GREENVILLE COUNTY
SHERIFF'S OFFICE

GO - 252

GENERAL ORDERS

COMPUTER CRIMES AND INTERNET CRIMES AGAINST CHILDREN

PURPOSE:

The Greenville County Sheriff's Office's (GCSO) Computer Crimes and Internet Crimes Against Children Unit (CCU/ICAC or "the Unit") exists to investigate all computer crime related offenses and serves as a part of the South Carolina Attorney General's Office Internet Crimes Against Children Taskforce. The Unit provides quality forensic services to the GCSO, the legal community, and the residents of Greenville County through the identification, collection, preservation, extraction, and interpretation of digital evidence from electronic storage devices.

AREAS OF INVESTIGATIVE AUTHORITY:

Computer Crimes: The Unit investigates all crimes outlined in the South Carolina Code of Laws Title 16, Chapter 16 ("Computer Crimes Act"). In instances where the technical aspect of a case exceeds the training of the investigators, investigators make proper referrals to state and federal law enforcement partners for assistance.

Digital Forensic Services: Members of the unit are certified to use forensic software and provide rapid forensic examinations of digital evidence to the GCSO as a whole. Deputies maintain and document the integrity of the original digital media for presentation in court, and to provide copies of electronic data evidence to investigators, prosecutors, and defense attorneys in accordance with applicable laws and judicial requirements.

Internet Crimes Against Children: The Unit maintains an active and leading role in the South Carolina ICAC Taskforce. The Unit is the primary recipient and investigative unit for Cybertips (online reports of child exploitation) provided by the National Center for Missing and Exploited Children for crimes occurring in Greenville County. ICAC related crimes are investigated both reactively and proactively, in an effort to reduce child exploitation in Greenville County.

DIGITAL FORENSICS SOFTWARE/HARDWARE USAGE RESTRICTIONS:

Digital forensic companies (such as Cellebrite, Magnet Forensics, Greyshift, Berla, etc.) provide proprietary hardware and software that are at the cutting edge of digital forensic capabilities. The Unit will respect and protect the intellectual property of the companies by fully

complying with any usage agreements and terms and conditions provided by each individual company and program.

Digital forensics software products are to be used within the scope of criminal investigations, internal investigations, or to assist in the data recovery for Greenville County owned devices. Any other usage must be approved by the Unit supervisor in advance.

USE OF DIGITAL FORENSICS SOFTWARE:

Consent or Warrant Required. The use of forensic software is permitted only when the deputy has obtained a signed written consent from the device owner or obtained a signed search warrant specific to that device. Notably, investigators must maintain working law enforcement accounts with any Electronic or Internet Service Provider to ensure rapid communication of legal process.

Use of Write Blockers. Whenever possible, original media should be connected to Sheriff's Office forensic computers through a hardware write blocker. This device ensures that no data can be changed or written to the original media.

Use of Forensic Copies. Prior to any forensic examination, outside of a forensic preview, a forensic image of the original media should be made using the proper software. Upon the completion of the creation of the forensic image investigators will verify the hash of the image to confirm it is a true copy. Forensic analysis of the image should be conducted and not an analysis directly from the original media.

DIGITAL FORENSICS QUALITY ASSURANCE:

Reporting. It is the responsibility of any member working in or for the digital forensics unit to report any quality assurance problem with any hardware, software, supply or material to the Sergeant of the Computer Crimes/ Internet Crimes Against Children Unit (SID-CCU/ICAC) immediately and suspend using the item until appropriate action is taken to remedy the problem. When a quality assurance problem with any hardware, software, supply, or material is encountered, it will be marked with an identifying sign or label stating "out of service" until the problem is corrected.

Software Updates. Personnel working within the unit have the responsibility to maintain and update all digital forensics unit software and documents as needed. Forensic Software is routinely updated by the vendor to adapt to changing technology; investigators are responsible for updating their forensic software as soon as practically possible to ensure evidence is being properly analyzed, parsed, and carved.

Verification of Data. Digital forensic software products are tools to assist investigators in rapidly processing large amounts of data collected from evidentiary devices. Investigators must have a working knowledge of how and where data is stored on evidentiary devices. Investigators should not solely rely on the presentation of data made of the forensic software and are responsible for independently verifying, as needed, the artifacts presented by the software.

PROCEDURES FOR HANDLING DIGITAL EVIDENCE:

The procedures outlined below are intended to work in harmony with the already existing procedures found in General Order 203 (Collection, Preservation and Disposal of Evidence).

Digital evidence, which includes forensic images, copies of digital media processed, and any derivative evidence, may be stored on the digital forensics unit server, on hard drives, magnetic/digital tapes, optical media (CDs, DVDs, Blu-Ray, etc.) or other backup media. Digital evidence may include forensic images created during analysis, or any data or files derived from forensic examinations or copied from suspect/source devices.

Digital evidence from forensic examinations must be stored and maintained within the Unit for at least a period of two (2) years, unless destruction is authorized by the primary investigator or the office of the appropriate prosecutor.

After a period of two (2) years, digital evidence maintained at the CCU/ICAC unit will be destroyed, archived, or stored in accordance with the standard procedures or in accordance with South Carolina state law, which requires that scientific evidence for specified crimes be maintained longer or indefinitely.

