



Homeland Security Investigations

Child Sexual Exploitation Investigations Handbook

HSI HB 20-07 / November 24, 2020



U.S. Immigration
and Customs
Enforcement

Foreword

The Child Sexual Exploitation Investigations Handbook provides a uniform source of national policies, procedures, responsibilities, guidelines, and controls that should be followed by U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agents and Criminal Analysts when conducting or assisting in investigations relating to the sexual exploitation of children. This Handbook contains instructions and guidance that will help ensure uniformity and operational consistency across all HSI field offices. Oversight over the National Child Sexual Exploitation Investigations Program resides with the Unit Chief, Child Exploitation Investigations Unit.

This Handbook supersedes the Child Sexual Exploitation Investigations Handbook (HSI HB 12-05), dated November 19, 2012.

The Child Sexual Exploitation Investigations Handbook is an internal policy of HSI. It is not intended, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter, nor are any limitations hereby placed on otherwise lawful enforcement prerogatives of ICE. This Handbook is For Official Use Only (FOUO) – Law Enforcement Sensitive. It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security policy relating to FOUO information and the ICE Directive on Safeguarding Law Enforcement Sensitive Information. This information shall not be distributed beyond the original addressees without prior authorization of the originator. If disclosure of this Handbook or any portion of it is demanded in any judicial or administrative proceeding, the HSI Information Disclosure Unit, as well as the ICE Office of the Principal Legal Advisor and/or the appropriate U.S. Attorney’s Office, are to be consulted so that measures can be taken to invoke privileges against disclosure. This Handbook contains information which may be exempt from disclosure to the public under the Freedom of Information Act, Title 5, United States Code, Section 552(b), and protected from disclosure in civil discovery. Any further request for disclosure of this Handbook or information contained herein should be referred to the HSI Information Disclosure Unit.

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

Alysa D. Eriks (for)

Derek N. Benner
Executive Associate Director
Homeland Security Investigations

11/24/20

Date

CHILD SEXUAL EXPLOITATION INVESTIGATIONS HANDBOOK

Table of Contents

Chapter 1. PURPOSE AND SCOPE.....	1
Chapter 2. INTRODUCTION.....	1
• 2.1 Child Sexual Abuse Material	1
• 2.2 Transnational Child Sex Offenders.....	2
Chapter 3. DEFINITIONS.....	2
• 3.1 Child Erotica	2
• 3.2 Child Molester	2
• 3.3 Child Pornography/Child Sexual Abuse Material	3
• 3.4 Child Sexual Abuse.....	3
• 3.5 Child Sexual Exploitation	3
• 3.6 Coercion.....	3
• 3.7 Commercial Sex Act.....	3
• 3.8 Computer Forensics Agents and Computer Forensics Analysts.....	3
• 3.9 Forensic Interview	3
• 3.10 Forensic Interviewers.....	4
• 3.11 HERO Corps Interns	4
• 3.12 Lascivious Exhibition	4
• 3.13 Minor.....	4
• 3.14 Morphing.....	5
• 3.15 Pedophile.....	5
• 3.16 Pedophilia Disorder	5
• 3.17 Sexually Explicit Conduct	5
• 3.18 Transborder	5
• 3.19 Transnational Child Sex Offender	5
• 3.20 Victim Assistance Specialist.....	6
• 3.21 Visual Depiction	6
Chapter 4. AUTHORITIES/REFERENCES	7
• 4.1 Authorities.....	7
• 4.2 References.....	8

Chapter 5. RESPONSIBILITIES	10
• 5.1 Executive Associate Director, Homeland Security Investigations	10
• 5.2 Assistant Director, Operational Technology and Cyber Division	10
• 5.3 Deputy Assistant Director, Cyber Crimes Center	10
• 5.4 Unit Chief, Child Exploitation Investigations Unit	10
• 5.5 Special Agents in Charge, Assistant Special Agents in Charge, and Resident Agents in Charge.....	10
• 5.6 Attachés.....	10
• 5.7 Criminal Analysts	10
• 5.8 Computer Forensics Agents and Computer Forensics Analysts.....	11
• 5.9 Special Agents, Criminal Analysts, and Foreign Service National Investigators.....	11
Chapter 6. HOW TO OBTAIN ELECTRONIC EVIDENCE.....	11
• 6.1 Preservation Letter	11
• 6.2 19 U.S.C. § 1509 Summons.....	11
• 6.3 Administrative Subpoena.....	13
• 6.4 Grand Jury Subpoena.....	13
• 6.5 Search Warrant.....	14
• 6.6 (b) (7)(E)	14
• 6.7 Border Search.....	14
• 6.8 (b) (7)(E)	15
Chapter 7. GUIDELINES FOR SEARCHING AND SEIZING DIGITAL DEVICES.....	16
Chapter 8. JURISDICTIONAL RESPONSIBILITY	16
• 8.1 Transborder Investigations.....	16
• 8.2 Domestic Investigations.....	16
• 8.3 HSI’s Role in Child Sexual Exploitation Investigations.....	17
Chapter 9. CHILD SEXUAL EXPLOITATION INVESTIGATIONS	18
• 9.1 Collection of Child Sexual Abuse Material	18
• 9.2 Transnational Child Sex Offenders.....	19
• 9.3 Search Warrants in Child Sexual Exploitation Cases	20
• 9.3.1 Physical Border Importation of Child Sexual Abuse Material	20
• 9.3.2 Internet Importations of Child Sexual Abuse Material.....	21
• 9.3.3 Affidavit Considerations	21
• 9.4 Online Investigative Principles	23
• 9.5 (b) (7)(E)	25

- 9.6 Interviewing and Defenses.....25
- 9.6.1 Interviewing Child Victims.....25
- 9.6.2 Interviewing Suspects26
- 9.7 Polygraph Examinations27
- 9.8 Transmission of Child Sexual Abuse Material28
- 9.9 Protocol for the Publication of Child Victims of Sexual Abuse29
- 9.10 Use of an Anatomically Life-Like Investigative Apparatus31
- 9.10.1 History of (b) (7)(E) Policy32
- 9.10.2 (b) (7)(E) Policy32
- 9.10.3 Approval of (b) (7)(E) Images33
- 9.10.4 Protocols for the Use of (b) (7)(E) Images34
- 9.10.5 Qualifications to Use (b) (7)(E) Images36
- 9.10.6 Deconfliction of (b) (7)(E) Images36
- 9.10.7 Documentation/Report of Use of (b) (7)(E) Images37
- 9.10.8 Disclosure of (b) (7)(E) Information37

Chapter 10. MANAGEMENT OF CHILD EXPLOITATION CASES38

- 10.1 National Center for Missing and Exploited Children38
- 10.2 NCMEC Virtual Private Network Leads to Attaché Offices.....39
- 10.3 Utilization of (b) (7)(E) Case Categories and Program Codes39
- 10.4 Child Exploitation Investigations Unit, Programs, and Intake Section40
- 10.5 Mandatory Identified Victim Reporting40
- 10.6 New Victim Identification Report of Investigation in (b) (7)(E)42
- 10.7 Internet Crimes Against Children Task Forces.....42
- 10.8 (b) (7)(E) Images42
- 10.9 U.S. Postal Inspection Service43
- 10.10 National Child Exploitation Material Library.....43
- 10.11 (b) (7)(E)43
- 10.12 (b) (7)(E)44
- 10.13 HSI Tip-line Unit Assistance44

Chapter 11. ANGEL WATCH CENTER44

- 11.1 (b) (7)(E)45
- 11.2 Notifications.....45
- 11.3 Coordination45
- 11.4 IML Criteria46

Chapter 12. VICTIM IDENTIFICATION AND NCMEC IMAGE SUBMISSION.....46

- 12.1 Victim Identification46
- 12.2 Victim Identification Program47

- 12.3 NCMEC Image and Video Submission (b) (7)(E)49
- 12.4 Child Pornography Notification Preference Form.....49

Chapter 13. AWARENESS AND RESILIENCE MENTORING FOR OPERATIONAL READINESS (b) (7)(E) PROGRAM.....49

- 13.1 Purpose.....50
- 13.2 Process50
- 13.3 Safeguards.....50
- 13.4 Objectives51
- 13.5 Mechanism.....51

Chapter 14. OUTREACH PROGRAM.....52

- 14.1 (b) (7)(E)52
- 14.2 (b) (7)(E)52

APPENDICES

Appendix A Interview Questions for Computer-Related Child Sexual Exploitation Investigations A-i

Appendix B Acronyms..... B-i

CHILD SEXUAL EXPLOITATION INVESTIGATIONS HANDBOOK

Chapter 1. PURPOSE AND SCOPE

The Child Sexual Exploitation Investigations Handbook establishes policies and procedures for U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agents (SAs) and Criminal Analysts (CAs) when conducting or assisting in investigations relating to the sexual exploitation of children.

Chapter 2. INTRODUCTION

Children of all ages, including infants, are being abused sexually all over the world. The Child Exploitation Investigations Unit (CEIU) at the HSI Cyber Crimes Center (C3) leads HSI's efforts to counteract the increase in child sexual exploitation by focusing its investigative efforts on child sexual exploitation material and transnational child sex offender (TCSO) (defined in Section 3.19) violations, many of which are facilitated by the internet. CEIU also works with HSI Attachés worldwide who partner with foreign law enforcement agencies to facilitate and support international investigations related to the sexual exploitation of children.

Coordination between HSI, state, local, and other federal agencies and non-governmental organizations (NGOs) is essential for combatting all aspects of child exploitation. CEIU is responsible for coordinating all of HSI's programs and resources that are dedicated to combatting the sexual exploitation of children. This central coordination and oversight allow for the creation and implementation of uniform policies and practices within HSI. CEIU investigates the sexual exploitation of children, both as facilitated through the advertisement, production, and distribution of Child Sexual Abuse Material, and by TCSOs.

