UNION COUNTY PROSECUTOR'S OFFICE **STANDARD OPERATING PROCEDURE**			
VOLUME: **2021**	CHAPTER: **011**	# OF PAGES: **36**	
SUBJECT: **CYBER CRIME TASK FORCE**			

EFFECTIVE DATE: OCTOBER 13, 2021	**REVISIONS**		
	DATE	**PAGE #**	**SECTION**
ISSUED BY: HARVEY A. BARNWELL CHIEF OF DETECTIVES _____ **UNDER THE AUTHORITY OF:** WILLIAM A. DANIEL PROSECUTOR			

PURPOSE

The purpose of this policy is to establish written guidelines to direct and provide guidance to the sworn law enforcement personnel under the direction of the Union County Prosecutor's Office Cyber Crime Task Force

POLICY

The Union County Prosecutor's Office Cyber Crime Task Force was created on March 5, 2019. The Task Force combined the Electronic Surveillance Unit, High-Tech Crimes Unit, and the Internet Crimes Against Children (ICAC) Unit, and will include, when assigned, on-loan officers from Union County municipal police departments. This agency recognizes that technology is an important part of nearly every law enforcement investigation, and the Cyber Crime Task Force was formed to streamline the agency's technological investigative functions, while giving municipal police departments the opportunity to have their officers trained in such disciplines. It is the policy of the Union County Prosecutor's Office to manage the administrative and operational functions of the Cyber Crime Task Force in an effective and efficient manner through the procedures outlined within this directive.

PROCEDURE

A. Duties & Responsibilities

1. The Cyber Crime Task Force shall be responsible for investigating the following:

   a. Internet Crimes Against Children (ICAC). These investigations include any investigation where digital technology is used in the exploitation of children. The CCTF will investigate all CyberTipline reports referred from the National Center for Missing and Exploited Children (NCMEC) and, when deemed appropriate by the Special Prosecutions Legal Supervisor or Investigations Supervisor, referrals

from local police departments regarding investigations into the possession and/or distribution of child sexual abuse material.

b. When deemed appropriate by the Special Prosecutions Legal Supervisor or Investigations Supervisor, referrals from local police departments regarding investigations into the sharing of revealing or sexually explicit images or videos of a person on the Internet without the consent of the subject and in order to cause them distress or embarrassment, commonly referred to as "Revenge Porn."

c. When deemed appropriate by the Special Prosecutions Legal Supervisor or Investigations Supervisor, referrals from local police department regarding investigations into Cyber Harassment and/or Cyber Stalking.

2. The Cyber Crime Task Force shall be responsible for providing the following support functions and investigative techniques to the other units within the Union County Prosecutor's Office, local Union County police agencies, and outside police agencies requesting assistance:

[redacted]

i. Video Collection and Enhancement

   1) Collection, documentation, and analyzation of video evidence.

   2) Enhancement of video evidence.

   3) Extraction of video evidence directly from a hard drive.

j. Video Compilation

   1) Compilation of video clips on a timeline in a linear video editor.

   2) Use of software to redact/blur/zoom video.

k. Audio editing

   1) Redaction or amplification of audio clips.

[redacted]

[redacted]

3. The Cyber Crime Task Force shall be responsible for providing training to the assigned on-loan officers from local Union County police departments, which is separated into two training tracks referred to as “Track 1: Technical Operations Technician (TOT)” and “Track 2: Digital Forensics Examiner (DFE).”

4. The Cyber Crime Task Force shall be responsible for teaching assigned classes at the John H. Stamler Police Academy, to include Cell Phone Bootcamp and Cyber Crime Scene & Internet Investigations. The Cyber Crime Task Force shall also be responsible for conducting presentations or teaching classes regarding Cyber Crime related topics requested and approved by the Chain of Command of the Union County Prosecutor’s Office.

5. As the Cyber Crime Task Force detectives attend additional training or obtain additional certifications, and if the personnel of the Cyber Crime Task Force changes, the capabilities of the Cyber Crime Task Force may change. It will be the Cyber Crime Task Force Commander’s responsibility to adjust the duties and responsibilities of the Cyber Crime Task Force as the capabilities change.

B. Task Force Composition

[redacted]

2. The composition of the task force is at the discretion of the Chief of Detectives, and may be changed at any time.

3. On-loan officers are assigned to the Cyber Crime Task Force by the Commander with approval through the Chain of Command of the Union County Prosecutor’s Office,

after a request is made by a Chief of Police from a local police department, or his/her designee.

a. On-loan officers must be assigned to the Cyber Crime Task Force for a minimum of six weeks plus a one-week training course to complete Track 1.

b. On-loan officers must complete Track 1 prior to being assigned to Track 2.

c. On-loan officers must be assigned to the Cyber Crime Task Force for a minimum of four weeks plus a one-week training course to complete Track 2.

