

Exhibit B

LAW ENFORCEMENT SENSITIVE



Internet Crimes Against Children Program

OPERATIONAL AND INVESTIGATIVE STANDARDS

ICAC Program Operational and Investigative Standards
FOR LAW ENFORCEMENT PURPOSES ONLY

Page 1 of 16

Exhibit B

LAW ENFORCEMENT SENSITIVE

Definitions

As used herein, the following definitions shall apply:

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

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

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

“ICAC” is the Internet Crimes Against Children program composed of Task Forces and Affiliates.

“TASK FORCE” is defined as an ICAC law enforcement agency designated by OJJDP to act as a State and/or Regional Task Force.

“AFFILIATE” is defined as a law enforcement agency that is working in partnership with a Task Force and has agreed in writing to adhere to ICAC Operational and Investigative Standards.

“PARTNER” is defined as an agency assisting a Task Force absent a written agreement.

“NATIONAL INITIATIVE” is defined as any investigative proposal that relies on the cooperation and resources of all Task Forces or mandates action by OJJDP.

“CVIP” is the Child Victim Identification Program operated by the National Center for Missing & Exploited Children.

“CYBERTIPLINE” is a reporting mechanism for cases of online child sexual exploitation and enticement operated by the National Center for Missing & Exploited Children.

For the purposes of this program, *crime* is defined as any offense that involves the exploitation of children facilitated by technology.

Investigative interest is established when there is reasonable suspicion that a screen name or other potentially identifiable entity has committed a crime or that entity is engaged in a sequence of activities that is likely to result in the commission of a crime.

Exhibit B

LAW ENFORCEMENT SENSITIVE

A proactive investigation is designed to identify, investigate and prosecute offenders, which may or may not involve a specific target, and requires online interaction and a significant degree of pre-operative planning.

A reactive investigation involves the investigation of a complaint of a crime.

Reasonable suspicion is established when sufficient facts exist to lead a law enforcement officer to believe that an individual or organization is involved in a definable criminal activity.

Exhibit B

LAW ENFORCEMENT SENSITIVE

1. Oversight

1.1 Each ICAC agency shall have supervisory systems and procedures, which shall provide for observation, documentation, and periodic review of ICAC activity. Such system should comply with the principles of quality case management and ensure that ICAC activities comply with both agency and ICAC Standards.

1.2 Task Forces shall submit all proposed national initiatives to OJJDP prior to project initiation.

1.3 OJJDP may suggest amendments to the original proposal following consultation with the presenting Task Force and other federal, state, and local entities.

Exhibit B

LAW ENFORCEMENT SENSITIVE

2. Selection and Retention of ICAC Task Force Personnel

2.1 Managers and supervisors should evaluate prospective ICAC candidates for work history that indicates prior investigative experience, court testimony skills, ability to handle sensitive information prudently, and a genuine interest in the protection of children.

2.2 Given the graphic nature of evidence routinely encountered in ICAC related cases, the mental health of investigators working such cases is a great concern. Task force supervisors at all levels are encouraged to make reasonable efforts to ensure that all assigned officers remain fit for duty in accordance with applicable departmental policies and procedures.

Exhibit B

LAW ENFORCEMENT SENSITIVE

3. Training

3.1 All Investigators will be supplied with appropriate training consistent with the ICAC Operational and Investigative Standards.

3.2 ICAC Task Force Commanders are responsible for ensuring that the individuals nominated for ICAC sponsored training are employed by agencies that have agreed in writing to adhere to the ICAC standards of investigation and that any prerequisite requirements for the training session have been met.

3.3 ICAC task forces may give regional training. The training shall comply with current ICAC standards. Any subsequent support required as a result of the regional training shall be the responsibility of the task force providing the training.

Exhibit B

LAW ENFORCEMENT SENSITIVE

4. Case Management

4.1 Case Predication and Prioritization

4.1.1 Cases may be initiated by referrals from the CyberTipline, Internet service providers, or other law enforcement agencies, and by information gathered through subject interviews, documented public sources, direct observations of suspicious behavior, public complaints, or by any other source acceptable under agency policies.

4.1.2 ICAC supervisors are responsible for determining investigative priorities and selecting cases for investigation. Assuming the information is deemed credible, that determination should begin with an assessment of victim risk and then consider other factors such as jurisdiction and known offender behavioral characteristics. The following prioritization scale shall be considered:

- a) A child is at immediate risk of victimization
- b) A child is vulnerable to victimization by a known offender
- c) A known suspect is aggressively soliciting a child(ren)
- d) Manufacturers, distributors or possessors of images that appear to be home photography with domiciled children
- e) Aggressive, high-volume child pornography manufacturers or distributors who either are commercial distributors, repeat offenders, or specialize in sadistic images
- f) Manufacturers, distributors and solicitors involved in high-volume trafficking or belong to an organized child pornography ring that operates as a criminal conspiracy
- g) Distributors, solicitors and possessors of images of child pornography
- h) Any other form of child victimization.