Original/physical evidence will be retained in the Unit during imaging or as long as necessary to conduct analysis. Original/physical evidence may remain in the Unit’s secured office space and/or secured storage location overnight and over prolonged periods as necessary to facilitate analysis/examination, as the Unit’s office space and/or assigned secure storage locations are authorized as departmental evidence room(s).

Digital evidence and case files will be stored within the CCU/ICAC unit on hard drives or magnetic tape and will be labeled with a case number. Reports made for Investigators outside of the CCU/ICAC unit will be provided to them via a shared drive transfer, an external storage device, or optical media. A copy of the report will also be

delivered to Property and Evidence, unless, the report is too large for a Blu-Ray disc, then the report will be stored in the Unit office. Investigators will note in their report where the evidence related to non-CCU/ICAC crimes was stored.

The Unit office will maintain limited access locks on all doors, video monitoring of common areas and storage rooms, and monitored alarm service. Access to the Unit work area, storage rooms, and offices will be limited to Unit investigators and their direct supervisors unless a Unit employee is present.

Child Sexual Abuse Material shall not be released to defense counsel unless directed by a court order and with approval of the prosecutor's office. Child Sexual Abuse Material in itself is contraband by law, which is illegal to possess. Investigators will make themselves available to meet with defense counsel in the Unit offices as needed so the defense or their designee can properly review data considered contraband in preparation for court.

Child Sexual Abuse Material will only be released to officers in person or through approved secure electronic means. Child Sexual Abuse Material should be encrypted during transport or transmission.

INTERNET CRIMES AGAINST CHILDREN:

The ICAC Unit obtains cases in four primary ways: (1) Cybertips from the National Center for Missing and Exploited Children, (2) Peer-to-Peer network investigations and referrals, (3) online chatting, and, (4) reports submitted by the Uniform Patrol or directly by the public.

National Center for Missing and Exploited Children

The National Center for Missing and Exploited Children (NCMEC) is the nation's central clearinghouse for all reports of child exploitation and child sexual abuse. Reports, commonly referred to as Cybertips, are submitted to NCMEC by online companies conducting business in the United States. The origin of the suspected criminal activity reported in the Cybertip is determined through the Internet Protocol (IP) addresses and other data, which is then forwarded to the appropriate taskforce. For instance, NCMEC might pass a Cybertip along to the South Carolina Attorney General's Office, which leads the statewide South Carolina ICAC Task Force, which in turn assigns the Cybertips to local investigators (such as the GCSO's ICAC Unit).

ICAC investigators must review all Cybertips in a timely manner. Cybertips will be triaged and investigators will determine each cases priority to be investigated. If there is not a distinguishing priority,

then the cases will be investigated in the order received. Upon conclusion of an investigation, a disposition of the Cybertip must be reported to the South Carolina Attorney General's Office.

Peer-to-Peer Investigations and Referrals

Peer-to-Peer investigations and referrals are governed by the ICAC Standards Manual. Investigators must be trained in operation and tools for each specific Peer-to-Peer network.

Chatting Investigations

Online chatting operations are governed by the ICAC Standards Manual and this agency will follow all established protocols for online chatting. Prior to any chatting, Investigators must complete an approved course in online chatting.

Prosecution

The Greenville County Sheriff's Office maintains an agreement with the South Carolina Attorney General's Office and the 13th Circuit Solicitor's Office regarding the prosecution of child exploitation cases. All ICAC related cases will be forwarded to the Attorney General's Office ICAC section for prosecution. Upon the arrest of an individual for an ICAC related case the investigator, whether an ICAC investigator or not, will complete a SCAG arrest sheet and forward to the Attorney General's Office. Investigators are required to maintain communication with prosecuting attorneys and provide all case related files to their office in a timely manner.

REPORTING REQUIREMENTS TO EXTERNAL AGENCIES: Each month the Unit Supervisor, or their designee, is required to report statistics to supporting state and federal agencies.

Each month, Investigators will provide aggregated case statistics to the South Carolina ICAC Taskforce through the ICAC DATA SYSTEM website. These numbers are reviewed by the South Carolina Attorney General's Office and then submitted to the Office of Juvenile Justice and Delinquency Prevention.

Each month, Investigators conducting digital forensic examinations will provide a report of their work to any federal partner agency that requires such a report. The report will be made on the form provided by the federal agency.

TRAINING:

Due to the ever changing world of digital technology, investigators must maintain proficiency and understanding in current cellular, computer, and other digital technologies. This understanding will be supplemented through general digital forensic continuing education and tool specific training. Investigators must also receive training in the investigative protocols and maintain a current understanding of online child exploitation trends.

Certifications. Certain forensic tools have corresponding certifications offered by their developer to ensure proper usage and interpretation of the presentation of the data. Investigators must obtain, and maintain, certifications in any digital forensic software product they use during the course of their investigation. This policy should not be construed to mean that uncertified investigators cannot review data presented by the digital forensics software, but the interpretation of the presented data must be made by an investigator who is certified in that tool.

If a member of the department wishes to be considered for certification of a digital forensics tool they will submit a training request to their supervisor.

Hobart Lewis, Sheriff