C. Legal Reporting/Guidance

1. The Cyber Crime Task Force will report directly to the legal staff of the Special Prosecutions Unit for all reactive/CyberTipline-related ICAC investigations.

2. The Cyber Crime Task Force shall seek legal guidance from the legal staff of the unit who requested assistance when providing the above-mentioned support functions and investigative techniques. If the request for assistance was made by an outside agency, the Cyber Crime Task Force shall seek legal guidance from the legal staff of the Special Prosecutions Unit and Major Crimes Division Legal Director, who will determine which assistant prosecutor will be assigned.

D. Work Environment

[redacted]

E. On-Call Schedule

1. The Cyber Crime Task Force Lieutenant/Commander or his/her designee shall prepare an on-call schedule via memorandum of the assigned detectives who shall be responsible for responding when assistance is requested of the Cyber Crime Task Force for at least the upcoming week.

2. The Cyber Crime Task Force on-call schedule shall include a primary on-call detective.

3. It is the responsibility of the on-call detective to make any necessary on-call coverage changes and make proper notifications.

4. The Cyber Crime Task Force on-call schedule shall be provided to the appropriate personnel in the Union County Police Department, as well as the appropriate personnel from the Union County Prosecutor's Office and any personnel on the schedule.

F. On-Call Response

1. Prior to responding to any scene, an on-call detective must notify the Cyber Crime Task Force Sergeant.

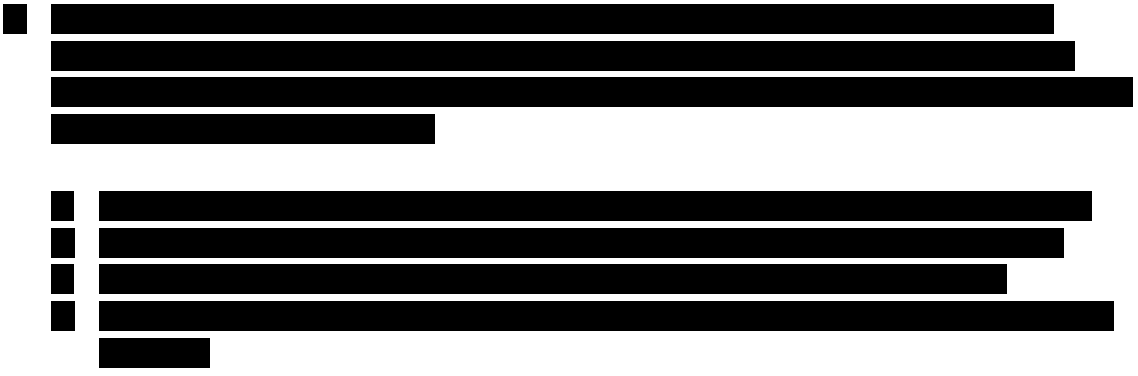
2. While in the field during a call-out, an on-call detective must update the Cyber Crime Task Force Sergeant of his/her progress, so that it can be determined if additional personnel is needed.

3. When an on-call detective clears from a scene, and has been dismissed, he/she must notify the Cyber Crime Task Force Sergeant.

G. Training

1. All training requests must be submitted via a Request for Training memorandum through the chain of command for approval. If there are costs associated with the training, a Union County E.P.E.C. form must also be submitted.

2. The Commander of the Cyber Crime Task Force shall maintain a training record for each detective assigned to the Task Force.



[redacted]

[redacted]

6. The Cyber Crime Task Force detectives who conduct ICAC investigations should also attend additional training related to ICAC. The Cyber Crime Task Force detectives are expected to attend training related to emerging technology and trends in ICAC, and are encouraged to continually seek new training in technology and investigative enhancements pertaining to ICAC.

7. In order to perform any of the above-mentioned support functions and investigative techniques mentioned in the Duties and Responsibilities section of this policy, the Cyber Crime Task Force detective must have attended a training course related to the function or technique and/or be proficient in the use of any software or technology used to perform said function or technique. If a Cyber Crime Task Force detective has not attended a training course related to the function or technique, but has prior experience conducting the function or technique, it will be up to the discretion of the Cyber Crime Task Force Commander if the detective can complete the function or technique.

8. In order to conduct forensic examinations on mobile or cellular devices, a Cyber Crime Task Force detective must be trained and certified in the use of the software he/she would use to conduct the examination.