2.1 Child Sexual Abuse Material

The production of Child Sexual Abuse Material (CSAM) requires that the sexual exploitation of an actual child, including the image of a real child being cropped and placed into a sexually explicit image, be recorded on video, film, digital media, or other method; the resulting images become the permanent record of the sexual abuse of an actual child. There is no way to produce child sexual abuse material except by victimizing a child. The Supreme Court has held that child pornography (legal definition) is child abuse and is not entitled to the First Amendment protection of freedom of speech. *See New York v. Ferber*, 458 U.S. 747 (1982). CSAM is produced primarily for consumption by preferential child molesters (defined in Section 3.2), pedophiles (defined in Section 3.15), and private and commercial collectors and distributors. Without the demand created by this market, there would be little CSAM.

2.2 Transnational Child Sex Offenders

In addition to investigating CSAM cases, HSI conducts investigations involving TCSOs. TCSOs are a pervasive international problem. Child sexual offenses committed by TCSOs are often conducted through diverse and evolving networks that exploit the most innocent and vulnerable members of society. TCSOs are part of an international industry that thrives in countries that lack laws to protect minors and often have weak law enforcement to effectively prosecute TCSOs.

TCSOs travel to destinations known for leniency regarding illegal child sex trade practices to seek anonymity while engaging in child molestation and exploitation, involving such acts as prostitution and manufacturing pornography. TCSOs who are U.S. citizens or lawful permanent residents can be found in a wide range of foreign locations looking to exploit children made vulnerable by poverty and deprivation. These individuals often have a long history of abusing children in both domestic and foreign locations. They plan their trips carefully to minimize their risk of arrest. TCSOs use impoverished countries as their exploitative playgrounds and they do so because they feel they can act with impunity. The internet and social media have facilitated and provide TCSOs with an abundance of sources of information to utilize and share.

Chapter 3. DEFINITIONS

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

3.1 Child Erotica

Child erotica is material involving minors that does not rise to the level of CSAM because it does not involve sexually explicit conduct but is used for the purpose of sexual arousal or gratification by an individual. Some examples of child erotica include books about children, nudist children magazines, images depicting children in lingerie, fantasy writings, diaries, sexually suggestive photographs of children, psychological books on pedophilia, drawings, etc. Generally, possession and distribution of child erotica do not constitute a violation of law, but they can provide reasonable suspicion to further the investigation.

3.2 Child Molester

A child molester is an adult who engages in any type of sexual activity with individuals legally defined as children. Child molesters are divided in two categories: situational and preferential. The situational child molester does not have a true sexual preference for children but engages in sex with children because of availability. The preferential child molester has a definite sexual proclivity for children. Sexual fantasies and erotic imagery of children are motivating factors for their sexual behavior. This type of offender would most appropriately be referred to as a pedophile. (See Section 3.15 and Kenneth V. Lanning, Child Molesters: A Behavioral Analysis, National Center for Missing & Exploited Children (5th ed. 2010)).

3.3 Child Pornography/Child Sexual Abuse Material

Child pornography or child sexual abuse material is the visual depiction of persons under 18 years of age who have been made to engage in sexually explicit activity (actual or simulated), including sexual intercourse, bestiality, masturbation, sadistic or masochistic abuse, or lascivious exhibition of the genitals or pubic areas of any person.

3.4 Child Sexual Abuse

Child sexual abuse involves contacts or interactions by adults with a child when the child is used for the sexual stimulation of the adult or another person. Child sexual abuse may also be committed by a person under the age of 18 when that person is either significantly older than the victim or is in a position of power or control over the child.

3.5 Child Sexual Exploitation

Child sexual exploitation is a summary term, generally encompassing the following four categories: 1) the physical molestation of children, 2) child prostitution, 3) transportation for illegal sexual activity, and 4) CSAM, but may also include other crimes against children of a sexual nature.

3.6 Coercion

Coercion involves threats of serious harm to or physical restraint against any person; any scheme, plan, or pattern intended to cause a person to believe that failure to perform an act would result in serious harm to or physical restraint against any person; or the abuse or threatened abuse of law or the legal process.

3.7 Commercial Sex Act

A commercial sex act is defined as any sex act on account of which anything of value is given or received by any person.

3.8 Computer Forensics Agents and Computer Forensics Analysts

All Computer Forensics Agents (General Schedule (GS)-1811 series) and Computer Forensics Analysts (GS-1801 series), for the purpose of this Handbook both known as (CFAs), have the requisite training and experience in the collection and analysis of computer-based evidence. These individuals are designated by the C3 Computer Forensics Unit.

3.9 Forensic Interview

A forensic interview is an investigative interview conducted by a forensic interview specialist (FIS) who has been trained in conducting interviews of victims/witnesses of all ages. A forensic interview is a fact-finding interview that is designed to elicit accurate and complete information in an investigation, which the SA will document in an ROI, (b) (7)(E)

(b) (7)(E)

3.10 Forensic Interviewers

In every SAC office, HSI employs Forensic Interview Specialists (FISs) who are subject matter experts and use non-leading, developmentally appropriate, and victim sensitive interview techniques. SAs should consult HSI FISs and VASs each time minors are encountered in an investigation. A forensic interview can be used with victims and witnesses of all ages, including adults with histories of chronic abuse and those with disabilities. FISs work with SAs in both domestic and international offices. FISs should work collaboratively with SAs and VASs as integral members of the investigative team. (See ICE Directive 10071.1, "Victim Assistance Program," dated August 25, 2011, or as updated, for information regarding the HSI Victim Assistance Program (VAP)).

3.11 HERO Corps Interns

In 2013, HSI established the Human Exploitation Rescue Operative (HERO) Corps. The purpose of the HERO Corps is to recruit and train wounded, ill, or injured active duty service members, transitioning active duty service members and military veterans for employment to support law enforcement in the areas of child exploitation investigations, child victim identifications, TCSOs, and digital forensics. All HERO Corps interns receive the same training, equipment, and certifications as all other CFAs employed by HSI. During the course of the internship, HERO Corps interns have the same latitude to conduct computer forensic analysis and computer forensic previews in the field as full time CFAs. (b) (7)(E)

3.12 Lascivious Exhibition

(b) (7)(E)

3.13 Minor

Under federal criminal law, a minor is any person under the age of 18.

3.14 Morphing

Morphing is the digital manipulation of an image.

3.15 Pedophile

A pedophile is one who is afflicted with pedophilia disorder.

3.16 Pedophilia Disorder

Pedophilia disorder involves adult sexual activity with a prepubescent child. The American Psychiatric Association diagnostic criteria for a person with pedophilia disorder are provided in its Diagnostic and Statistical Manual of Mental Disorders (DSM-5) and include the following: A) Over a period of at least six months, recurrent, intense sexually arousing fantasies, sexual urges, or behaviors involving sexual activity with a prepubescent child or children (generally 13 years old or younger); B) The person has acted on these sexual urges, or the sexual urges or fantasies cause marked distress or interpersonal difficulty; and C) The person is at least 16 years of age and at least 5 years older than the child or children in Criterion A. (Note: This does not include an individual in late adolescence involved in an ongoing sexual relationship with a 12- or 13-year-old.)

In order for pedophilia to be classified as a mental condition, a person must feel personal distress about his or her interest, or have a sexual desire or behavior that involves another person's psychological distress, injury, or death, or a desire for sexual behaviors involving unwilling persons or persons unable to give legal consent.

3.17 Sexually Explicit Conduct

Sexually explicit conduct is actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.

3.18 Transborder

A transborder nexus equates to an international nexus. Transborder does not refer to interstate nexus.

3.19 Transnational Child Sex Offender

A transnational child sex offender (TCSO) is a person who travels in interstate commerce or travels into the United States or its territories, or a United States citizen or an alien admitted for permanent residence in the United States who travels in foreign commerce with intent to engage in any illicit sexual conduct with a person under 18 years of age (minor).

3.20 Victim Assistance Specialist

HSI employs victim assistance specialists (VAS) who are subject matter experts on victimization issues in the context of criminal investigations and carry out victim assistance responsibilities on a full-time basis for a SAC office. VASs should work collaboratively with SAs and FISs as integral members of the investigative team. VASs are responsible for working with SAs to integrate victim assistance throughout the full lifecycle of HSI investigations. SAs should consult with their office's VAS as soon as possible if an investigation has the potential to identify victims. VASs play a central role in stabilizing the victim by assessing victims' needs, ensuring that victims are informed of their rights and understand the victim notification preference, providing access to resources, and crisis response. (See ICE Directive 10071.1, "Victim Assistance Program," dated August 25, 2011, or as updated, for information on the HSI VAP.)

3.21 Visual Depiction

A visual depiction includes developed and undeveloped film, videotape, and data stored on computer disk or electronic means that are capable of conversion into a visual image. A visual depiction can also include printed material, such as commercial magazines and printed copies of digital images.

(b) (7) (E)

This guidance shall be separate and apart from the policy addressed in section 9.10 which defines the creation and use of [REDACTED] images.

Chapter 4. AUTHORITIES/REFERENCES

4.1 Authorities

The primary federal statutes in relation to and defining child pornography and sex trafficking are Title 18, United States Code (U.S.C.), Sections 2251-2260 and 18 U.S.C. §§ 2421-2427. Additionally, 18 U.S.C. § 1470 governs the transfer of obscene materials to minors. 18 U.S.C. § 2258A specifically mandates the reporting of child pornography by electronic communication service providers. SAs should also be aware that 18 U.S.C. §§ 2251-2260 and 2421-2424 are predicate offenses for the Money Laundering Control Act and that asset forfeiture is a viable investigative technique in these cases.

