

LIMITED OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE



Internet Crimes Against Children Task Force Program

OPERATIONAL AND INVESTIGATIVE STANDARDS

ICAC Task Force Program Operational and Investigative Standards
FOR ICAC PURPOSES ONLY
Revised: October 1, 2018

**LIMITED OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE**

Table of Contents

Definitions of Terms	2
1. Purpose of the ICAC Standards	4
2. ICAC National Program.....	5
3. Oversight of the ICAC Program.....	6
4. Selection and Retention of Task Force Members	7
5. Training	8
6. Case Management	9
7. Task Force Reporting Requirements to OJJDP.....	10
8. Investigations	11
9. Work Environment and Equipment.....	14
10. Victim Identification	15
11. Public Awareness and Community Outreach.....	16
12. Media Relations and Media Releases.....	17

**LIMITED OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE**

Definitions of Terms

Applicability of Terms

Although some of the definitions below may be generally applicable to law enforcement, they are intended for use in the interpretation of these *Standards*. As such, where any term defined below is capitalized in these *Standards*, the *Standards* are referring to that term as defined below. By contrast, where any term defined below is not capitalized in these *Standards*, the *Standards* are referring to that term as it is used generally in the field of law enforcement. Additionally, the capitalized terms have been italicized to ease their recognition.

“**Affiliate**” or **Affiliate Agency**” is an agency that is working with a *Lead Agency* as part of a regional or state ICAC *Task Force*. An *Affiliate* has agreed in writing to adhere to these *Standards*.

“**Authorized Personnel**” are *Members* who themselves lack powers of arrest but have been authorized by their respective agency to participate in *Investigations* and are being supervised by *Sworn Personnel*.

“**Commander**” is the *Member* of a *Lead Agency* who has been designated by that *Lead Agency* and recognized by *OJJDP* as the leader of the corresponding *Task Force*.

“**CEOS**” is the Child Exploitation and Obscenity Section of the Criminal Division of the Department of Justice.

“**Contraband Image**” is a visual depiction in any form (including printed/digital or video) of child sexual exploitation as defined by federal and/or state statute.

“**Crime**” is any offense (or group thereof) that involves (or involve) the exploitation/victimization of children facilitated by technology.

“**CVIP**” is the Child Victim Identification Project operated by NCMEC.

“**CyberTipline**” is a reporting mechanism operated by NCMEC that allows for the reporting of suspected *Crimes*.

“**Deconfliction**” is a process whereby *Members* are able to submit *Investigative* information to each other and/or to ICAC-related databases in order to determine whether other *Members* or other law enforcement agencies have information concerning the same targets or *Crimes*.

“**DOJ**” is the United States Department of Justice.

“**Employee**” is a sworn or compensated individual, or any individual working under the direction and control of a law enforcement agency.

LIMITED OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

“**Equipment**” is any article, device or resource, including but not limited to computers, phones, online accounts and internet services which are purchased or obtained for use in ICAC-related matters.

“**ICAC Program**” is the Internet Crimes Against Children Task Force Program, a national program composed of state and regional *Task Forces* administered by *OJJDP*.

“**Investigation**” is an investigation into a *Crime*. Likewise, “*Investigate*” “*Investigating*” and “*Investigative*” are used within the same context.

“**Investigative Persona**” – any identity established or created by an *Employee* to aid an *Investigation*.

“**Investigator**” is a *Member* who is a part of the *Sworn Personnel* of a *Task Force*.

“**Lead**” or “**Lead Agency**” is the law enforcement agency that receives the ICAC grant and is designated by *OJJDP* to act as the *Lead Agency* for the corresponding *Task Force*.

“**Member**” is a *Lead* or *Affiliate Agency’s Employee* who is either *Sworn Personnel* or *Authorized Personnel* and who has been designated to work on ICAC-related matters for his/her respective agency and *Task Force*.

“**National Initiative**” is any proposal that relies on the cooperation and resources of a significant number of *Task Forces* and, accordingly, has been approved by *OJJDP*.

“**NCMEC**” is the National Center for Missing and Exploited Children.

“**OJJDP**” is the Office of Juvenile Justice and Delinquency Prevention within the *DOJ*.

“**Supervisor**” is a *Member* who has been designated by his/her respective agency to supervise *Investigations* and other ICAC-related matters.