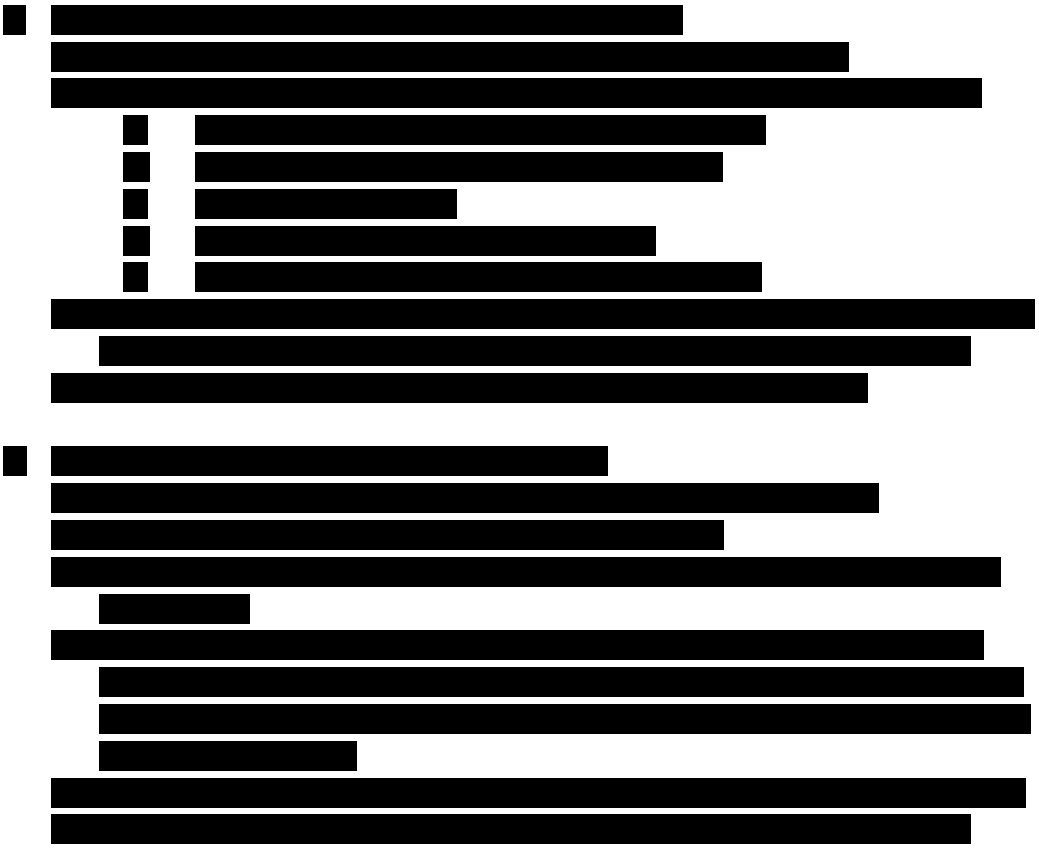
9. In order to conduct forensic examinations on computers and/or devices with the Windows Operating System, a Cyber Crime Task Force detective must be trained and certified in the use of the software he/she would use to conduct the examination.

10. In order to conduct forensic examinations on computers and/or devices with the Mac Operating System, a Cyber Crime Task Force detective must be trained and certified in the use of the software he/she would use to conduct the examination.

11. In order to recover video from security cameras for criminal investigations, a Cyber Crime Task Force detective must be trained in recovering video, and must have attended the Recovery of Evidence from CCTV Video Recording (RECVR) course at FLETC, the LEVA Level 1: Forensic Video Analysis & The Law course, or a course with the equivalent training, or be proficient in the recovery of evidence due to prior experience. The Cyber Crime Task Force Commander will determine if an equivalent course and/or experience is sufficient enough for the Cyber Crime Task Force detective to recover video evidence.

12. The Cyber Crime Task Force detectives who perform the support functions and investigative techniques mentioned in the Duties and Responsibilities section of these Standard Operating Procedures, should also attend additional training related to these functions and techniques. The Cyber Crime Task Force detectives are encouraged to continually seek new training in technology and techniques related to Cyber Crime.

13. The on-loan officers assigned to the CTTF must complete two tracks of training which are referred to as "Track 1: Technical Operations Technician (TOT)" and "Track 2: Digital Forensics Examiner (DFE)." The training tracks shall consist of the following.



14. The training received by the on-loan officers assigned to the CTTF may be amended at any time due to scheduling conflicts and availability of training courses.