The following statutes and case law are specific to child sexual exploitation matters:

- A. 18 U.S.C. § 1590, Trafficking with respect to peonage, slavery, involuntary servitude, or forced labor.
- B. 18 U.S.C. § 1591, Sex trafficking of children or by force, fraud, or coercion.
- C. 18 U.S.C. § 1592, Unlawful conduct with respect to documents in furtherance of trafficking, peonage, slavery, involuntary servitude, or forced labor.
- D. 18 U.S.C. § 2251, Sexual exploitation of children.
- E. 18 U.S.C. § 2252, Certain activities relating to material involving the sexual exploitation of minors.
- F. 18 U.S.C. § 2256, Definitions for chapter.
- G. 18 U.S.C. § 2421, Transportation generally.
- H. 18 U.S.C. § 2422, Coercion and enticement.
- I. 18 U.S.C. § 2423, Transportation of minors.
- J. 18 U.S.C. § 3509, Child victims' and child witnesses' rights.
- K. 18 U.S.C. § 2703, Required disclosure of customer communications or records.
- L. 22 U.S.C. § 212b, International Megan's Law to Prevent Child Exploitation and Other Sexual Crimes Through Advanced Notification of Traveling Sex Offenders (IML) (2017).
- M. The Adam Walsh Child Protection and Safety Act of 2006, Pub. L. No. 109-248, 120 Stat. 587 (2006).

- N. Money Laundering Control Act of 1986, Pub. L. No. 99-570, 100 Stat. 3207-18 & 3207-39 (1986).
- O. Electronics Communication Privacy Act (ECPA) of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).
- P. Child Protection Act of 1984, Pub. L. No. 98-292, 98 Stat. 204 (1984).
- Q. Privacy Protection Act of 1980, Pub. L. No. 96-440, 94 Stat. 1879 (1980).
- R. Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002).
- S. Oliver v. United States, 466 U.S. 170 (1984).
- T. New York v. Ferber, 458 U.S. 747 (1982).

(Note: The predecessor of 22 U.S.C. § 212b is IML (Pub. L. 114-119) (2016). 22 U.S.C. § 212b is the passport marking codification that followed IML.)

4.2 References

- A. Memorandum of Agreement between the ICE HSI Operational Technology and Cyber Division and the U.S. Marshals Service (USMS) National Sex Offender Targeting Center (NSOTC) Regarding International Megan’s Law (IML) to Prevent Child Exploitation and Other Sexual Crimes Through Advance Notification of Traveling Sex Offenders, signed by the last signatory on March 1, 2019.
- B. ICE Policy Number 10082.1, Use of Public and Non-Public Online Information, dated June 28, 2012, or as updated.
- C. ICE Directive 10044.1 (former number: 7-6.1), “Border Searches of Electronic Devices,” dated August 18, 2009, or as updated.
- D. ICE Directive 10071.1, Victim Assistance Program, dated August 25, 2011, or as updated.
- E. HSI Directive 18-03, ARMOR: The Child Exploitation Investigations Resilience Program, dated August 16, 2018, or as updated.
- F. Controlled Deliveries Handbook (HSI Handbook (HB) 19-02), dated September 27, 2019.
- G. Interviewing Techniques Handbook (HSI HB 17-04), dated May 10, 2017, or as updated.

- H. Polygraph Examinations Handbook (HSI HB 16-02), dated June 2, 2016, or as updated.
- I. Technical Operations Handbook (HSI HB 14-04), dated July 21, 2014, or as updated.
- J. Search and Seizure Handbook (HSI HB 12-04), dated September 14, 2012, or as updated.
- K. Cyber Crimes Investigations Handbook (HSI HB 11-03), dated August 9, 2011, or as updated.
- L. Computer Forensics Handbook (HSI HB 20-03), dated June 12, 2020, or as updated.
- M. Undercover Operations Handbook (Office of Investigations (OI) HB 08-04), dated April 14, 2008, or as updated.
- N. OI Memorandum, “Border Searches of Electronic Devices Directive,” dated August 31, 2009.
- O. Department of Justice (DOJ), Online Investigative Principles for Federal Law Enforcement Agents, dated November 1999, or as updated (which can be obtained from DOJ’s Computer Crimes & Intellectual Property Section.)
- P. Seized Asset Management and Enforcement Procedures Handbook (SAMEPH) (U.S. Customs and Border Protection (CBP) HB 4400-01B), dated July 2011, or as updated.
- Q. Kenneth V. Lanning, Child Molesters: A Behavioral Analysis, National Center for Missing & Exploited Children (5th ed. 2010), available at www.missingkids.com/en_US/publications/NC70.pdf.
- R. Eva J. Klein, Heather J. Davis & Holly A. Hicks, Child Pornography: The Criminal-Justice-System Response, American Bar Association Center and the Law for the National Center for Missing & Exploited Children (2001), available at <http://www.ncjrs.gov/App/Publications/abstract.aspx?ID=201355>.
- S. Diagnostic and Statistical Manual of Mental Disorders, (5th ed., text rev.; DSM-5 American Psychiatric Association, 2013).

Chapter 5. RESPONSIBILITIES

5.1 Executive Associate Director, Homeland Security Investigations

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

5.2 Assistant Director, Operational Technology and Cyber Division

The Assistant Director, Operational Technology and Cyber Division, has the overall responsibility for the implementation of the policies and procedures set forth in this Handbook.

5.3 Deputy Assistant Director, Cyber Crimes Center

The Deputy Assistant Director (DAD), C3, is responsible for the management and supervision of operations undertaken by or assigned to C3. The DAD, C3, is also responsible for establishing, maintaining, and maximizing inter- and intra-agency liaisons in the area of computer-based criminal activity as related to violations of laws and regulations, specifically relating to the sexual exploitation and/or victimization of children.

5.4 Unit Chief, Child Exploitation Investigations Unit

The CEIU Unit Chief is responsible for the investigative, analytical, policy, and planning resources in the area of child sexual exploitation and for the HSI Child Exploitation Program. The CEIU Unit Chief is also responsible for observing and checking the progress of all undercover operations relating to child sexual exploitation, managing Operation Predator (*see* Section 10.12) and Operation Angel Watch (*see* Chapter 11), and coordinating all child sexual exploitation investigations, including CSAM and TCSO investigations.

5.5 Special Agents in Charge, Assistant Special Agents in Charge, and Resident Agents in Charge

Special Agents in Charge (SACs) are responsible for implementing the provisions of this Handbook in their respective areas of responsibility (AORs). Additionally, each SAC, Assistant Special Agent in Charge, and Resident Agent in Charge will designate an HSI Group Supervisor or SA to serve as the Child Sexual Exploitation Coordinator.

5.6 Attachés

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

5.7 Criminal Analysts

CSAM Criminal Analysts are responsible for complying with the provisions of this Handbook.

5.8 Computer Forensics Agents and Computer Forensics Analysts

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

5.9 Special Agents, Criminal Analysts, and Foreign Service National Investigators

SAs and CAs, as well as Foreign Service National Investigators (FSNIs) assigned to HSI are responsible for complying with the provisions of this Handbook.

Chapter 6. HOW TO OBTAIN ELECTRONIC EVIDENCE

6.1 Preservation Letter

An 18 U.S.C. § 2703(f) letter, commonly referred to as a “Preservation Letter,” sent by a government entity, orders the system administrator of a wire or electronic communications provider to “take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other legal process.” The period of retention is 90 days, which may be extended for an additional 90-day period upon a renewed request by the government entity. This is only for information already possessed, not for future information. For the purposes of this Handbook, the “government entity” is any of the following: the CEIU Unit Chief, the Unit Chief of the Cyber Crimes Unit, the Unit Chief of the Computer Forensics Unit, or the SAC or his or her designee or the GS-15 Attaché or their designee.

Where the data records are physically maintained does not affect the preservation and delivery of those records. In 2018, the Supreme Court acknowledged, in *United States v. Microsoft Corporation* (2018, No. 17-2), that the 2018 Clarifying Lawful Overseas Use of Data (CLOUD) Act requires that under the provisions of 18 U.S.C. § 2703, a U.S. provider of email services must disclose to the Government electronic communications within its control even if the provider stores the communications abroad.

6.2 19 U.S.C. § 1509 Summons

Administrative Subpoena for Investigations Relating to Child Exploitation and Abuse Investigations, 18 U.S.C. § 3486(a)(1)(A)(i)(II), (a)(1)(C) - Source and Scope of Subpoena Authority under 18 U.S.C. § 3486(a): The Attorney General or the Attorney General’s designee is authorized under 18 U.S.C. § 3486(a) to issue administrative subpoenas for a limited category of information in criminal investigations of child pornography, sex abuse and transportation for illegal sexual activity offenses, where the victim was under 18. The underlying investigation must relate to an act or activity involving a violation of 18 U.S.C. §§ 1201, 2241(c), 2242, 22260, 2421, 2422, or 2423, when the victim was a minor who had not attained the age of 18.

Administrative subpoena power enables government investigators to bypass the Fourth Amendment's probable cause requirement to obtain private records.¹

A statute or conditions precedent to judicial enforcement, however, may require what the Constitution does not. Nevertheless, when asked if the Internal Revenue Service (holding that the standards set in *Powell* govern all administrative subpoenas²) must have probable cause before issuing a summons for the production of documents, the Court intoned the standard often repeated in response to an administrative subpoena challenge:

“Reading the statutes as we do, the Commissioner need not meet any standard of probable cause to obtain enforcement of his summons...He must show [1] that the investigation will be conducted pursuant to a legitimate purpose, [2] that the inquiry may be relevant to the purpose, [3] that the information sought is not already within the Commissioner’s possession, and [4] that the administrative steps required by the Code have been followed...This does not...mean that under no circumstances may the court inquire into the underlying reason for the examination. It is the court’s process which is invoked to enforce the administrative summons and a court may not permit its process to be abused,” *United States v. Powell*, 379 U.S. 48, 57-8 (1964)²

The 19 U.S.C. § 1509 summons, commonly referred to as the “Customs Summons,” is a broad summons that may be used in an HSI investigation or inquiry conducted for the purpose of ensuring compliance with the laws of the United States, as administered by HSI. With respect to obtaining records related to a child exploitation case, SAs may be authorized to use a 19 U.S.C. § 1509 summons in the course of an HSI investigation.

Telecommunication service providers are permitted to seek reimbursement for processing and responding to administrative summonses or subpoenas (*see* 18 U.S.C. § 2706(a)).