“**Standards**” are all of the provisions of these, the ICAC Operational and Investigative Standards.

“**Sworn Personnel**” are *Members* with powers of arrest.

“**Task Force**” is the *Lead Agency* and their *Affiliate(s)* (combined) as designated by *OJJDP* for a particular state or region.

**LIMITED OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE**

1. Purpose of the ICAC Standards

These *Standards* are established by *OJJDP* to guide the administration and operation of the *ICAC Program* and its *Members* when working on ICAC-related *Investigations* and matters.

Members should make every reasonable effort to comply with these *Standards*. However, since many aspects of *Investigations* are dynamic and because laws vary widely between jurisdictions, it is difficult to anticipate every circumstance that might present itself. Thus, reasonable deviations from these *Standards* may occur depending upon various factors (e.g., emergency situations; timing constraints; accessibility constraints; resource constraints; technology constraints; perceived conflicts between the *Standards* and statutes, decisional law, and court orders; etcetera).

Commanders may supplement, but not contradict, these *Standards* in the written agreements they establish with their *Affiliates* to promote the effective operation of their *Task Forces*. Should questions regarding the interpretation of these *Standards* arise or conflicts occur between these *Standards* and agency policies or law, the *Commander* faced with the issue shall seek the guidance of an *OJJDP* Program Manager. However, nothing in these *Standards* is meant to interfere with a *Commander's* or *Supervisor's* lawful tactical decision-making.

**LIMITED OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE**

2. ICAC National Program

2.1 Mission of the ICAC Program

The Internet Crimes Against Children (ICAC) Task Force Program helps state and local law enforcement agencies develop an effective response to technology-facilitated child sexual exploitation and internet crimes against children. This support encompasses forensic and *Investigative* components, training and technical assistance, victim services, prevention and community education.

2.2 ICAC Background

The Internet Crimes Against Children (ICAC) Task Force Program was developed in 1998 in response to the increasing number of children and teenagers using the internet and other technology, the proliferation of child sexual abuse images available electronically, and the heightened online activity by predators seeking unsupervised contact with potential underage victims.

The *ICAC Program* is a national network of 61 coordinated task forces representing more than 4,500 federal, state, and local law enforcement and prosecutorial agencies. These agencies are engaged in both proactive and reactive investigations, forensic examinations, and criminal prosecutions. By helping state and local agencies develop effective, sustainable responses to online child victimization – including responses to child sexual abuse images (*Contraband Images*), the *ICAC Program* has increased law enforcement's capacity to combat technology-facilitated crimes against children at every level.

Because arrests alone cannot resolve the problem of technology-facilitated child sexual exploitation, the *ICAC Program* is also dedicated to training law enforcement personnel, prosecutors and other professionals working in the ICAC field, as well as educating parents, youth, and the community about the potential dangers of online activity including online child victimization.

**LIMITED OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE**

3. Oversight of the ICAC Program

3.1 The oversight of the *ICAC Program* and the administration of ICAC grants are the responsibility of *OJJDP*. The oversight of each *Task Force* falls to its *Commander*. The oversight of each agency, both *Lead* and *Affiliate*, falls to its designated *Supervisor*.

3.2 *Commanders* shall ensure there are supervisory systems and protocols in place that provide for observation, documentation, and review of ICAC activity. Said systems shall comply with the principles of quality case management and shall ensure that ICAC activities comply with agency policies and these *Standards*.

3.3 *Commanders* shall ensure that each *Member* in his/her *Lead Agency* and each *Supervisor* of an *Affiliate Agency* receives a copy of the *Standards*.

3.3.1 *Supervisors* shall have the discretion to provide *Members* with only the sections of the *Standards* applicable to their job functions.

3.4 *Commanders* shall submit all proposed *National Initiatives* to *OJJDP* prior to the start of the project.

3.4.1 *OJJDP* may suggest amendments to the original proposal following consultation with the presenting *Commander* and, as appropriate, other federal, state, and local entities.

3.5 *Supervisors* shall inform their *Members* about departmental employee assistance programs and *Task Force* resources available to them.

