Germantown Police Department

Policies and Procedures

Number: **3-7**
Effective Date: **January 9, 2012**
Subject: **Electronic Crimes and ICAC Investigations**
Previous Revisions: **March 21, 2011**

I. PURPOSE

The purpose of this policy is to establish responsibilities and guidelines for the Germantown Police Department's Electronic Crimes and Internet Crimes Against Children (ICAC) investigations in which digital media is used to commit those crimes.

II. POLICY

It is the policy of the Germantown Police Department that all officers responding to calls of electronic crimes and/or the exploitation of children will act in accordance with established departmental procedures. The standards adopted pursuant to this policy are prescribed by the Office of Juvenile Justice and Delinquency Prevention's (OJJDP) ICAC Task Forces and ensure compliance with those protocols accepted by the Federal Bureau of Investigations (FBI), United States Secret Service, (USSS), United States Customs (ICE), United States Postal Inspectors' Office (USPIO), and the United States Attorney's Office.

III. DEFINITIONS

A. Digital Media is any electronic device designed or utilized to store data, including, but not limited to, computers, personal digital assistants (PDAs), computer disks or tapes, removable storage devices, cellular phones, smartphones, and digital cameras.

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

C. A reactive investigation involves the investigation and prosecution of a known offender. It also includes a response within the community or area of jurisdiction to a specific complaint reported to the ICAC Task Force by another law enforcement agency, a reputable source of information such as the Cyber-Tipline at the National Center for Missing and Exploited Children, or a corporate Electronic Service Provider. Germantown Police Department ICAC detectives will investigate complaints made by citizens, schools, libraries, or businesses who believe illegal

material has been transmitted or potentially dangerous situations exist, such as child enticement or solicitation attempts have been communicated through the Internet or other electronic means.

C. The term Internet Crimes Against Children (ICAC) includes both proactive and reactive investigative activities as outlined above.

D. An investigation is deemed to be urgent when there is a reasonable belief that the suspect presents an imminent threat to the well-being of potential victims.

IV. PROCEDURE

A. Workspace and Equipment

1. The workspace for ICAC investigations shall have limited access to Electronic Crime/ICAC detectives and their supervisors, when there is an ongoing investigation or any evidence related to an ICAC investigation is secured within the workspace. Under no circumstances shall a civilian be left unattended in the workspace.

2. Equipment must be maintained and documented to ensure proper performance. Germantown Police Department owned forensic computers and ICAC computers, equipment, and software shall be kept up-to-date and in suitable working order. The manufactures' manuals and other relevant documentation for software and equipment will be readily available.

3. ICAC computers, accessories, and software shall be reserved for the exclusive use of Germantown Police Department designated personnel. When possible, undercover computers, software, and online accounts shall be purchased covertly. No personally owned computers may be used in ICAC investigations, and all software shall be properly acquired and licensed.

4. The undercover Internet connection utilized by ICAC detectives shall have no association to the Germantown Police Department or the City of Germantown and shall be billed to covert names and addresses.

5. The undercover Internet connection and computers shall not be accessible to anyone other than Electronic Crime/ICAC Task Force detectives, without the approval of an Investigations Division supervisor.

6. Absent exigent or unforeseen circumstances, all ICAC online investigations shall be conducted in the workspace designated by the Germantown Police Department chief of police.

B. Case Predication and Prioritization

1. Cases may be initiated by referrals from the Cyber-Tipline, electronic service providers, other law enforcement agencies, by information gathered through suspect interviews, documented public sources, direct observations of suspicious behavior, public complaints, or by any other acceptable sources.

2. ICAC supervisors and their designees are responsible for determining investigative priorities and selecting cases for investigation. Assuming that the information is deemed credible, the determination should begin with an assessment of the victim's risk and then considerations of other factors, such as jurisdiction and known offender behavioral characteristics. The following prioritization scale was established by the ICAC Task Force and will apply to the opening and assignment of cases within the Germantown Police Department:

   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.

   d. Traders of pornographic images that appear to be home photography with domiciled children.

   e. Aggressive, high-volume child pornography traders who are commercial distributors, repeat offenders, or specialized in sadistic images.

   f. Traders and solicitors involved in high-volume trafficking or who belong to an organized child pornography ring that operates as a criminal conspiracy.

   g. Traders in previously known images.

   h. Traders in digitally altered images.