In child exploitation cases, the 19 U.S.C. § 1509 summons is used to obtain basic subscriber information from an electronic communications service provider, including the following:

- A. Name;
- B. Date of birth;
- C. Social Security number;
- D. Address;
- E. Local and long-distance telephone number associated with the account;

¹ Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities, Pursuant to Public Law 106-544 https://www.justice.gov/archive/olp/rpt_to_congress.htm#2a1

² *United States v. Powell*, 379 U.S. 48, 57 (1964) (rejecting probable cause as the standard governing Internal Revenue Service administrative subpoenas); *see SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 741-42 (1984) (holding that the standards set in *Powell* govern all administrative subpoenas) (<https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4078&context=flr>)

- F. Connection records or records of session times and duration;
- G. Beginning and ending dates of service;
- H. Types of service utilized;
- I. Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
- J. Means and sources of payment for such service (including any credit card and/or bank account number) rendered, pursuant to 19 U.S.C. § 1509(d)(1)(A)(ii).

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

(Note: For questions regarding the use of the 19 U.S.C. § 1509 Summons, SAs should contact the Office of the Principal Legal Advisor (OPLA)’s HSI Law Division (HSILD) at Headquarters (HQ) or their local OPLA field location).

6.3 Administrative Subpoena

Electronic Service Providers (ESPs) vary in their policies of disclosure of law enforcement legal process to their customers. As such, CEIU recommends that SAs apply for non-disclosure orders under 18 U.S.C. § 2705(b). Also, SAs will ensure that the subject line of an email submitted to an ESP shows: “Summons/Child Exploitation Investigation.” This subject line in an email prioritizes child exploitation-related subpoenas.

18 U.S.C. § 3486 provides administrative subpoena authority for child sexual exploitation investigations. The authority to issue this subpoena has been delegated to DOJ, including U.S. Attorneys and the Federal Bureau of Investigation (FBI). SAs must contact their local U.S. Attorney’s Office (USAO) to obtain a subpoena under this authority.

6.4 Grand Jury Subpoena

For electronic communication in storage for more than 180 days for opened email and for other account transactional data, a grand jury or administrative subpoena with notice to the subscriber is legally sufficient. (b) (7)(E)

6.5 Search Warrant

For electronic communications in storage for 180 days or less, SAs must obtain a search warrant. Search warrants can be used for any electronic communication. If probable cause has been established, this is the preferred method of obtaining electronic evidence (when seeking something other than subscriber information). (b) (7)(E)

(b) (7)(E)

6.7 Border Search

At the border (or its functional equivalent), HSI has broad authority to conduct routine searches of persons and things upon their entry into or exit out of the United States without first obtaining a warrant and without suspicion. This authority stems from a long-standing and well-recognized exception to the Fourth Amendment that is premised on the government's interest in protecting its citizens from the entry of persons and items harmful to U.S. interests. The U.S. Supreme Court has recognized that "searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." See *United States v. Ramsey*, 431 U.S. 606, 616 (1977).

In general, HSI does not distinguish between the search of documents and electronic devices and the search of any other items crossing the U.S. borders. With respect to the border search of electronic devices, federal courts, including the U.S. Court of Appeals for the Ninth Circuit, have concluded that searching documents, including those in electronic form, is well within the broad border search exception exercised by HSI and they have generally endorsed the view that laptop computers or other electronic devices are neither conceptually nor constitutionally different from other closed containers subject to less suspicious searches at the border. *See U.S. v. Arnold*, 523 F.3d 941 (9th Cir. 2008). The exercise of this plenary authority has been critical to ensuring national security at U.S. borders. *See United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (en banc); the panel held that manual cell phone searches may be conducted by border officials without reasonable suspicion but that forensic cell phone searches require reasonable suspicion. *See United States, Plaintiff-Appellee, v. Miguel Angel Cano, Defendant-Appellant*, (9th Cir. 2019). *See Anibowei v. Wolf*, No. 16-3495, 2020 WL 208818 (N.D. Tex. Jan. 14, 2020).

SAs should consult ICE Directive 10044.1 (former number: 7-6.1), “Border Searches of Electronic Devices,” dated August 18, 2009, or as updated; the HSI EAD Message, “Border Searches of Electronic Devices,” dated January 16, 2018; and the Search and Seizure Handbook (HSI HB 12-04), dated September 14, 2012, or as updated, for further direction on such searches.

As specified in ICE Directive 10044.1 (former number: 7-6.1), border searches of electronic devices must be conducted by HSI SAs or other properly authorized officers with customs border search authority, such as persons cross-designated as customs officers (e.g., task force officers (TFOs)) under 19 U.S.C. § 1401(i). At any point during a border search, SAs may detain electronic media or copies thereof for further review, either on-site or at an off-site location, including an associated demand for assistance from a third agency, pursuant to 19 U.S.C. § 507.

Authorities under the customs laws of the United States in no way limit authorities to search and retain evidence available to SAs under the Immigration and Nationality Act of 1965, as amended.

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

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Chapter 7. GUIDELINES FOR SEARCHING AND SEIZING DIGITAL DEVICES

Before preparing a warrant to search and seize a digital device, it is critical to determine the role of the device in the crime. (b) (7)(E)

SAs should refer to the Computer Forensics Handbook (HSI HB 11-01), dated April 27, 2011, or as updated, for specific guidance on searching and seizing a computer or computer-related equipment. SAs must also adhere to the SAMEPH (CBP HB 4400-01B), dated July 2011, or as updated, which details policy and procedures relating to computer searches and seizures. Additionally, SAs may consult the Search and Seizure Handbook (HSI HB 12-04), dated September 14, 2012, or as updated.

Chapter 8. JURISDICTIONAL RESPONSIBILITY

8.1 Transborder Investigations

HSI investigates transborder (defined in Section 3.18) violations of the Child Protection Act of 1984, which makes the transportation of minors for the purpose of producing CSAM and the trafficking of CSAM illegal. (b) (7)(E)

8.2 Domestic Investigations

Although HSI focuses on transborder violations, (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. This does not preclude HSI offices from disseminating and investigating leads developed during the course of other HSI investigations.

8.3 HSI's Role in Child Sexual Exploitation Investigations

As stated in Section 8.1, HSI is responsible for investigating the transborder violations of the Child Protection Act of 1984, as well as the illegal transportation of minors to engage in criminal sexual activity and travel to engage in a sexual act with a juvenile.

The examples below are provided for reference only; however, they are not all-encompassing of HSI's investigative jurisdiction. Questions related to HSI's child sexual exploitation investigative jurisdiction should be addressed to the CEIU Unit Chief.

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

[Redacted]

[Redacted]

[Redacted]

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

[Redacted]

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

[Redacted]

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

[Redacted]

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

[REDACTED]

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

[REDACTED]

Chapter 9. CHILD SEXUAL EXPLOITATION INVESTIGATIONS

9.1 Collection of Child Sexual Abuse Material

A. There are four common categories of CSAM consumers (*see Klein, et al., Child Pornography: The Criminal-Justice-System Response*, American Bar Association Center and the Law for the National Center for Missing & Exploited Children (2001), page 5):

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

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

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

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

(b) (7)(E)

9.2 Transnational Child Sex Offenders

(b) (7)(E)

There are numerous NGOs that have identified international TCSOs as a global problem affecting both developed and developing countries.

Targets of TCSO investigations can include individual travelers who seek children on their own, individuals who procure children for others, and individuals who actively seek out travelers who may want to engage in sexual activity with children. TCSOs are often willing to travel to any country in the world, including the United States, to engage in illicit sexual conduct with minors.

(b) (7)(E)

HSI Attaché offices are vital to TCSO investigations because they facilitate HSI investigations in foreign locations and often originate these investigations. A successful (b) (7)(E)

[REDACTED]

9.3 Search Warrants in Child Sexual Exploitation Cases

Child sexual offenders protect and preserve their collections in different ways. They must first protect their collection from accidental erasure or equipment failure. (b) (7)(E)

(b) (7)(E)

9.3.1 Physical Border Importation of Child Sexual Abuse Material

Prior to the expansion of computer use, HSI CSAM investigations typically involved the seizure of actionable material which was imported into the United States. (b) (7)(E)

(b) (7)(E)

³ Exploring the Impact of Child Sex Offender Suicide, Hoffer, Shelton, Behnke, and Erdberg, November 2010

(b) (7)(E)

A. (b) (7)(E)

[REDACTED]

9.3.2 Internet Importations of Child Sexual Abuse Material

Sexual offenders – and others who commit crimes against children – long ago realized that digital technology provided the ability to produce illegal images of children; trade and share images of their own sexual exploits with like-minded people; and organize, maintain, and increase the size of their collections of CSAM. (b) (7)(E)

9.3.3 Affidavit Considerations

SAs should comply with the provisions of Section 6.5 of this Handbook and with the Search and Seizure Handbook (HSI HB 12-04), dated September 14, 2012, or as updated, when seeking a search warrant. In search warrants relating to the sexual exploitation of children, the possibility of suppression exists when legal guidelines are not properly followed. (b) (7)(E)

⁴ The National Strategy for Child Exploitation Prevention and Interdiction, U.S. Department of Justice, Apr. 2016, at <https://www.justice.gov/psc/file/842411/download> (last visited Nov. 16, 2018) (on file with the International Centre for Missing & Exploited Children).

A. Affiant expertise on CSAM warrants can be critical in establishing the scope of the items to be searched. (b) (7)(E)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

B. (b) (7)(E)

[Redacted]

C. (b) (7)(E)

[Redacted]

D. (b) (7)(E)

[Redacted]

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

E.

(b) (7)(E)

F. When there is evidence of ongoing child molestation, if the intended distributor or recipient of CSAM is a parent, legal guardian, or caretaker; resides in a home with children; or is involved with children or is in a position of trust, such as a school counselor, physician, coach, teacher, “big brother/big sister,” Boy or Girl Scout leader, law enforcement officer, or religious leader, appropriate enforcement action with relevant warrant(s) must be effected as soon as possible. (b) (7)(E)

[Redacted]

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

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

(b) (7) (E)

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

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

(b) (7)(E)

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

(b) (7)(E)

9.5

(b) (7)(E)

(b) (7)(E)

9.6 Interviewing and Defenses

(b) (7)(E)

9.6.1 Interviewing Child Victims

(b) (7)(E)

(b) (7) (E)

9.6.2 Interviewing Suspects

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

[Redacted text block]

[Redacted text block]

A. Denial

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

B. Minimization

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

C. Justification

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

D. Fabrication

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

(Note: Suggested suspect interview questions for use in computer-related child sexual exploitation investigations are provided in Appendix A.)