H. Wellness

1. ICAC investigations expose the Cyber Crime Task Force detectives to graphic images and videos of child sexual abuse material. These images and videos may have an effect on the members of the Cyber Crime Task Force. Because all the Cyber Crime Task Force detectives are exposed to child sexual abuse material, whether they are conducting ICAC investigations or forensic examinations on devices seized during

ICAC investigations, all the Cyber Crime Task Force detectives will adhere to the following guidelines:

a. The Cyber Crime Task Force detectives must attend "Shift Wellness Foundation in Mental Health," a one-day training for individuals exposed to child exploitations.

b. The Cyber Crime Task Force detectives are required to complete one training course annually on topics including, but not limited to Stress Management, Trauma and Resiliency.

c. The Cyber Crime Task Force detectives are to be familiar with the Union County Employees Assistance Program in the event they need personal assistance.

d. The Cyber Crime Task Force detectives are encouraged to leave their workspace and take breaks in the event of prolonged exposure to child sexual abuse material.

I. Peer Review

1. Peer review is an important component of digital forensics. A review of digital forensic examinations are a review of reports describing the results of an examination, and is not a validation of the equipment. A review of these examinations should be conducted for the following reasons:

   a. It constitutes an independent and objective review of the examiner's objectives, methodology and calculations. A fresh set of eyes can provide a different and much needed perspective on the examiner's work.

   b. It assesses whether the requisite analysis has been undertaken and if any further work is merited.

   c. The reviewer provides commentary as to the soundness of any opinions and conclusions reached.

   d. The reviewer offers suggestions on report structure and grammatical issues.

2. A Cyber Crime Task Force detective's digital forensic examination shall be reviewed by another Cyber Crime Task Force detective when the detective who conducted the examination is expected to testify in court at an evidentiary hearing and/or trial. The guidelines for such reviews will be set forth in this Standard Operating Procedure.

J. Forensic Tool/Software Validation

1. The Cyber Crime Task Force will use various forensic tools and software to conduct the support functions and investigative techniques listed in the Duties and Responsibilities section of this Policy. Cyber Crime Task Force detectives will only

utilize hardware and software which is fully licensed for professional use and owned by the Union County Prosecutor's Office or another government agency.

2. These forensic tools and software must be validated because it is important to ensure that they are working properly and suitable for their intended purpose. For these purposes, validation is defined as an evaluation to determine if a forensic tool or software is functioning correctly and as intended by the manufacturer.

3. All forensic tools and software used by the Cyber Crime Task Force will be validated upon initial purchase or acquisition, prior to being used for any of the support functions and investigative techniques.

4. All forensic tools and software used by the Cyber Crime Task Force will be re-validated when a major update is released for the forensic tool or software. For these purposes, a major update is defined as a full version number change.

5. The guidelines for forensic tool/software validation will be set forth in the Procedures section of this Standard Operating Procedure.

K. Report System

1. Reports for ICAC Investigations:

   a. All Cyber Crime Task Force reports and updates for ICAC investigations shall be completed or documented in Infoshare.

   b. While an ICAC investigation is in the Intake stage of Infoshare, all pertinent information for the investigation shall be documented in the Intake Detail section of Infoshare.

   c. If an ICAC investigation has been approved to move to the Investigation stage of Infoshare, all pertinent information must be documented in either an Investigation Report, Supplemental Report, or Arrest Report.

   d. All Cyber Crime Task Force reports completed for the Investigation stage shall first be submitted through the Cyber Crime Task Force Chain of Command as a draft hard-copy and/or emailed Microsoft Word document for review.

   e. Once the draft of a report has been approved by the Cyber Crime Task Force Sergeant and Cyber Crime Task Force Commander, it may be submitted via the workflow in Infoshare.

   f. Cyber Crime Task Force detectives will be responsible for maintaining a case file for their ICAC investigation and shall do so pursuant to the policy set forth by the

Union County Prosecutor's Office, and with the guidance set forth in the ICAC Investigation section of this SOP.

g. Details that will be included in the Intake Detail and in reports were mentioned with further detail in the ICAC Investigations section of this SOP.

2. Reports for support functions and investigative techniques requested by other units within the Union County Prosecutor's Office, local Union County police agencies, and outside police agencies requesting assistance:

a. All Cyber Crime Task Force reports for support functions and investigative techniques requested by other units within the Union County Prosecutor's Office, local Union County police agencies, and outside police agencies shall be completed on an appropriate Cyber Crime Task Force form and uploaded to ASAP to the corresponding ASAP ticket.

b. All Cyber Crime Task Force reports shall first be submitted through the Cyber Crime Task Force Chain of Command as a draft hard-copy or emailed Microsoft Word document for review.

c. Once the draft copy of a report has been approved by the Cyber Crime Task Force Sergeant and Cyber Crime Task Force Commander, it should then be uploaded to the ASAP ticket with all supporting documents and/or notes for that request.