4.2 Record Keeping

4.2.1 ICAC agencies shall be subject to existing agency incident reporting procedures and case supervision systems. At a minimum, a unique identifier shall be assigned to each ICAC case.

4.2.2 All affiliated agencies will report their activity to the respective Task Force Commander by the 10th of each month using the ICAC Monthly Performance Measures Report.

Exhibit B

LAW ENFORCEMENT SENSITIVE

4.2.3 Task Forces will compile and submit their monthly performance measures report to the OJJDP designated location before the end of the following calendar month. This monthly report does not replace the semi-annual progress report required by the Office of Justice Program's Financial Guide.

4.2.4 ICAC Case Tracker – Task Forces will compile and submit information on all cases referred for either state or federal prosecution. Information is required for all cases referred by the grant receiving agency, as well as all affiliates that received more than \$20,000 a year. This report is on-going and begins with the prosecutorial agency the case is referred to and continues through the final disposition of the case. This on-going quarterly report will be due within five (5) business days of the start of the quarter and does not replace either the semi-annual progress report required by the Office of Justice Program's Financial Guide nor the quarterly statistical performance measures report (see 4.2.3 above). The report is submitted to icaccasetracker@usdoj.gov and copied to the ICAC Program Manager assigned to the task force.

4.3 Undercover Investigations

4.3.1 Carefully managed undercover operations conducted by well-trained officers are among the most effective techniques available to law enforcement for addressing ICAC offenses. Undercover operations, when executed and documented properly, collect virtually unassailable evidence regarding a suspect's predilection to exploit children.

4.3.2 ICAC supervisors are responsible for ensuring that ICAC investigators receive a copy of the ICAC Operational and Investigative Standards.

4.3.3 ICAC investigations shall be conducted in a manner consistent with the principles of law and due process. ICAC investigators are encouraged to work in conjunction with their local, state or federal prosecutors.

4.3.4 The following minimum standards apply to ICAC investigations:

- a. Only sworn, on-duty ICAC personnel shall conduct ICAC investigations in an undercover capacity. Private citizens shall not be asked to seek out investigative targets, nor shall they be authorized to act as police agents in an online Undercover capacity.
- b. ICAC personnel shall not electronically upload, transmit, or forward pornographic or sexually explicit images.
- c. Other than images or videos of individuals, age 18 or over, who have

Exhibit B

LAW ENFORCEMENT SENSITIVE

provided their informed written consent, and at the time consent was given were employed by a criminal justice agency, no actual human images or videos shall be utilized in an investigation. Employee is defined as a salaried or compensated individual.

d. During online dialogue, undercover officers should allow the investigative target to set the tone, pace, and subject matter of the online conversation. Image transfer shall be initiated by the target.

e. Undercover online activity shall be recorded and documented. Any departures from this policy due to unusual circumstances shall be documented in the relevant case file and reviewed by an ICAC supervisor.

4.4 Evidence Procedures

4.4.1 The storage, security, and destruction of investigative information shall be consistent with agency policy. Access to these files should be restricted to authorized personnel.

4.4.2 The examination of computers and digital media shall be consistent with agency policy and procedure.

4.4.3 Child pornography is contraband and should be maintained pursuant to each agency's policies regarding such. It is recommended that absent a court order specifically ordering otherwise, evidence containing child pornography shall not be released to any defendant or representative thereof.

4.4.4 The transfer of evidence containing child pornography among law enforcement shall be done in a secure manner. Methods of transfer may include hand-delivery, transmission of digitally protected files, delivery via a service which tracks the shipment, or other methods consistent with agency policy and practices.

4.5 Workspace and Equipment

4.5.1 ICAC computers and software shall be reserved for the exclusive use of agency designated ICAC personnel. When possible, undercover computers, software, and online accounts shall be purchased covertly. No personally owned equipment shall be used in ICAC investigations and all software shall be properly acquired and licensed.

4.5.2 ICAC personnel shall not use ICAC computers, software or online accounts for personal use.

4.5.3 Absent exigent or unforeseen circumstances, all ICAC online investigations shall be conducted in government workspace as designated by the agency. Exceptions

ICAC Program Operational and Investigative Standards
FOR LAW ENFORCEMENT PURPOSES ONLY

Exhibit B

LAW ENFORCEMENT SENSITIVE

must be approved in advance by an ICAC supervisor.

