidental to a predicated substantive investigation. Incidentally collected intelligence must be forwarded to the for evaluation and potential dissemination against collection requirements. In preliminary investigations, the immediate objectives include such matters as determining whether a federal crime has occurred, is occurring, or if planning or preparation for such a crime is taking place; identifying, locating, and apprehending the perpetrators; obtaining evidence needed for prosecution; or identifying threats to the national security. The investigation of threats to national security may constitute an exercise of the FBI's criminal investigation authority, as well as its authority to investigate threats to national security. As with criminal investigations, detecting and solving crimes and arresting and prosecuting perpetrators are objectives of investigations relating to threats to the national security. These investigations, however, serve important purposes outside the scope of normal criminal investigations, by providing the basis for making informed decisions concerning other measures needed to protect the national security.

b7E

(U) **Pretexting:** the act of creating and using an invented scenario (the pretext) to persuade a targeted victim to release information or perform an action. Pretexting is typically done over the telephone. It is more than a simple lie, as it often involves some prior research to set up and use the pieces of information (e.g., date of birth, Social Security number [SSN], or last bill amount) to establish legitimacy and perceived authority in the mind of the target. (See also: social engineering, vishing, spear phishing.)

(U) **Provider of electronic communication services:** any service that provides the user thereof the ability to send or receive wire or electronic communications.

(U) **Publicly available:** information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public.

(U) **Records:** All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by, in connection with the transaction of public business.

(U) **Remote computing services:** the provision to the public of computer storage or processing services by means of an electronic communication system. In essence, a remote computing service is an off-site computer that stores or processes data for a customer.

(U) **Sensitive investigative matter:** an investigative matter involving a domestic public official; political candidate; religious or political organization or individual prominent in such an organization; news media, or any other matter which, in the judgment of the official authorizing an investigation, must be brought to the attention of FBIHQ and other DOJ officials.

(U) **Sensitive circumstance:** a circumstance arising in a UCO that requires FBIHQ approval. A comprehensive list of sensitive circumstances for criminal activities is contained in the AGG-UCO and for national security matters in Section 28 of the NFIPM. The Criminal Operations Undercover Review Committee (CUORC) and the Undercover Program Review Committee (UCRC) must review and approve UCOs that involve sensitive circumstances. See the DIOG and the FGUSO.

b7E

b7E

(U) **Signal theft:** Certain businesses, such as cable television and satellite broadcasting firms, serve an important role in developing systems for the dissemination of intellectual property. Five federal statutes are often used, along with a host of state statutes, to protect these systems from traffickers who sell devices that facilitate interception of the signal carrying the protected intellectual property (see 18 U.S.C. §§ 1341, 1343, and 2512 and 47 U.S.C. §§ 553 and 605). These violations include the unauthorized reception and unauthorized publication or use of communications.

(U) **Smishing:** a form of criminal activity using short message service (SMS) technology to deliver text messages to bait a user into clicking on a Web site embedded in the message. The name derives from a combination of the terms "SMS" and "phishing." Smishing is a form of social engineering.

(U) **Social engineering:** the act of manipulating people into performing actions or divulging confidential information. The term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases, the attacker never comes face to face with the victim. At their core, all types of social engineering rely on a variation of "pretexting" and exploit attributes of human decision-making known as cognitive biases, sometimes called "bugs in the human hardware." Although the term applies to a broad range of fraudulent behavior, common examples of social engineering practices include phishing, spear phishing, vishing, and smishing.

(U) **Spam:** the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately. The messages are nearly always "spoofed," and may include fraudulent phishing e-mails or Web site links. Often, spam is the vehicle for malware intended to compromise users' computer systems or networks.

(U) **Spear phishing:** a targeted form of phishing where e-mails or Web sites are transmitted to an identified target of the activity, as opposed to the use of phishing, designed to ensnare targets that have not been previously identified (i.e., spamming). Spear phishing is a form of social engineering.

(U) **Special Agent in Charge:** The SAC of an FBI field office (including an acting Special Agent in Charge), except that the functions authorized for SACs by these guidelines may also be exercised by the Assistant Director in Charge (ADIC) or by any SAC designated by the ADIC in an FBI field office headed by an AD, and by FBIHQ officials designated by the Director of the FBI.

(U) **Spoofing:** a scheme in which a person or program masquerades as another by falsifying data resulting in the deception of the recipient or user. Spoofing takes many forms. Web page spoofing involves use of a Web page that reproduces the "look and feel" of a legitimate site, but is under the control of another for the purpose of collecting

information from a user who believes he or she is interacting with the trusted site. URL spoofing involves the false display of a URL to collect password information. Caller ID spoofing involves creating false caller ID for display on the recipients device. E-mail address spoofing involves faking the e-mail address in the "from" field of an e-mail. “Man-in-the-middle” attacks are an advanced form of Internet Protocol spoofing that can permit the interception of encrypted communications.