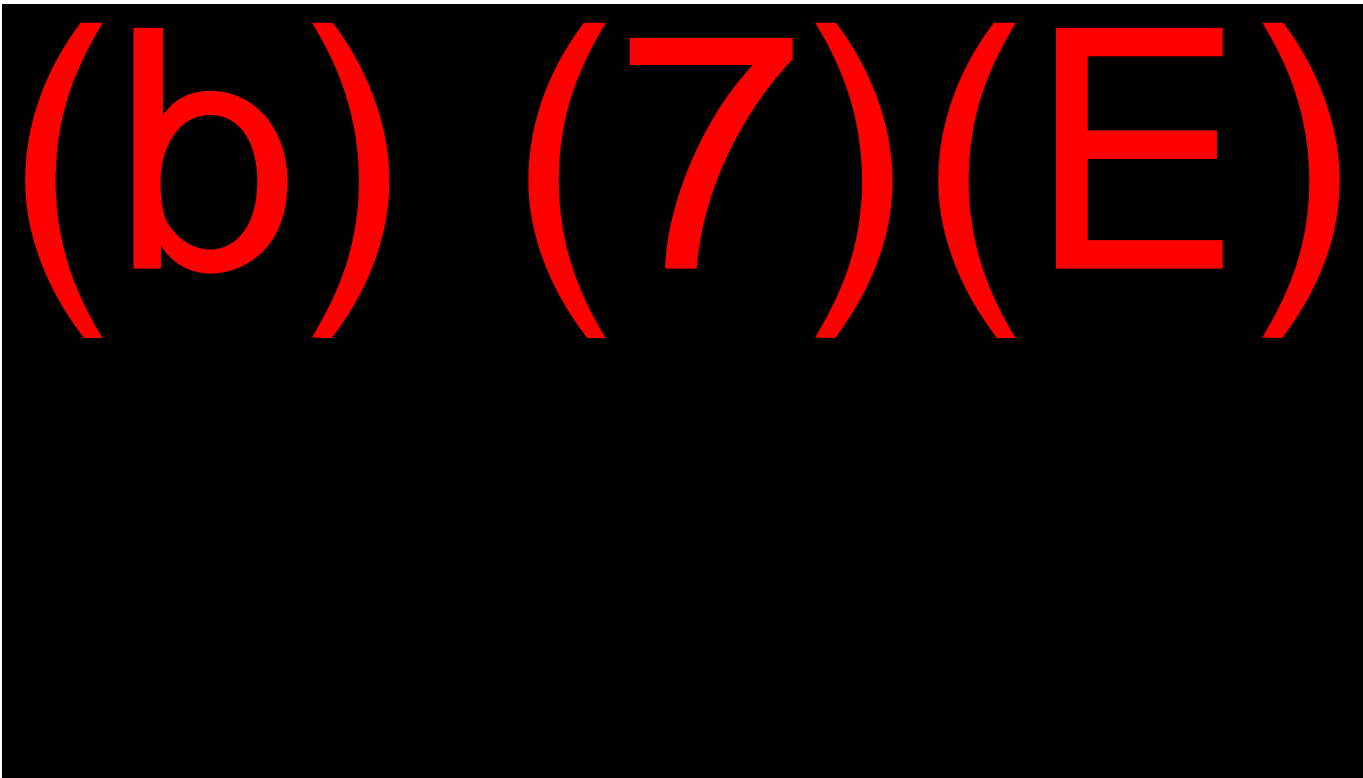
9.7 Polygraph Examinations

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

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

In cases where the transmission of original evidence is required, the evidence packet containing the CSAM will include a Custody Receipt for Seized Property and Evidence (Department of Homeland Security (DHS) Form 6051S) for tracking purposes. If the material being sent is not original evidence, a DHS Form 6051S is not required.

9.9 Protocol for the Publication of Child Victims of Sexual Abuse



With the guidance of its law enforcement committee, NCMEC has developed a similar policy for its organization. NCMEC also has resources that could assist HSI SAs with the HSI mandated preliminary steps, as described below:

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

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

[Redacted]

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

[Redacted]

[Redacted]

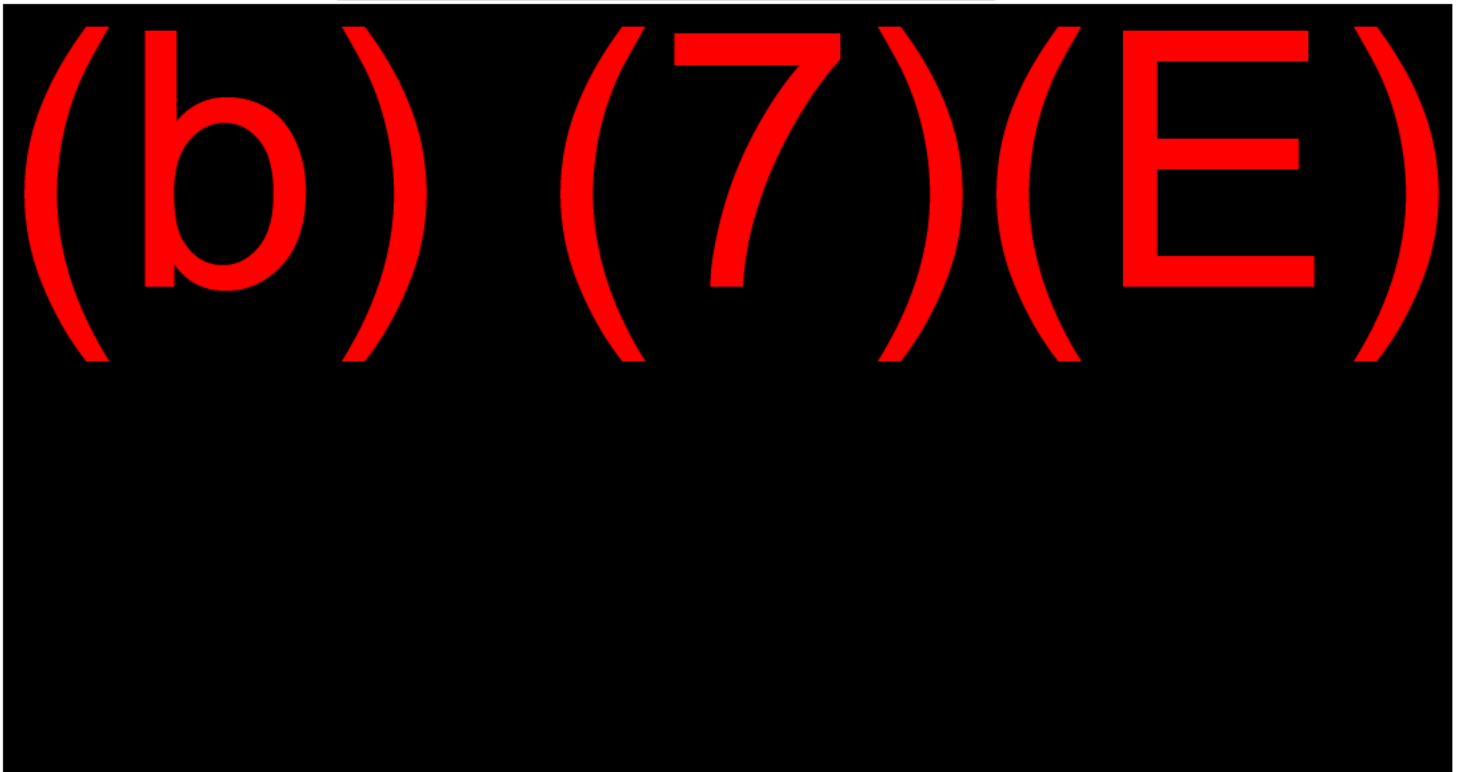
(b) (7) (E)

(b) (7)(E)

Step 4: Publication

Publishing will not occur through media outlets without prior approval from the C3 Division Chief, OPLA's HSILD (which will coordinate with OPLA's Government Information Law Division), and OPA. Images will be released to the media only through OPA. To protect the privacy of the victim, images are to be published without reference to the sexual nature of the crime (e.g., "Have you seen me?") and are to be altered so that the sexual content of the image is removed. While attempting to identify a victim, SAs shall not display any pornographic images. At all times, SAs shall take all necessary and reasonable precautions to protect the victim's dignity and privacy. It should be noted that ICE-originated images cannot be released by any other party to mainstream media outlets without the expressed written consent from the C3 Division Chief and certification that the release of the images has adhered to the provisions of this Handbook.

9.10 Use of an **(b) (7)(E)**



(b) (7) (E)

9.10.1 History of [REDACTED] Policy

[REDACTED]

9.10.2 [REDACTED] Policy

(b) (7) (E)

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

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

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

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

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

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

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

2) (b) (7)(E)

3) (b) (7)(E)

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

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E)
(b) (7)(E)

9.10.3 Approval of [Redacted]

(b) (7)(E)

B. C3 CEIU Approval Process

- 1) (b) (7)(E) [REDACTED]
- 2) The CEIU POC, CEIU Section Chiefs, and CEIU Unit Chief will promptly review [REDACTED] and its use. They will then notify the SA or TFO of the POC's decision to approve or disapprove use, including any limitations imposed.
- 3) All approved and disapproved [REDACTED] will be maintained by the CEIU POC.