**LIMITED OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE**

4. Selection and Retention of Task Force Members

4.1 When practicable during the selection process of *Members*, *Commanders* and *Supervisors* shall evaluate prospective candidates for work histories that indicate prior *Investigative* experience, courtroom testimony skills, technical knowledge and ability, an ability to prudently handle sensitive information, a genuine interest in the protection of children, and an understanding of the effects that *Members* may experience when exposed to *Contraband Images*.

4.2 *Commanders* and *Supervisors* shall acknowledge the potential effects of *Investigations* of and exposure to *Contraband Images* and recognize that the viewing of *Contraband Images* should be restricted. When practicable, the following techniques may help mitigate some of the potential negative effects of this work may aid with the retention of *Members*:

- **Work flexibility** - *Commanders* and *Supervisors* are encouraged to allow flexibility for *Investigators* and others who are exposed to *Contraband Images* (e.g., frequent breaks, having an open-door policy, etc.).
- **Exposure to *Contraband Images*** - *Commanders* and *Supervisors* are encouraged to implement best practices which minimize the exposure to *Contraband Images* by *Members*.
- **Mental Health Providers (MHP)** - In compliance with their agency guidelines, *Commanders* and *Supervisors* are encouraged to work with MHP to make recommendations for care of *Members* and to provide education and training designed to minimize the impact of exposure to *Contraband Images*.
- **Impact of *Contraband Images*** - *Commanders* and *Supervisors* are encouraged to share or pursue best practices for minimization of the impact of *Contraband Images* and to promote attendance at trainings regarding methods used to minimize said impact.

4.3 *Commanders* and *Supervisors* shall recognize that ICAC *Investigations* typically focus on child sex offenders who have committed serious state or federal crimes and due to this life-changing event, the impact on these offenders can result in a violent response to authorities.¹

¹ FBI's Investigation Behavioral Analysis Unit's *Operational Safety Considerations While Investigating Child Sex Offenders, A Handbook for Law Enforcement*, Volume 1, March 2012.

**LIMITED OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE**

5. Training

Ensuring that personnel are well-trained in conducting effective *Investigations* in a manner consistent with applicable laws is integral to the *ICAC Program*.

5.1 All national training curricula supported by *ICAC Program* resources shall be conducted consistent with the *Standards* and shall be approved by *OJJDP*.

5.2 Commanders shall ensure that nominees to attend any *ICAC Program*-sponsored national in-person training event are current *Members*.

5.3 Individual *Task Forces* may develop and deliver *Task Force* specific training. This training shall comply with the *Standards* and shall be approved by the *Commander*. All costs to develop and deliver the training shall be the responsibility of the *Task Force* or *Affiliate* providing the training.

**LIMITED OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE**

6. Case Management

6.1 *Commanders and Supervisors* are responsible for determining *Investigative* priorities and selecting cases for *Investigation* in their respective agencies. Those determinations shall include an assessment of victim risk, jurisdiction, known offender behavioral characteristics, and the likelihood of securing the information necessary to pursue each *Investigation*.

6.2 Conventional boundaries often are meaningless in today's digital world where the usual constraints of time, place, and distance lose their relevance. These factors increase the possibility of *Lead* and/or *Affiliate Agencies* targeting other law enforcement personnel, *Investigating* the same target, or inadvertently disrupting an ongoing *Investigation*. To foster effective case coordination, collaboration, and communication, each *Member* shall make every effort to *Deconflict* all active *Investigations*.

6.3 *Lead* and *Affiliate Agencies* shall be subject to their respective agency's incident reporting procedures and case supervision systems. At a minimum, a unique identifier shall be assigned to each case.

**LIMITED OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE**

7. Task Force Reporting Requirements to OJJDP

7.1 The reports described below do not replace the semi-annual progress report required by the Office of Justice Programs' Financial Guide.

7.2 *Commanders* shall compile and submit a Task Force Monthly Performance Measures Report to the *OJJDP*-designated location before the end of the following calendar month.

7.2.1 *Affiliates* shall report their activity to their respective *Commander* by the 10th of each month using the ICAC Monthly Performance Measures Report.

7.3 *Commanders* shall compile and submit an annual report which details each of their *Affiliates*. This annual report shall be submitted within 30 days of the end of the calendar year. The report shall be submitted in a method determined by *OJJDP* and shall include the following information:

7.3.1 The name of each *Affiliate Agency*.

7.3.2 The staffing level of each *Affiliate Agency* including the number of *Investigators*, prosecutors, education specialists, and forensic specialists dedicated to *Investigating* and prosecuting *Crime*.