(U) **State, local, or tribal:** relating to any state or territory of the United States or political subdivision thereof, the District of Columbia (D.C.), or Indian tribe.

(U) **Subpoena:** A grand jury subpoena *duces tecum* compels an individual or collective entity (e.g., corporation, limited liability company) to produce documents, records (including electronic records), or other tangible objects to the grand jury, or compels an individual to submit or display personal physical evidence to the grand jury, see *In re Grand Jury Proceedings (Mills)*, 686 F.2d 135, 145 (3d Cir. 1982) (concurring opinion) ("grand jury demand for physical evidence [e.g., hair, fingerprints] should be viewed as a subpoena duces tecum—i.e., a subpoena for the 'production of ... objects,' Fed. R. Crim. P. 17(c)"). *Duces tecum* is a Latin phrase that means "bring with you." *Black's Law Dictionary* 538 (8th ed. 2004).A grand jury subpoena can compel both testimony and the production of records and other tangible objects. Often, however, a party compelled to produce items is given the opportunity to provide the items directly to the prosecution prior to the date of production, which then waives the appearance before the grand jury.

(U) **Surveillance (electronic):** Electronic surveillance is the nonconsensual electronic collection of information (usually communications) under circumstances in which the parties have a reasonable expectation of privacy and court orders or warrants are required. ELSUR is only authorized as an investigative method in the conduct of full investigations. ELSUR requires (1) administrative or judicial authorization prior to its use; (2) contact with the field office ELSUR support employee to coordinate all necessary recordkeeping; and (3) consultation with a technical advisor (TA) or a designated TTA to determine feasibility, applicability, and use of the appropriate equipment.

(U) **Surveillance (physical):** Physical surveillance is the deliberate observation by an FBI employee [redacted] of persons, places, or events, on either a limited or continuous basis, in a public or a semipublic (e.g., commercial business open to the public) setting. The duration and frequency of the observation of a particular person or location; the location of the observation point; whether the observation is done from a stationary position or a moving position; and whether the observation is being done with the unaided eye are considerations in determining whether observations are casual observation or physical surveillance. The use of mechanical devices operated by the user (e.g., binoculars; hand-held cameras; radiation, chemical, or biological detectors) is authorized, provided that the device is not used to collect information in which a person has a reasonable expectation of privacy. b7E

(U) **Theft of trade secret:** The Economic Espionage Act of 1996, 18 U.S.C. §§ 1831-1839 contains two separate provisions that criminalize the theft or misappropriation of trade secrets. The first provision, codified at 18 U.S.C. § 1831(a), is directed towards foreign economic espionage and requires that the theft of the trade secret be utilized to benefit a foreign government, instrumentality (company), or agent (individual). For the

more serious nature of foreign government-sponsored economic espionage, an individual convicted of violating 18 U.S.C. § 1831(a) can be imprisoned for up to 15 years and fined $500,000 or both. Organizations found guilty can be fined up to $10 million for violating 18 U.S.C. § 1831(a). The second provision of the EEA, 18 U.S.C. § 1832, centers around the criminal activity between U.S. companies and/or individuals in which the theft is purely for economic gain, commercial advantage, or revenge. "Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret…"

(U) **Threat to the national security:** international terrorism; espionage and other intelligence activities; sabotage and assassination conducted by, for, or on behalf of, foreign powers, organizations, or persons; foreign computer intrusion; and other matters determined by the AG, consistent with Executive Order 12333 or a successor order.

(U) **Trademark:** the interest in using a commercial identity or brand to distinguish a product or service to consumers is protected federally by the law of trademark. The Lanham Act, 15 U.S.C. § 1051-1127, prohibits the unauthorized use of a trademark. A trademark is defined as "any word, name, symbol, device, or any combination thereof -- (1) used by a person, or (2) which a person has a bona fide intention to use in commerce and applies to register on the principal register, 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, even if that source is unknown" (15 U.S.C. § 1127). Congress established a federal administrative process for registering trademarks, and federal registration is a jurisdictional prerequisite for federal criminal prosecution. The statute itself requires that the "use" of the counterfeit mark be "likely to cause confusion, to cause mistake, or to deceive." The criminal violation associated with trademarks derives directly from the protection a trademark was intended to establish: preventing counterfeiters from using trademarked "marks" in the trafficking of their counterfeit goods. Most large-scale copyright cases involve the unauthorized use of a trademark in violation of 18 U.S.C. § 2320; for instance, infringing copies of movies will typically be sold with packaging bearing the trademark of the rightful owner or distributor.