V. RECORDKEEPING

The Germantown Police Department's Electronic Crime/Internet Crimes Against Children (ICAC) detectives shall be subject to the existing Germantown Police Department's reporting and supervision procedures.

Electronic Crime/ICAC detectives will obtain a Germantown Police Department incident number at the beginning of each case and will fully document their activities through the completion of the case, including supplemental reports. All reports will be stored in the Germantown Police Department's computer server's ICAC folder, and this folder shall only be accessible by Electronic Crime/ICAC detectives and Investigations Division supervisors. Completed reports shall be printed and submitted to a supervisor for review. No images of child pornography are to be uploaded to any servers.

Germantown Police Department Electronic Crime/ICAC detectives will submit their activity report to the ICAC Task Force commander with the Knoxville, Tennessee Police Department by the 10th day of each month, using the appropriate ICAC forms.

VI. UNDERCOVER INVESTIGATIONS

A. 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 sexually exploit children. However, these investigations can trigger serious legal and ethical considerations due to concern that inappropriate government conduct may induce an otherwise innocent citizen into committing a crime.

B. All undercover investigations shall be conducted in a manner consistent with the principles of due process. Electronic Crime/ICAC detectives will avoid unlawful . inducement of any individual not otherwise disposed to committing the offenses being investigated and will not engage in conduct that is shocking or offensive to notions of fundamental fairness as described in applicable case law. See, for example, *Jacobson v U.S.,* 503 U.S. 540 (1992) and *U.S. v. Archer,* 486 F.2d (2nd Cir.1973).

C. Electronic Crime/ICAC detectives should always be aware that their actions, in addition to those of the suspect, may be at issue in deciding if charges are placed, whether referrals to other law enforcement agencies are acted upon, and as a factor in determining the guilt or innocence of the suspect at trial. Therefore, it is critical that Electronic Crime/ICAC detectives work closely with state and/or federal prosecutors when investigating ICAC offenses.

D. The following standards apply to all undercover investigations:

1. Only sworn, on-duty investigative personnel will conduct ICAC investigations in an undercover capacity. Private citizens shall not be asked to seek out possible suspects nor will they be authorized to act as police agents in an online undercover capacity.

2. Employees shall not, under any circumstances, upload, transmit, or forward

pornographic or sexually explicit images.

3. Other than photographs of law enforcement officers who have provided their informed written consent, no human images shall be uploaded, transmitted, or forwarded by ICAC Task detectives.

4. Other than where authorized above, images considered for uploading shall be approved by a supervisor and reviewed by the state and/or federal prosecutor. Sexually suggestive titles shall not be used.

5. During online dialogue, undercover officers shall allow the suspect to set the tone, pace, and subject matter of the initial online conversation. Image uploading shall be initiated by the suspect.

VII. EVIDENCE PROCEDURES

A. All undercover online activity shall be recorded and documented. Any deviations from this policy due to unusual circumstances shall be documented in the relevant case file and reviewed by an Investigations Division supervisor.

B. The storage, security, and destruction of investigative information shall be consistent with existing evidentiary policy and procedures. A safe within the computer investigations workspace is to only be used as a temporary storage of evidence during an active investigation, and a chain of evidence log will be maintained. Access to investigative files and any evidence collected shall be restricted to authorized personnel with a legitimate need to know.

C. Only qualified personnel who have received specific training in this field will conduct forensic examinations of computers and related evidence.

VIII. EXAMINATION PROCEDURES

A. If the investigator assigned to the case is not an Electronic Crime/ICAC detective, then the detective shall complete a request for examination and coordinate together on securing either a consent to search with a waiver or a search warrant, identifying the computer and for what evidence they are searching. Absent a signed consent and waiver form, a search warrant will be required.

B. Once the appropriate paperwork has been acquired and completed, the examiner shall make a request of a property room custodian, so that they may remove the hard drive(s) from the suspect's computer. The hard drive(s) must be documented by identifiers, such as model and serial number, prior to examination on a Computer Forensic Exam Checklist form.

C. The Electronic Crime/ICAC detective shall prepare a forensically-wiped hard drive

for imaging the suspect's hard drive.