**LIMITED OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE**

8. Investigations

8.1 *Investigations* shall be conducted in a manner consistent with applicable laws and the ICAC *Standards*.

8.2 Only *Sworn Personnel* shall conduct *Investigations*.

8.2.1 *Authorized Personnel* acting under the direction and supervision of *Sworn Personnel* may participate in *Investigations*.

8.2.2 *Members* shall not approve, condone, encourage, or promote cyber-vigilantism by private citizens. As such, *Members* shall not use unauthorized private citizens to proactively seek out *Investigative* targets.

8.2.3 The above section (8.2.2) shall not preclude the use of information related to a *Crime* provided by victims or public citizens who discover evidence (e.g., CyberTip reports, mandated reports from professionals, computer repair shop complaints, parental complaints, et cetera). Nor does it preclude the use of authorized over-hears or other similar *Investigative* methods designed to further an *Investigation*.

8.3 *Investigations* shall be documented. Any departures from this provision due to unusual or exigent circumstances shall be documented in the relevant case file and reviewed by the *Supervisor*.

8.3.1 The access, retention, storage, security, and disposal of *Investigative* or case information shall be consistent with the subject agency's policies and federal and state law regarding same.

8.4 *Members* shall not electronically upload, transmit, or forward any *Contraband Images*.

8.4.1 **Exception to Section 8.4.** Section 8.4 shall not prohibit the transfer of evidence between *Investigators* as provided for by sections 8.9 and 8.10 of these *Standards* nor does it prohibit the submission of *Contraband Images* to CVIP as provided for by section 10.1 of these *Standards*.

8.5 *Members* shall not use any visual depiction of any type (including a manipulated or electronically generated visual depiction) of any person, purported person, or body part of a person or purported person, with the sole exception that a *Member* may use a visual depiction as a representation of an *Investigative Person*/person/purported person when the following **four** requirements are met:

- (1) The visual depiction is of an actual person;
- (2) That person is an *Employee*;

LIMITED OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

(3) The *Employee* has given his or her written consent for the visual depiction to be used; and

(4) The *Employee* was at least 18 years old at the time when the *Employee* gave consent for such use. The visual depiction may be of the *Employee* that was produced when the *Employee* was under the age of 18. The visual depiction may also be modified to suit *Investigative* needs (*i.e.*, it may be an altered or age-regressed visual depiction of the *Employee*).

8.5.1 **Exception to Section 8.5.** Section 8.5 does not prohibit a federal or federally-approved *Member* (*e.g.*, an FBI/HSI agent, or an FBI/HSI Task Force Officer) from using a visual depiction that does not meet the four requirements of Section 8.5, so long as the visual depiction is one that has been authorized for use by the FBI or HSI in accordance with that respective federal agency's guidelines and the visual depiction is being used pursuant to those guidelines.

8.6 Absent prosecutorial input to the contrary, during online dialogue, *Investigators* shall allow the *Investigative* target to set the tone, pace, and subject matter of the online conversation.

8.6.1 Section (8.6) shall not be construed to prohibit *Investigators* from performing any of the following activities when initiating or conducting an *Investigation*: (a) posting information including visual depictions (image or video/printed or digital) to establish an online presence, (b) placing or posting advertisements, or (c) sending messages.

8.6.2 *Members* shall familiarize themselves with relevant state and federal law, including but not limited to those regarding the defense of entrapment, and shall confer with prosecutors, as needed.

8.6.3 Prior to conducting any large-scale (multi-target) operations, *Members* shall notify the *Commander* and shall consult relevant prosecutors about the operation.

8.7 The examination of digital storage devices shall be performed consistent with the subject agency's protocol.

8.8 *Contraband Images* shall be maintained pursuant to the subject agency's policy.

8.8.1 Absent a court order specifically ordering otherwise, evidence containing *Contraband Images* shall not be released to any defendant or representative thereof.