Note: If the completion of a support function or investigative technique by a Cyber Crime Task Force detective results in the identification, arrest, or apprehension of a suspect in an active investigation, the Cyber Crime Task Force detective shall expedite his/her investigation report and complete it immediately. Additionally, the report shall be completed regardless if the evidence has been returned to the submitting detective.

L. Evidence System

1. The Cyber Crime Task Force shall use the BEAST Evidence System to document the chain of custody of all evidence seized during ICAC investigations and submitted to the Cyber Crime Task Force Forensic Lab for examination.

2. When a Cyber Crime Task Force detective is conducting an ICAC investigation, all evidence seized during the investigation must be submitted via the BEAST.

a. If the evidence is to be submitted to the Cyber Crime Task Force Forensic Lab, the Cyber Crime Task Force case detective for the ICAC Investigation should submit the evidence to the Cyber Crime Task Force Forensic Lab.

b. All evidence not being submitted to the Cyber Crime Task Force Forensic Lab must be submitted to the High Tech Temporary Vault.

c. All evidence submitted to the High Tech Temporary Vault should only remain in the vault temporarily and/or as needed by the case detective. When it is no longer needed for investigative, Grand Jury or Trial purposes, evidence should be submitted to the Union County Prosecutor's Office Main Evidence Vault.

3. When a Cyber Crime Task Force detective is accepting evidence at the Cyber Crime Task Force Forensic Lab from another Union County Prosecutor's Office Unit, he/she must transfer custody to the Cyber Crime Task Force Forensic Lab.

   a. The detective must then place the evidence into a clear file folder along with a printout of the ASAP Ticket, BEAST Chain of Custody Receipt, and any other provided documents. One file folder shall be used for each item of evidence.

   b. The detective must then place the clear file folder with the evidence and paperwork in the Intake Drawer in the Cyber Crime Task Force Forensic Lab.

   c. The clear file folder with the evidence will remain in the Intake Drawer until the ASAP Ticket is assigned by the Cyber Crime Task Force Sergeant or Lieutenant/Commander. The Cyber Crime Task Force detective assigned to complete the examination may then remove the evidence from the Intake Drawer.

4. When a Cyber Crime Task Force detective is accepting evidence at the Cyber Crime Task Force Forensic Lab from an outside agency, he/she must create a new case in BEAST in order to accept the evidence into the Cyber Crime Task Force Forensic Lab.

   a. The detective must then place the evidence into a clear file folder along with a printout of the ASAP Ticket, BEAST Chain of Custody Receipt, and any other provided documents. One file folder shall be used for each item of evidence.

   b. The detective must then place the clear file folder with the evidence and paperwork in the Intake Drawer in the Cyber Crime Task Force Forensic Lab.

   c. The clear file folder with the evidence will remain in the Intake Drawer until the ASAP Ticket is assigned by the Sergeant or Lieutenant/Commander. The Cyber Crime Task Force detective assigned to complete the examination may then remove the evidence from the Intake Drawer.

5. When a Cyber Crime Task Force detective is accepting evidence on-scene from another Union County Prosecutor's Office Unit, or outside agency, the item should be

entered into BEAST in order to document the proper chain of custody. However, there may be circumstances when BEAST is not accessible to the submitting detective. In these circumstances, the Cyber Crime Task Force detective must document the chain of custody on a UCPO Field Transfer of Evidence form.

M. Ticketing System

1. The Cyber Crime Task Force shall use the ASAP Ticketing System produced by Support System to receive requests for support functions and investigative techniques from units within the Union County Prosecutor's Office and outside agencies. Each individual request or item submitted to the Cyber Crime Task Force Forensic Lab must have its own assigned ASAP Ticket.

2. The Commander of Cyber Crime Task Force and/or the Cyber Crime Task Force Sergeant shall be responsible for assigning tickets to the Cyber Crime Task Force detectives via Support System.

3. The Cyber Crime Task Force detectives shall be responsible for updating their assigned tickets in the ASAP System.

4. Tickets in the ASAP System will only be closed when the assigned work for the examination is completed and all of the corresponding reports and paperwork have been approved, and submitted to the Cyber Crime Task Force Commander.

N. ICAC Investigations

1. All of the Cyber Crime Task Force detectives must adhere to the Department of Justice ICAC Operational and Investigations Standards when conducting investigations.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

[redacted]

- [redacted]

- [redacted]

[redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

    - [redacted]

    - [redacted]

    - [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

- [redacted]

- [redacted]