C. Exigent Circumstances

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

2) (b) (7)(E)

3) (b) (7)(E)

9.10.4 Protocols for the Use of [REDACTED]

A. Use of [REDACTED] should be reserved for:

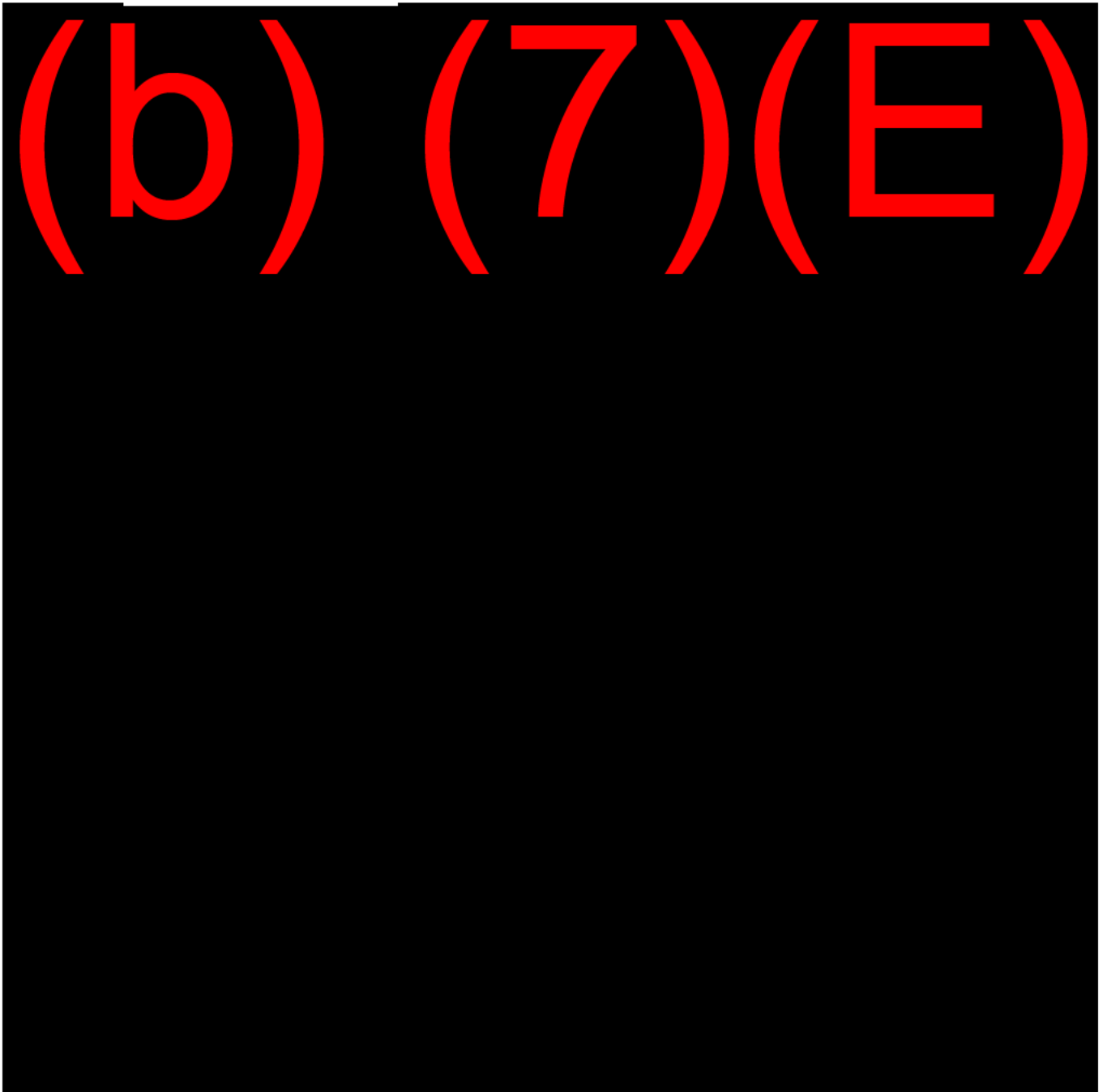
1) (b) (7)(E)

2) (b) (7)(E)

(b) (7)(E)

B. Non-Target Offenders

(b) (7)(E)



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

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

9.10.7 Documentation/Report of Use of [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(b) (7) (E)

9.10.8 Disclosure of [REDACTED]

(b) (7) (E)

Chapter 10. MANAGEMENT OF CHILD EXPLOITATION CASES

10.1 National Center for Missing and Exploited Children

HSI was one of the first federal law enforcement agencies to partner with NCMEC (Project Code (b) (7)(E) and become a POC for tips and leads from NCMEC. The public forwards these tips to NCMEC's toll free hotline which are then referred to HSI's CEIU. This working relationship began with the inception of the "Cyber-Tipline" in 1986 with what was originally known as the "Child Pornography Tipline, 1-800-THE-LOST." Tips from the public and law enforcement partners are also received 24 hours a day, 7 days a week by the HSI Tip-line Unit via (866) 347-2423, (800) BE-ALERT, and via the internet accessible HSI Tip Form located at www.ice.gov/tips.

CEIU has full-time liaison position(s) at NCMEC. CEIU's liaison/representative to NCMEC is responsible for the day-to-day interaction with NCMEC in support of cybertips with an international nexus, in support of NCMEC efforts relating to missing children and non-compliant Registered Sex Offenders, and for the receipt and processing of HSI requests for image analysis against the Child Recognition Identification System (CRIS) and newly identified victim submissions. All suspected images of CSAM must be forwarded to the CEIU liaison pursuant to Section 12.3 of this Handbook, who will forward them to NCMEC. NCMEC will provide a submitting SA with a Child Identification Report (CIR) with an assigned Technical Assistance (TA) number. The CIR lists the identified series and corresponding law enforcement POC for each image/series submitted in the SA's CRIS request.

NCMEC forwards CIRs created as a result of CRIS reviews to the requesting federal SA, and copies the FBI Office for Victim Assistance, Child Pornography Victim Assistance Program (CPVA). The CPVA then provides the requesting SA a Victim Information Report (VIR) based on the identified series found in each NCMEC CIR. The VIR is for use in federal prosecution only for the purpose of victim restitution. The VIR should be forwarded to the USAO/Victim-Witness Coordinator handling the SA's federal case. VIRs that contain victim information are to be distributed only to Federal entities and affiliated counterparts at the USAO. VIRs must be forwarded to the VAS so that they can enter the victim information in the Victim Notification System. The VIR includes information on the actual victim and/or guardian, with their notification preferences, and identifies which victim has a current Victim Impact Statement (VIS) on file and/or which victims want to submit a VIS and if they are asking for restitution. SAs and TFOs are prohibited from contacting the victim and/or guardian directly.

CEOS maintains and distributes the VIS on file for those series in which one was previously submitted.

(b) (7)(E)

(b) (7)(E)

SAs can also submit requests to NCMEC for deconfliction purposes. SAs can email NCMEC at (b) (7)(E) regarding email addresses, usernames, names, and phone numbers to determine if other law enforcement entities have queried NCMEC regarding the user(s) or if ESPs have reported the user(s). The HSI Liaison to NCMEC can assist with providing copies of NCMEC Cybertip reports to HSI SAs.

10.2 NCMEC Virtual Private Network Leads to Attaché Offices

If the HSI Attaché Office holds the Virtual Private Network (VPN), that Attaché Office will directly receive the cybertips from NCMEC. If the Attaché Office does not hold the VPN, the HSI NCMEC Liaison will receive the cybertips and those cybertips will be forwarded to that Attaché's OwnCloud account.

10.3 Utilization of (b) (7)(E) Case Categories and Program Codes

For case management purposes, HSI SAs must use (b) (7)(E) case category (b) (7)(E) when conducting (b) (7)(E) and (b) (7)(E) cases, (b) (7)(E) for pornography not related to children, and (b) (7)(E) for pornography related to animals, violence, and excretion not relating to children. Only (b) (7)(E), and (b) (7)(E) should be utilized as case categories for these types of investigations. The following Program/Project Codes must be utilized when entering Investigative Case Records ("Case Openings") into (b) (7)(E) and when entering (b) (7)(E) Incident Reports for "(b) (7)(E)" type cases. (b) (7)(E)

(b) (7)(E)

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

Close attention to these case categories and (b) (7)(E)
[Redacted text block]

(b) (7)(E)

10.4 Child Exploitation Investigations Unit, Programs, and Intake Section

CEIU has programmatic oversight within HSI and ICE regarding child exploitation investigations. In this role, CEIU provides support to HSI offices worldwide regarding ongoing investigations.

(b) (7)(E)

(b) (7)(E)

10.5 Mandatory Identified Victim Reporting

(b) (7)(E)

(b) (7)(E)

In addition to the Victim Reporting ROI, the completion of a (b) (7)(E) in the (b) (7)(E) for each instance when a victim is identified in the course of a child exploitation investigation is mandated by the HSI memorandum titled, Operational Reporting Requirements, dated May 20, 2014, or as updated.

Victims identified are required to be reported through both the Victim Reporting ROI and a (b) (7)(E) regardless of whether the suspect is charged with production of CSAM and regardless of whether prosecution of the case is accepted. Victims discovered during joint federal and/or task force cases should be reported only when HSI has been involved in the identification of, interview of, or has provided assistance to, the victims identified. The victims should be documented in a (b) (7)(E) and also reported to the local Victim-Witness Coordinator regardless of whether HSI provides services to the victims.

Victim identification (b) (7)(E) should include “identification of a victim” in the title and contain the following information for each victim reported:

- A. Date of identification;
- B. Sex of the victim;
- C. Current age of the victim;
- D. Age at the time of victimization (if different from the current age); and
- E. Victim’s initials or victim designator (i.e., (b) (7)(E))

Victim identification (b) (7)(E) should be filed by the office that interacts with the victim, including conducting and/or arranging for the victim to be interviewed or provided services. This should be the office closest to where the victim resides and may or may not be the office that originated the investigation through which the victim was discovered. Victims should be reported via a (b) (7)(E) within five to ten business days of positive identification. Multiple victims can be reported via a single (b) (7)(E) if they are identified within this period of time. Victim identification can be concurrently reported with other enforcement actions but should be noted in the title of the (b) (7)(E) along with the action taken.