LIMITED OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

8.9 Absent exigent circumstances, all *Members'* case referrals between *Task Forces* shall include:

- Notification to and acceptance by the *Commander(s)* of both *Task Forces* that are involved in the referral;
- A secure (i.e., digitally-protected) copy of the case file;
- An official *Investigative* report or affidavit containing case details; and,
- Documentation, preferably the original, of all legal process conducted and all compliance with same, especially those documents related to the issue of jurisdiction and identification of suspect(s).

8.10 Law enforcement transfers of evidence containing *Contraband Images* shall be done in a secure manner.

**LIMITED OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE**

9. Work Environment and Equipment

9.1 *Investigations* shall be conducted in an approved work environment, using approved *Equipment*, as designated by a *Commander* or *Supervisor*.

9.2 *Commanders* and *Supervisors* are encouraged to provide a work environment that provides for discreet and sensitive *Investigations* while simultaneously minimizing chances of inadvertent or unnecessary exposure to *Contraband Images*.

9.3 *ICAC Equipment* shall be reserved for the exclusive use of its *Members*, and shall be used in accordance with these *Standards* and with their respective agency's policies.

9.4 When practicable, *Equipment* which may be used in undercover aspects of an *Investigation* shall be purchased covertly.

9.5 No personally-owned equipment, accounts or networks shall be used in *Investigations*.

9.6 Software shall be properly acquired and licensed.

**LIMITED OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE**

10. Victim Identification

10.1 Identifying child victims of *Crime* is a critical element of the *ICAC Program*. *DOJ* and *OJJDP* require the *Lead* and *Affiliate Agencies* to submit *Contraband Images* to CVIP as a means to improve child victim identification. Absent exigent circumstances, *Contraband Images* shall be sent to CVIP pursuant to NCMEC's standards regarding same. In addition, *Lead* and *Affiliate Agencies* are encouraged to collaborate with NCMEC in their effort to identify children depicted in *Contraband Images*.

10.2 Absent exigent circumstances, victim-identifying information shall be protected from public disclosure pursuant to the protections set forth in federal and state law.

10.3 *Lead* and *Affiliate Agencies* shall adhere to local, state, and federal laws, as well as their agency's policies regarding mandated reporting, victim notification, and victim assistance.

**LIMITED OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE**

11. Public Awareness and Community Outreach

11.1 Public awareness activities and community outreach are a critical component of the *ICAC Program*. *Lead* and *Affiliate Agencies* shall foster awareness and shall provide practical relevant guidance to children, parents, educators, and others concerned with child safety.

11.1.1 Social media can be used to promote educational awareness as long as it is consistent with all agency policy and these *Standards*.

11.2 Presentations to school personnel, parents, and community groups are excellent ways to promote awareness. These presentations shall not include any visual depiction of a victim unless the victim has consented to its use and the victim is currently at least 18 years of age. No *Contraband Image* shall be used in these presentations nor shall a presenter discuss confidential *Investigative* tools and techniques.

11.3 No individual affiliated with *ICAC Program* may speak on behalf of the national *ICAC Program* without the express written consent of *OJJDP*. While making public presentations, *Members* may indicate a preference for a product or service, but, when done, shall avoid an implicit endorsement and shall include alternatives in the presentation.

11.4 Materials and presentations shall be consistent with the *ICAC Program's* mission and background, as enumerated in Section 2 of these *Standards*.

**LIMITED OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE**

12. Media Relations and Media Releases

12.1 Media releases relating to prosecutions, *Crime* alerts, or other matters concerning ICAC operations shall not include information regarding confidential *Investigative* techniques, and shall be coordinated, when applicable, with the law enforcement agencies involved with the subject *Investigations*, in a manner consistent with sound information management and sound media relations practices.

12.2 *Commanders* and *Supervisors* may speak to members of the media about their own agency's ICAC-related activities per the terms of their agency's policy on such media relations. No individual affiliated with *ICAC Program* may speak on behalf of the national *ICAC Program* without the express written consent of *OJJDP*.

12.3 *Commanders* shall inform their *OJJDP* Program Manager if approached by national media outlets about the national *ICAC Program* (as opposed to media seeking information from a particular *Task Force* about its local activities) so that a coordinated national response can be prepared by *OJJDP*.

12.4 Information provided by *Task Forces* to the media shall be consistent with *ICAC Program*'s mission and background, as described in Section 2 of these *Standards*.

End of ICAC Standards