(U) **Trade secret:** a trade secret is any formula, pattern, device, or compilation of information used in a business to obtain an advantage over competitors who do not know or use it. A "trade secret" includes all forms and types of information – financial, business, scientific, technical, economic or engineering – that the owner has taken reasonable measures to keep secret, and that has independent economic value because it is not generally known or ascertainable by the public (see theft of trade secret).

(U) **Trap and trace device:** captures incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, provided that such information does not include the contents of any communication.

b7E

b7E

b7E

(U) **United States:** when used in a geographic sense, means all areas under the territorial sovereignty of the United States.

(U) **United States Person:** Any of the following, but not including any association or corporation that is a foreign power:

1) An individual who is a United States citizen or an alien lawfully admitted for permanent residence.
2) An unincorporated association substantially composed of individuals who are United States Persons.
3) A corporation incorporated in the United States.

In applying number (2) above, if a group or organization in the United States that is affiliated with a foreign-based international organization operates directly under the control of the international organization and has no independent program or activities in the United States, the membership of the entire international organization must be considered in determining whether it is substantially composed of United States Persons. If, however, the United States-based group or organization has programs or activities separate from, or in addition to, those directed by the international organization, only its membership in the United States must be considered in determining whether it is substantially composed of United States Persons. A classified directive provides further guidance concerning the determination of United States Person status.

b7E

(U) **Vishing:** the criminal practice of using social engineering over a telephone system to gain access to personal and financial information from the public. This can take the form of victims receiving voicemails on their home and cellular telephones to call a specific number to verify account numbers and personal identification numbers (PIN). The name derives from a combination of the words voice and phishing. Vishing is a form of social engineering.

(U) Appendix F: Acronyms

(U) Acronyms

ACDC	Assistant Chief Division Counsel
ACS	Automated Case Support
AD	Assistant Director
ADIC	Assistant Director in Charge
AFID	Alias False Identification
AG	Attorney General
AGG	Attorney General's Guidelines
AGG-CHS	The Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources
AGG-Dom	The Attorney General's Guidelines for Domestic FBI Operations
AGG-Ext	The Attorney General's Guidelines for Extraterritorial FBI Operations
AGG-UCO	The Attorney General's Guidelines on FBI Undercover Operations
a.k.a.	Also Known As
AOR	Area of Responsibility
ASAC	Assistant Special Agent in Charge
AUSA	Assistant United States Attorney
BAU	Behavior Analysis Unit
BSA	Bank Secrecy Act
CA	Cooperative Agreement
CAC	Crimes Against Children
CART	Computer Analysis Response Team
CBP	United States Customs and Border Protection

CCD	Consular Consolidated Database
CCDAS	Consolidated Consular Database Alert System
CCIPS	Computer Crime and Intellectual Property Section (DOJ)
CCU	Cyber Criminal Unit
CD	Counterintelligence Division
CDC	Chief Division Counsel
CEDU	Cyber Education and Development Unit
CEOS	Child Exploitation and Obscenity Section
CFR	Code of Federal Regulations
CHIP	Computer Hacking and Intellectual Property
CHS	Confidential Human Source
CHSPM	Confidential Human Source Policy Manual
CHSVSM	Confidential Human Source Validation Standards Manual
CI	Counterintelligence
CIA	Central Intelligence Agency
CIA/IOC	Central Intelligence Agency Information Operations Center
CIKR	Critical Infrastructure and Key Resource Sectors
CID	Criminal Investigative Division
CIRFU	Cyber Initiative and Resource Fusion Unit
CIRG	Critical Incident Response Group
CNA	Computer Network Attack
CNCI	Comprehensive National Cyber Initiative

CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
CNSS	Cyber National Security Section
COG	Computer Operations Group
CPD	Corporate Policy Directive
CPO	Corporate Policy Office
CSE	Child Sexual Exploitation
CSS	Central Security Service
CSSB	Control Systems Security Branch
CSO	Chief Security Officer
CT	Counterterrorism
CTD	Counterterrorism Division
CUORC	Criminal Undercover Operations Review Committee
CVIP	Child Victim Identification Program
CyD	Cyber Division
CyD PG	Cyber Division Policy Implementation Guide
DAD	Deputy Assistant Director
DAG	Deputy Attorney General
DAIS	Data Acquisition Intercept Section
DARC	Data Analysis Research Center
DC3	Department of Defense Cyber Crimes Center
DCO	Division Compliance Officer
DDoS	Distributed Denial of Service