D. Only after all appropriate paperwork has been acquired and completed will the suspect's hard drive(s) be moved to the computer investigations workspace. The suspect's hard drive(s) shall only be stored temporarily in the computer investigations workspace during the image process, including verification. Once the image and verification are complete, the suspect's hard drive(s) shall be returned to the property and evidence room.

E. At the completion of the exam, the Electronic Crime/ICAC detective shall complete a report of exam, via the forensic software, to include any images or files of evidence found and will then file an investigative supplement to the original case report.

IX. INFORMATION SHARING

Conventional boundaries are virtually meaningless in the electronic world of the Internet, and the usual constraints of time and distance do not apply. These factors increase the possibility of investigators targeting one another, investigating the same subject, or inadvertently disrupting an ongoing investigation. To foster coordination, collaboration, and communication, investigators are required to contact law enforcement where an investigation may occur if outside Germantown City limits. If the agency has the capabilities to investigate, then ICAC detectives may assist, if needed, and may follow up for a disposition. If the agency does not accept jurisdiction, then the ICAC detectives shall notify their supervisor.

X. SUPERVISION

A. Existing agency supervisory systems and procedures shall apply, with specific emphasis observation, documentation, and periodic evaluation of cases assigned to investigators. Given the nature of these investigations, consistent and on-going supervision of these cases and investigative personnel assigned to computer investigations is essential.

B. Management or supervisory practices shall include:

1. Periodic review of undercover session records.

2. Participation in formulating undercover investigative plans and establishing investigative priorities.

3. Development of work schedules including approval of specific overtime expenditures.

4. Assessment of equipment and training needs.

5. Review and approval of any fiscal matters.

XI. SELECTION OF PERSONNEL

A. The commander of the Investigations Division will be responsible for making all assignments of eligible detectives for Electronic Crime/ICAC investigations.

B. Prospective Electronic Crime/ICAC investigative candidates will be evaluated for work history that indicates prior investigative experience, court testimony skill, ability to handle sensitive information prudently, and a genuine interest in computers and the protection of children. Candidates must have demonstrated the ability to perform well under pressure and posses the emotional stamina needed to investigate cases of a graphic sexual nature involving children that can be emotionally disturbing.

C. Eligible candidates must have investigative experience, be computer literate, knowledgeable regarding child exploitation issues, and familiar with federal and state statutory case law pertaining to Electronic Crime/ICAC investigations.

D. Due to the sensitive nature of these investigations, the length of this assignment will be determined by the Investigations Division commander.

XII. TRAINING

Initial training for Electronic Crime/ICAC detectives shall include, but not be limited to the following:

A. Computer crimes

B. Basic data recovery

C. FBI cyber crimes

D. USSS electronic crime

E. ICAC Investigative Techniques

F. ICAC U/C Chat Investigations

G. ICAC Peer to Peer Investigations

H. Computer Forensics with Forensic Recovery of Evidence Device (FRED)

I. Access Data FTK

J. Encase or approved substitute

K. Other training may include, but shall not be limited to, on-the-job training by other Electronic Crime/ICAC detectives and/or approved courses.

XIII. PREVENTION AND EDUCATION ACTIVITIES

Prevention and education activities are a critical component of the Germantown Police Department's proactive stance against electronic crimes and crimes against children. Consequently, supervisors and investigators are expected to develop and lead prevention programs to foster awareness and provide practical and relevant guidance to children, parents, educators, librarians, first responders, other investigators, and other individuals concerned about child safety issues. Presentations to school staff, parents, community groups, and police in-service training are excellent ways to promote awareness. However, these presentations shall not depict identifiable victims nor shall they use pornographic or sexually explicit images. **Presenters shall not discuss investigative techniques outside of law enforcement.** One valuable source of educational information is the Exploited Child Unit of the National Center for Missing and Exploited Children (NCMEC), which can be reached at (800) 843-5678 or through e-mail at exploited@ncmec.org. The Department of Justice recommends Cyberethics for Parents and Educators and Cyberethics for Kids and Cyberethics, which are websites providing information on developing and delivering awareness and safety education programs.

Germantown Police Department's Electronic Crime/ICAC detectives shall strive to provide a prevention presentation at least six times per year to a variety of persons.

XIV. REVIEW PROCESS

An annual review of this policy will be conducted to determine if it should be revised, cancelled or continued in its present form.

This policy shall remain in effect until revoked or superseded by competent authority.