Exhibit B

LAW ENFORCEMENT SENSITIVE

5. Information Sharing

5.1 Conventional boundaries are virtually meaningless in the electronic world of the Internet and the usual constraints of time, place, and distance lose their relevance. These factors increase the possibility of ICAC agencies targeting one another, investigating the same subject, or inadvertently disrupting an ongoing investigation. To foster coordination, collaboration, and communication, each ICAC agency shall contribute case information on all active investigations (local, interstate, reactive and proactive) to a common database as designated by OJJDP currently, referred to as the ICAC Data Exchange.

5.2 If any common target is identified, the initiating ICAC agency is responsible for contacting the other law enforcement agency targeting the suspect.

5.3 Initiating ICAC agencies should also consider contacting other local, state, and federal agencies which may be involved in similar investigations.

Exhibit B

LAW ENFORCEMENT SENSITIVE

6. Victim Identification

6.1 Identifying child victims is a critical element of the ICAC Program. DOJ and OJJDP require all Task Forces to submit child victim images to the CVIP as a means to improve child victim identification. Absent exigent circumstances, child victim images will be sent to the CVIP consistent with NCMEC guidelines. In addition, ICAC agencies are encouraged to collaborate with NCMEC to identify children depicted in child pornography.

6.2 A focus of the ICAC Program is to protect children. In circumstances where reporting of child abuse is not required under existing laws, ICAC agencies are strongly encouraged to report instances in which a child may be at risk for abuse or exploitation.

6.3 Absent exigent circumstances, victim identifying information should be protected from public disclosure.

Exhibit B

LAW ENFORCEMENT SENSITIVE

7. Victim Notification

[New section to be drafted in 2009 about JUSTICE FOR ALL Act Provisions that govern victim notification.]

Exhibit B

LAW ENFORCEMENT SENSITIVE

8. Best Practices for Interacting with Potential Child Victims and their Non-Offending Family Members

[To be developed in 2009.]

Exhibit B

LAW ENFORCEMENT SENSITIVE

9. Community Education and Crime Prevention

9.1 Prevention education activities are a critical component of the OJJDP ICAC Program. ICAC agencies should foster awareness and provide practical, relevant guidance to children, parents, educators, librarians, and other individuals concerned about child safety issues.

9.2 Presentations to school staff, parents, and community groups are excellent ways to promote awareness. These presentations shall not depict identifiable victims, not otherwise in the public domain; nor shall they use pornographic or sexually explicit images. Presenters shall not discuss confidential investigative techniques.

9.3 No member of an ICAC Task Force may endorse any product or service without the express consent of an OJJDP Program Manager. While appearing at public presentations, ICAC members may indicate a preference for a product or service, but to avoid an implicit endorsement, such ICAC members should indicate adequate alternatives.

Exhibit B

LAW ENFORCEMENT SENSITIVE

10. Media Relations and Releases

10.1 Media releases relating to prosecutions, crime alerts or other matters concerning ICAC operations shall not include information regarding confidential investigative techniques and should be coordinated (when applicable) with other Task Force participants, Federal law enforcement agencies, and State and local agencies involved in the investigation consistent with sound information management and media relations practices.

10.2 ICAC Commanders (or their designees) may speak to members of the media about their own departments' ICAC-related activities according to their own agency's guidelines. No individual affiliated with the ICAC program may speak on behalf of the ICAC Program as a whole.

10.3 ICAC Commanders should inform their OJJDP Program Managers if approached by national media outlets about the ICAC Program (as opposed to media seeking information about local activities) so that a coordinated national response can be prepared by OJP.

10.4 Information provided by ICACs to the media shall be consistent with the guidance below:

Purpose of the ICAC Program

The mission of the Internet Crimes Against Children (ICAC) Task Force program is to assist state and local law enforcement agencies in developing an effective response to cyber enticement and child pornography cases. This support encompasses forensic and investigative components, training and technical assistance, victim services, prevention and community education.

Background on the ICAC Program

The Internet Crimes Against Children (ICAC) program is a national network of fifty-nine coordinated local task forces and their 1,800 local and regional affiliated agencies engaged in both proactive and reactive investigations, forensic examinations, effective prosecutions and community education. The ICAC Program was developed in response to the increasing number of children and teenagers using the Internet, the proliferation of child pornography, and the heightened online activity by predators searching for unsupervised contact with underage victims. By helping state and local law enforcement agencies develop effective and sustainable responses to online child victimization and child pornography, the ICAC program delivers national resources at the local level. The ICAC program actively protects children who use the Internet by proactively investigating the on-line sexual exploitation of children by predators. Because ICAC practitioners understand that arrests alone can not resolve the problem of on-line victimization, the ICAC program is dedicated to training law enforcement and educating parents and youth about the potential dangers online and offering safety tools.

ICAC Program Operational and Investigative Standards

FOR LAW ENFORCEMENT PURPOSES ONLY