DHS	Department of Homeland Security
DI	Directorate of Intelligence
DIOG	Domestic Investigations and Operations Guide
DNI	Director of National Intelligence
DOD	Department of Defense
DOJ	Department of Justice
DOJ-OIP	DOJ - Online Investigative Principles for Federal Law Enforcement Agents
DOS	Department of State
DTOU	Domestic Terrorism Operations Unit
DTSOS	Domestic Terrorism and Strategic Operations Section
DVD	Digital Video Disc
EA	Emergency Authority
EAD	Executive Assistant Director
EAP	Employee Assistance Program
E-business	Electronic Business
EC	Electronic Communication
ECG	Exploitation Capabilities Group
ECPA	Electronic Communication Privacy Act
ECS	Electronic Communication Service
EEA	Economic Espionage Act of 1996
ELSUR	Electronic Surveillance
E-mail	Electronic Mail
EO	Executive Order

ERS	ELSUR Records System
ESN	Electronic Serial Number
ESU	Electronic Surveillance Unit
FBI	Federal Bureau of Investigation
FBI HQ	FBI Headquarters
FBINET	FBI Network
FCC	Federal Communications Commission
FCRA	Fair Credit Reporting Act
FDA	Food and Drug Administration
FGJ	Federal Grand Jury
[redacted]	[redacted] b7E
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
FISA	Foreign Intelligence Surveillance Act
FISAMS	FISA Management System
FISC	Foreign Intelligence Surveillance Court
FISUR	Physical Surveillance
FLIR	Forward-looking Infrared
FOUO	For Official Use Only
FRCivP	Federal Rules of Civil Procedure
FRCP	Federal Rules of Criminal Procedure
[redacted]	[redacted] b7E

FY	Fiscal Year
FYI	For Your Information
GETA	Government Employees Training Act
GFI	Ground Fault Interrupt
[redacted]	[redacted] b7E
HR	House of Representatives
HSC	Homeland Security Council
HSPD	Homeland Security Presidential Directive
[redacted]	[redacted] b7E
IA	Intelligence Analyst
IAT	Investigative Assistance or Technique
IB	Intelligence Bulletin
IC	Intelligence Community
IC-IRC	Intelligence Community Incident Response Center
IC3	Internet Crime Complaint Center
ICAC	Internet Crimes Against Children
ICE	Bureau of Immigration and Customs Enforcement
ICS	Internet Crime Specialist
IICMS	Innocent Images Case Management System
IIITF	Innocent Images International Task Force
IINI	Innocent Images National Initiative
IINIU	Innocent Images National Initiative Unit
IIOU	Innocent Images Operations Unit

b7E

IIU	Innocent Images Unit
ILB	Investigative Law Branch
ILU	Investigative Law Unit
IMA	InfraGard® Members Alliance
INMA	InfraGard® National Members Alliance
INTERPOL	International Criminal Police Organization
IOB	Intelligence Oversight Board
IOC	Information Operations Center
IOC2	International Organized Crime Intelligence and Operations Center
IOD	International Operations Division
IOG	Information Operations Group
IP	Internet Protocol
IPR	Intellectual Property Rights
IPRU	Intellectual Property Rights Unit
IRC	Internet Relay Chat
IT	Information Technology
JTF-GNO	Joint Task Force for Global Network Operations
JWICS	Joint Worldwide Intelligence Communications System
LE	Law Enforcement
LEA	Law Enforcement Agency
Legat	Legal Attaché
LES	Law Enforcement Sensitive
LHM	Letterhead Memorandum

LND	Special Agent Liaison Officer
LNO	Liaison Officers
LSU	Louisiana State University
MAOP	Manual of Administrative Operations and Procedures
MIOG	Manual of Investigative Operations and Guidelines
MLAT	Mutual Legal Assistance Treaty
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPA	Management and Program Analyst
MSIN	Mobile Station Identification Number
NAFTA	North American Free Trade Association
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Agreement
NCAVC	National Center for the Analysis of Violent Crime
NCC	National Coordination Center
NCIC	National Crime Information Center
NCFTA	National Cyber Forensic and Training Alliance
NCIJTF	National Cyber Investigative Joint Task Force
NCMEC	National Center for Missing & Exploited Children
[redacted]	[redacted]
[redacted]	[redacted]
NCSD	National Cyber Security Division
NCTAUS	National Commission on Terrorist Attacks upon the United States
NCTC	National Counterterrorism Center

b7E

b7E

NISS	National Information Sharing Strategy
NOFORN	Not Releasable to Foreign Nationals
Non-USPER	Non-United States Citizen
NSA	National Security Agency
NSB	National Security Branch
NSD	National Security Division, DOJ
NSIS	National Security Information Security
NSL	National Security Letter
NSLB	National Security Law Branch
NSPD	National Security Presidential Directive
NTOC	National Threat Operations Center
NW3C	National White Collar Crime Center
OCE	Online Covert Employee
OCRS	Organized Crime and Racketeering Section
OCONUS	Outside Continental United States
OEM	Original Equipment Manufacturer
OGC	Office of the General Counsel
OI	Office of Intelligence, DOJ NSD
OIA	Otherwise Illegal Activity