10.6 New Victim Identification Report of Investigation in (b) (7)(E)

SAs are required to input a Victim Identification ROI for all victims identified in an HSI or a joint investigation. The mandatory requirements are below:

- A. All victims should be documented in a Victim Reporting ROI so that they will be included in the statistical count for each office.
- B. All child exploitation victims are also required to be documented via the submission of a SEN report. This remains an HSI reporting requirement and will be used for HSI leadership's visibility and informational purposes only. Victims who are reported in a SEN report but not documented in a Victim Reporting ROI will not be included in the annual victim statistics.
- C. Offices are also required to ensure that all information regarding victims identified or children rescued during investigations is supplied to their HSI Victim Assistance Specialist and/or Victim Assistance Coordinator for entry into the Victim Assistance Database.
- D. All victims should also be documented in a Newly Identified Child Victim submission to NCMEC.

10.7 Internet Crimes Against Children Task Forces

The ICAC task forces are composed of local, state, and federal law enforcement agencies that work together to combat internet-based or facilitated crimes that are committed against children. Each ICAC task force is led by a state or local law enforcement agency, many of which include participation from HSI SAs. The ICAC task forces are an excellent collaborative resource for HSI and maintain significant expertise in the child sexual exploitation investigative arena. ICAC resources include an extensive domestic investigative network, as well as training courses, such as online investigative methods and techniques that are available to HSI SAs who participate in an ICAC task force.

10.8 Innocent Images

Innocent Images is a nationwide FBI-sponsored initiative that is focused on the use of the internet to investigate and apprehend individuals who sexually exploit children. The program focuses on the production and distribution of CSAM, as well as on travelers who meet minors online and then travel interstate or internationally with the intent to engage in sexual activity with them.

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

10.9 U.S. Postal Inspection Service

HSI has a long-standing relationship with the U.S. Postal Inspection Service (USPIS) relating to investigative areas of mutual interest, including child sexual exploitation violations that are facilitated via intrastate, interstate, and foreign use of the U.S. mail system. HSI SAs are encouraged to continue their collaborative efforts in concert with USPIS and maintain close coordination and liaison with this important enforcement agency.

10.10 National Child Exploitation Material Library

All field offices are directed to forward seized CSAM magazines, other commercial hard copy printed materials, videotaped media, and celluloid motion picture films to CEIU. In addition, the HSI liaison at NCMEC forwards HSI New Victim Submission material to C3 for incorporation into the National Child Victim Identification System (NCVIS) upon completion of NCMEC analyses. The materials are available and utilized by law enforcement agencies worldwide for court use, training, and (b) (7)(E) operations.

10.11 (b) (7)(E)

(b) (7)(E)

[Redacted text block consisting of multiple lines of blacked-out content]

10.12 Operation Predator

In July 2003, ICE announced the launch of Operation Predator (OPPED), a coordinated and ongoing worldwide HSI law enforcement initiative that strives to protect children from pornographers, child prostitution rings, internet predators, alien smugglers, human traffickers, sex tourism operators, and other criminals who prey on children. OPPRED focuses on the identification, prosecution, and removal from the United States (when applicable) of criminals, and encompasses all the law enforcement authorities within ICE.

CEIU is responsible for developing, enhancing, coordinating, monitoring, reporting, and disseminating guidance, procedures, and policy for OPPRED. Also, OPPRED plays a critical role in managing the intake of information, evaluation, and reporting of significant events, incidents, and cases to ICE and external organizations.

10.13 HSI Tip-line Unit Assistance

The HSI Tip-line Unit is available to provide support 24 hours a day, 7 days a week to SAs and CAs with child exploitation investigations. The following assistance is available to HSI personnel by calling (866) 347-2423:

- A. Subjects, addresses, and businesses can be queried in more than 20 law enforcement and commercial databases (including (b) (7)(E) and [REDACTED]).
- B. (b) (7)(E) [REDACTED]
- C. (b) (7)(E) [REDACTED]
- D. The HSI Tip-line Unit will receive and compile all tips relating to a wanted poster including for “Jane/John Doe” warrants.

Chapter 11. ANGEL WATCH CENTER

The Angel Watch program functions to identify travelers convicted of child exploitation crimes. Flight manifests are cross referenced against the National Sex Offender Registry (NSOR) to ensure that a known sex offender is identified when traveling across international borders.

HSI and USMS entered into a Memorandum of Agreement between the ICE HSI Operational Technology and Cyber Division and USMS’s NSOTC Regarding International Megan’s Law (IML) to Prevent Child Exploitation and Other Sexual Crimes Through Advance Notification of Traveling Sex Offenders, signed by the last signatory on March 1, 2019.

Operation Angel Watch was created to identify and target individuals who have been convicted of sexual crimes against children and who are traveling in foreign commerce in an effort to:

- A. Reduce the risk of U.S. persons engaging in CST in foreign countries;
- B. Enable foreign countries to make fully informed decisions relating to admissibility, border inspections, surveillance or investigative measures, or any other action deemed appropriate; and
- C. Increase information sharing and encourage foreign countries to provide the United States with notifications when foreign nationals convicted of sexual crimes against children in their countries are traveling to the United States.

In support of its overall mission and in accordance with IML, HSI CEIU developed the Angel Watch Center (AWC), a robust partnership with CBP and USMS, to proactively identify and target convicted child sex offenders who are traveling to foreign countries.

11.1 Targeting

HSI CAs and CBP Officers utilize a variety of systems, including the (b) (7)(E)

[REDACTED]

11.2 Notifications

AWC disseminates notifications to HSI Attachés or CBP joint operations personnel in the traveler’s destination country for them to share with their appropriate foreign counterparts to utilize the information at their discretion. The notifications include the (b) (7)(E)

[REDACTED]

11.3 Coordination

AWC works onsite in partnership with the NSOTC. All notifications that are sent internationally are also sent to NSOTC personnel, who work closely with local law enforcement/sex offender registries to ensure that all traveling offenders comply with their local sex offender registration requirements and may pursue a federal criminal investigation on those who may be in violation.

AWC also works with the Department of State’s (DOS) Passport Office to identify offenders who lack the child sex offender endorsement on their current U.S. passport as required by IML. AWC sends a weekly submission to DOS with information for every child sex offender

identified through normal targeting operations who requires the passport endorsement but does not have it on his or her current document. DOS then revokes the current passport and advises the offender that he or she may apply for a new passport which would bear the endorsement. DOS will also provide information to AWC for offenders who self-report during the passport application process that they are required to have the endorsement. AWC will verify that the offender meets the IML criteria for the endorsement prior to the passport being issued. Only AWC can verify whether an offender is required to have a passport bearing the endorsement.

Passports bearing the endorsement will have either code **0100** (issued by a domestic office) or **011000** (issued by an international office) listed on the biographic data page of the document. The endorsement section in the back of the passport will bear the following statement:

(b) (7)(E)

11.4 IML Criteria

Per IML, the criteria for AWC to send foreign notification on a traveler is based on the traveler's conviction.

Per IML, the criteria for a sex offender to be issued a passport bearing the child sex offender endorsement is based on the conviction and sex offender registration requirements. Any sex offender convicted for any sexual offense involving a minor victim **and** who has a **current** duty to register as a sex offender in any U.S. jurisdiction is required to be issued a passport bearing the endorsement. Those who no longer have a duty to register in any U.S. jurisdiction are not required to have the passport endorsement, and, if previously issued a passport with the endorsement, may be issued a new one without it.

Chapter 12. VICTIM IDENTIFICATION AND NCMEC IMAGE SUBMISSION

12.1. Victim Identification

CEIU maintains the NCVIP (*see* Section 12.2) to assist in the identification of victims of child sexual abuse that has been captured in images and/or videos. NCVIP manages the National Child Exploitation Material Library (*see* Section 10.10) and NCVIS (*see* Sections 10.10 and 12.2), and CEIU coordinates with NCMEC's CVIP and INTERPOL's Victim Identification Working Group. (Note: All victim identification efforts must be coordinated with NCVIP.)

NCMEC maintains law enforcement POCs for identified children. This information is used to assist law enforcement agencies and prosecutors with determining if submitted images are of children who have been identified in past investigations, thereby reducing efforts spent trying to identify those children.

When new child victims are identified, SAs must submit to NCMEC case information and images obtained from the case pursuant to Section 12.3 below. Information submitted to

NCMEC will be included in the NCMEC, INTERPOL, and HSI child victim identification systems.

12.2. Victim Identification Program

The VIP is a national program under the oversight of CEIU covering several related components:

- A. NCVIS is HSI's repository of child exploitation material. (b) (7)(E)
[REDACTED]
- B. (b) (7)(E)
- C. The National Child Exploitation Material Library (*see* Section 10.10).
- D. An interagency liaison effort by CEIU to exchange child victim and abuser information with other foreign, federal, state, and local law enforcement agencies.
(b) (7)(E)

The VIP is the recognized U.S. law enforcement participant in the (b) (7)(E) Victim Identification Working Group. The mission of this group is to identify victims depicted in child abuse images and/or videos. (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

The VIP provides several services in support of child exploitation investigations and victim identification efforts, including:

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

12.3. NCMEC Image and Video Submission Procedures

CEIU and NCMEC have developed a streamlined process for assisting SAs with the analysis of child exploitation material to determine if victims have been identified by law enforcement in past investigations. NCMEC's CVIP strives to provide the fastest service possible to requesting agencies. Cases are processed in the order in which they are received. SAs should contact the CVIP staff or the HSI liaison if they need the report by a specific date. Questions can be directed to the HSI liaison at NCMEC at (877) 446-(b) (7)(E), ext. (b) (7)(E) or via email at (b) (7)(E)@ice.dhs.gov. The CVIP staff can be reached via email at (b) (7)(E)

SAs should contact the HSI liaison at NCMEC to obtain the current submission protocols for image review or for newly identified victims. As stated in Section 9.8 (C), due to system constraints, digital media submissions to NCMEC do not require password protection.

12.4. Child Pornography Notification Preference Form

SAs should coordinate with the HSI Victim Assistance Specialist or Victim Assistance Coordinator to complete a Child Pornography Notification Preference Form (ICE Form 73-053) for each identified victim of CSAM. Upon receipt of the series name from NCMEC, the SA should submit the completed ICE Form 73-053 to the HSI VAP. All ICE Forms 73-053 must be updated when the minor victim reaches the age of majority (18 years old).

Chapter 13. AWARENESS AND RESILIENCE MENTORING FOR OPERATIONAL READINESS (ARMOR) PROGRAM

(b) (7)(E)

13.1 Purpose

ARMOR was established as an official extension of the ICE Peer Support Program to help ensure that there is an HSI resilience program that includes a proactive focus on primary stressors and continual prevention of these stressors, confidential and voluntary assistance to personnel struggling with personal or job-related stressors, and transition services that help ensure a healthy shift when the employee is assigned to another group or to duties that do not include exposure to graphic material.

13.2 Process

ARMOR is a program designed to aid personnel directly involved in CEIs. It applies, but is not limited, to HSI SAs, CFAs, and CAs. TFOs assigned to HSI offices may participate in ARMOR, as needed. TFOs whose home agencies do not provide resilience-building services are encouraged to participate in ARMOR. Other ICE employees whose job duties include exposure to CEIs may also participate in the program.

In most cases, ARMOR services are offered at the SAC offices. Employees assigned to a location that is not affiliated with a SAC office will receive services through the nearest SAC office. C3 employees will receive ARMOR services through the Washington, DC, SAC office.

13.3 Safeguards

HSI has codified program-specific activities designed to build on individual and group strengths and has put in place safeguards designed to manage and mitigate risk. ARMOR is composed of four crucial activities that can positively influence the well-being and resilience of individuals engaged in CEIs:

- A. Protective or preventative measures deployed prior to initial exposure to potentially disturbing material when feasible, or as soon as possible following initial exposure when necessary;
- B. Regular and mandatory musters for those continually exposed, designed to build and maintain resilience, reduce symptoms if and when they begin to appear, and minimize stigma associated with having undesired reactions and asking for help with them;
- C. Response services, including group or individual debriefings, following particularly distressing exposure or whenever requested; and
- D. A transition-out plan, including the ability for employees who determine that they need a temporary or permanent break from exposure to disturbing content to request and receive reassignment of duties without fear of reprisals.

13.4 Objectives

(b) (7) (E)

13.5 Mechanism

ARMOR has four official mechanisms to accomplish the stated objectives:

- A. ARMOR Operational Readiness Training;
- B. ARMOR Time-Driven Resilient Mind Musters;
- C. ARMOR Event-Driven Support Services; and
- D. ARMOR Transition Training.

(Note: See HSI Directive 18-03, ARMOR: The Child Exploitation Investigations Resilience Program, dated August 16, 2018, or as updated.)

Chapter 14. OUTREACH PROGRAM

14.1 Project iGuardian

HSI is committed to combatting the sexual exploitation of children. Investigations of child sexual exploitation are among HSI's primary investigative priorities. The sexual abuse of children impacts the most vulnerable segment of our society. HSI recognizes the importance of education and community awareness regarding the dangers of online activity and has partnered with the NCMEC NetSmartz and ICAC task forces in this endeavor. NetSmartz is NCMEC's online safety education program. It provides age-appropriate videos and activities to help teach children to be safer online with the goal of helping children to become more aware of potential online risks and empowering them to help prevent victimization by making safer choices online and offline.

Project iGuardian ((b) (7)(E)) aims to counter a disturbing fact – many online child predators are able to find victims online because children and their parents are not aware of how dangerous online environments can be. It is focused on keeping minors safe from online predators through education and awareness. The project is an outreach effort to share information about the dangers of online environments, how to stay safe online, and how to report abuse and suspicious activity. In addition, the iGuardian team helps minors stay safe online by providing safety tips, a number to call, and a website with links to more information and resources. Project iGuardian helps minors, and parents be smart about online safety and stay safe from online sexual predators through audience-appropriate information about the dangers of online environments; conveying this information on how to stay safe online can help prevent many instances of this crime.

14.2 Project Beacon

Project Beacon is an HSI-led outreach program that seeks the partnership, cooperation, and assistance of private industries in preventing the spread of child exploitative material. In addition, Project Beacon seeks to leverage private industry information and resources to identify possible predators, generate leads to initiate new HSI investigations, and support ongoing HSI investigations. Project Beacon assists private industry by providing HSI POCs to facilitate guidance and dialogue when such entities encounter suspicious activity or require guidance in their particular industry.

Project Beacon specifically involves SAs conducting outreach visits and providing presentation materials to various private industries located in their respective AORs. The industrial and economic infrastructure of each geographic location will ultimately dictate which entities should receive a Project Beacon outreach visit. For example, companies and industries operating in the online, social media, data processing, and cloud hosting sectors are obvious candidates for Project Beacon outreach visits; however, SAs should also consider any company involved in computer-related sectors, including computer repair, as well as the travel industry that may see individuals involved in CST.

SAs can contact the CEIU Project Beacon POC for presentation materials relevant to the specific industry during each outreach visit, including discussion of all topics and concepts addressed in the presentation materials, to ensure consistency and uniformity in all presentations provided to private industry. Project Beacon presentation materials address several key topics, including the following: (1) an explanation of HSI’s jurisdiction, authorities, and child exploitation investigation mission; (2) an overview of the major U.S. laws regarding child exploitation; (3) a description of Project Beacon recipient responsibilities in complying with U.S. law; and (4) guidance to help partners identify the warning signs and indicators of illegal activity.

Prior to conducting a Project Beacon outreach visit, SAs should educate themselves regarding the prospective Project Beacon recipient’s line of business. Likewise, during a Project Beacon outreach visit, SAs should obtain additional information about the Project Beacon outreach recipient to document in an ROI, including the following: (1) the name, position, and job responsibilities of each person in attendance; (2) an explanation of the recipient’s existing knowledge of U.S. child exploitation law; (3) what steps they currently have in place to identify child exploitation, if any; and (4) if they have a program in place to contact law enforcement. In addition, SAs should always provide a business card or the contact information for their respective HSI office and remind the recipients to contact them or an HSI office if they encounter suspicious activity. C3 will maintain a table of industry POCs to facilitate better communication. Newly added POCs should be provided to C3 by the field to be added to the master list.

(b) (7)(E)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E)

(b) (7)(E)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

ACRONYMS

[REDACTED]	[REDACTED]
AOR	Area of Responsibility
ARMOR	Awareness and Resilience Mentoring for Operational Readiness
ASAC	Assistant Special Agent in Charge
AUSA	Assistant U.S. Attorney
AWC	Angel Watch Center
BBS	Bulletin Board System
BOLO	Be on the Look Out
C3	Cyber Crimes Center
CA	Criminal Analyst
CAC	Child Advocacy Center
CBP	U.S. Customs and Border Protection
CCD	Consular Consolidated Database
CD-ROM	Compact Disc-Read Only Memory
CEI	Child Exploitation Investigation
CEIU	Child Exploitation Investigations Unit
CEOS	Child Exploitation and Obscenity Section
CFA	Computer Forensics Agent
CFAN	Computer Forensics Analyst
CIR	Child Identification Report
(b) (7)(E)	[REDACTED]
(b) (7)(E)	[REDACTED]
CPS	Child Protective Services
CPVA	Child Pornography Victim Assistance
CRIS	Child Recognition Identification System
CSAM	Child Sexual Abuse Material
CST	Child Sex Tourism
CVIP	Child Victim Identification Program
DAD	Deputy Assistant Director
DHS	Department of Homeland Security
DOJ	Department of Justice
DOS	Department of State
DSM	Diagnostic and Statistical Manual of Mental Disorders
DVD	Digital Versatile Disc
EAD	Executive Associate Director
ECPA	Electronic Communications Privacy Act
ESP	Electronic Service Provider
EUROPOL	European Police
FBI	Federal Bureau of Investigation
FI	Forensic Interview
FIS	Forensic Interview Specialist

FOUO	For Official Use Only
GS	General Schedule
HB	Handbook F, 10, etc.
HERO	Human Exploitation Rescue Operative
HQ	Headquarters
HSI	Homeland Security Investigations
HSILD	HSI Law Division
ICAC	Internet Crimes Against Children
ICE	U.S. Immigration and Customs Enforcement
(b) (7)(E)	[REDACTED]
ICSE	International Child Sexual Exploitation
IML	International Megan's Law
INTERPOL	International Criminal Police Organization
IP	Internet Protocol
IR	Investigative Referral
MOU	Memorandum of Understanding
NCMEC	National Center for Missing & Exploited Children
NCVIP	National Child Victim Identification Program
NCVIS	National Child Victim Identification System
NGO	Non-Governmental Organization
NIAC	Nationwide Investigations Advisory Committee
(b) (7)(E)	[REDACTED]
NSOR	National Sex Offender Registry
(b) (7)(E)	[REDACTED]
(b) (7)(E)	[REDACTED]
OI	Office of Investigations
OPA	Office of Public Affairs
OPLA	Office of the Principal Legal Advisor
OPPREL	Operation Predator
P2P	Peer to Peer
POC	Point of Contact
ROI	Report of Investigation
SA	Special Agent
SAC	Special Agent in Charge
SAMEPH	Seized Asset Management and Enforcement Procedures Handbook
SD	Secure Digital
(b) (7)(E)	[REDACTED]
SEN	Significant Event Notification
SIR	Significant Incident Report
TA	Technical Assistance
TCSO	Transnational Child Sex Offender
TFO	Task Force Officer
UPAX	Unified Passenger
USAO	United States Attorney's Office
U.S.C.	United States Code
USMS	United States Marshals Service

USPIS	United States Postal Inspection Service
VAP	Victim Assistance Program
VAS	Victim Assistance Specialist
VIP	Victim Identification Program
VIR	Victim Information Report
VIS	Victim Impact Statement