OIC	Office of Integrity and Compliance
OIG	Office of the Inspector General
OIO	Office of International Operations (obsolete, see IOD)
OO	Office of Origin
OTD	Operational Technology Division
P.L.	Public Law
P2P	Peer-to-Peer (networking, file-sharing)
PAO	Public Affairs Officer
PAR	Performance Appraisal Report
PCLU	Privacy and Civil Liberties Unit
PD	Presidential Directive
PDD	Presidential Decision Directive
PDF	Portable Document Format
PG	Policy Implementation Guide
PGP	Pretty Good Privacy
PI	Preliminary Investigation
PI	Predicated Investigation
PII	Personally Identifiable Information
PIOB	Presidential Intelligence Oversight Board
PM	Program Manager
PMR	Program Management Review

b7E

POC	Point of Contact
PPAU	Public/Private Alliance Unit
PR	Pen Register
PR/TT	Pen Register/Trap and Trace
PROPIN	Proprietary Information
PSA	Public Service Announcement
RA	Resident Agency
RCAT	Regional Cyber Action Team
RCS	Remote Computing Service
REL	Releasable
RF	Radio Frequency
RFA	Request for Assistance and/or Information
RFII	Request for Investigative Information
RFPA	Right to Financial Privacy Act
RH	Restricted Handling
RICO	Racketeer Influenced and Corrupt Organizations (Act)
RMD	Records Management Division
(S)	Secret
SA	Special Agent
SAC	Special Agent in Charge
SAR	Suspicious Activity Report
SBP	Subpoena Sub-file
SC	Section Chief
SCADA	Department of Homeland Security's Industrial Control Systems

SCI	Sensitive Compartmentalized Information
SCION	Sensitive Compartmentalized Information Operational Network
SEG	Strategic Exploitation Group
SIA	Supervisory Intelligence Analyst
[redacted]	b7E
SIM	Sensitive Investigative Matter
SIPRNET	Security Intelligence Protocol Router Network
SIR	Situational Intelligence Report
SME	Subject Matter Expert
SMTJ	Special Maritime and Territorial Jurisdiction
SOG	Special Operations Group
SORC	Sensitive Operations Review Committee
SPM	Security Program Manager
SSA	Supervisory Special Agent
SSG	Special Surveillance Group
SSRA	Supervisory Senior Resident Agent
STAO	Special Technologies and Applications Office (obsolete)
TA	Technical Advisor
TFC	Threat Focus Cell
TFI	Threat Focus Initiative
TFU	Threat Focus Unit
TFO	Task Force Officer
TMD	Technical Management Database
TNII	Threat to the National Information Infrastructure

TRIPS	WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights
(TS)	Top Secret
TT	Trap and Trace
TTA	Technically Trained Agent
TTP	Tactics, Techniques, and Procedures
(U)	Unclassified
U.S.	United States
USAM	U.S. Attorney's Manual
U.S.C.	United States Code
UACB	Unless Advised to the Contrary by the Bureau
[redacted]	[redacted]
UCFN	Universal Case File Number
[redacted]	[redacted]
UDP	Undisclosed Participation
UNET	Unclassified Network
URL	Uniform Resource Locator
USA	United States Attorney
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
USAO	United States Attorney's Office

b7E

US-CERT	United States Computer Emergency Readiness Team
USG	United States Government
USIC	United States Intelligence Community
USMS	United States Marshals Service
[redacted]	[redacted] b7E
USP	U.S. Person; USPER
USPA IRA	USA PATRIOT Act Improvement and Reauthorization Act
USPS	United States Postal Service
USPTO	U.S. Patent and Trademark Office
USSS	United States Secret Service
[redacted]	[redacted] b7E
VPN	Virtual Private Network
WCC	White Collar Crime
WIPO	World Intellectual Property Organization
[redacted]	[redacted] b7E
WL	Watch List
WMD	Weapons of Mass Destruction
WTO	World Trade Organization