Description of document:	US Secret Service (USSS) Electronic Crimes Special Agent Program (ECSAP) Directives, 2010-2015
Requested date:	10-July-2017
Release date:	14-December-2018
Posted date:	24-February-2020
Source of document:	FOIA Request United States Secret Service Communications Center (FOIA/PA) 245 Murray Lane Building T-5 Washington, D.C. 20223 Fax: 202-406-5586 Email: FOIA@usss.dhs.gov DHS FOIA / Privacy Act Online Request Submission Form

DEPARTMENT OF HOMELAND SECURITY
UNITED STATES SECRET SERVICE
WASHINGTON, D.C. 20223

Freedom of Information Act & Privacy Act Program
Communications Center
245 Murray Lane, S.W., Building T-5
Washington, D.C. 20223

Date: DEC 14 2018

File Number: 20171888

Dear Requester:

This is the final response to your Freedom of Information Act (FOIA) request, originally received by the United States Secret Service (Secret Service) on July 10, 2017, for information pertaining to the Electronic Crimes Task Force (ECTF) Investigative Handbook/Manual.

Enclosed are documents responsive to your request. In efforts to provide you with the greatest degree of access authorized by law, we have considered the reference material under the FOIA regulation, Title 5 U.S.C. § 552. Pursuant to this Act, exemptions have been applied where deemed appropriate. The exemptions cited are marked below.

In addition, approximately 44 page(s) were released, and approximately 14 page(s) were withheld in their entirety. An enclosure to this letter explains the exemptions in more detail.

☒ If this box is checked, deletions were made pursuant to the exemptions indicated below.

Section 552 (FOIA)

□ (b) (1) □ (b) (2) □ (b) (3) Statute:
□ (b) (4) □ (b) (5) □ (b) (6) □ (b) (7) (A) □ (b) (7) (B)
□ (b) (7) (C) □ (b) (7) (D) ☒ (b) (7) (E) □ (b) (7) (F) □ (b) (8)

The following checked item(s) also apply to your request:

□ Some documents originated with another government agency(s). These documents were referred to that agency(s) for review and direct response to you.

□ Some of documents, in our files, contain information furnished to the Secret Service by another government agency(s). These documents were referred to that agency(s) for review and direct response to you.

☒ Fees: In the processing of this FOIA/PA request, no fees are being assessed.

□ Other:

If you deem our decision an adverse determination, you may exercise your appeal rights. Should you wish to file an administrative appeal, your appeal should be made in writing and received within sixty (60) days of the date of this letter, by writing to: Freedom of Information Appeal, Deputy Director, U.S. Secret Service, Communications Center, 245 Murray Lane, S.W., Building T-5, Washington, D.C. 20223. If you choose to file an administrative appeal, please explain the basis of your appeal and reference the case number listed above.

If you have any questions or would like to discuss this matter, please contact this office at (202) 406-6370. FOIA File No. 20171888 is assigned to your request. Please refer to this file number in all future communication with this office.

Sincerely,

Kim E. Campbell
Special Agent In Charge
Freedom of Information Act & Privacy Act Officer

Enclosure:

☒ FOIA and Privacy Act Exemption List

FREEDOM OF INFORMATION ACT
SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

Provisions of the Freedom of Information Act do not apply to matter that are:

(b) (1) (A) specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;

(b) (2) related solely to the internal personnel rules and practices any agency;

(b) (3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b) (4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b) (5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b) (6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b) (7) records or information compiled for law enforcement purposes, but only to the extent that the information: (A) could reasonable be expected to interfere with enforcement proceedings; (B) would deprive a person of a right to a fair trial or an impartial adjudication; (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy; (D) could reasonable be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source; (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law; (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b) (8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for regulation or supervision of financial institutions;

(b) (9) geological and geophysical information and data, including maps, concerning wells.

PRIVACY ACT
SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

The provisions of the Privacy Act do not apply to:

(d) (5) material compiled in reasonable anticipation of civil action or proceeding;

(j) (2) material reporting investigative efforts pertaining to enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) material is currently and properly classified pursuant to an Executive Order in the interest of national defense or foreign policy;

(k) (2) material compiled during investigations for law enforcement purposes;

(k) (3) material maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of Title 18;

(k) (5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or for access to classified information, but only to the extent that the disclosure of such material would reveal the identity of the person who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or prior to the September 27, 1975, under an implied promise that the identity of the source would be held in confidence;

(k) (6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process;

Electronic Crimes Special Agent Program

Table of Contents

United States Secret Service
Directives System

Manual : Electronic Crimes Special Agent Program
RO : CID

Section : ECSAP
Date : 09/10/2010

Subject: Electronic Crimes Special Agent Program

To: All Supervisors and All Manual Holders of the Electronic Crimes Special Agent Program

Filing Instructions:

- Remove and destroy sections ECSAP-01 thru ECSAP-10 in entirety (including any tables of contents, policy memoranda, and/or official messages that may be filed in these sections) and replace with the attached revised sections.

- File this Policy Memorandum in front of this section.

- This directive is in effect until superseded.

Impact Statement: This directive advises that the Electronic Crimes Special Agent Program (ECSAP) Manual has been updated throughout to reflect current Criminal Investigative Division/ECSAP policy and procedures. More specific changes to this directive are as follows:

- References to the previous Electronic Crimes Section (ECS) have been changed to reflect the new Computer Forensics and Research Development Branch (CFRB).

- Two new sections have been added to the Electronic Crimes Special Agent Program. Therefore, language has been added throughout advising of the new National Computer Forensics Institute (NCFI) in Hoover AL, and the Cell Phone Forensics facility in Tulsa, OK.

- Language has been incorporated advising that Computer Forensics (CF) examiners are now required to sign a contract with the United States Secret Service (USSS) prior to their entrance into the Electric Crimes Special Agent Program.

- The "On-line Reporting System" has replaced the Master Control Index (MCI) reporting requirements/procedures for receiving exam, preview, and clean room credit.

- Verbiage regarding the departure of ECSAP agents from the Electronic Crimes Special Agent Program has been revised.

Mandatory Review: The Responsible Office will review all policy contained in this section in its entirety by or before September 2013.

Questions regarding this policy should be directed to the Office of Investigations, Criminal Investigative Division at 202-406-9330.

Michael Merritt

Michael Merritt
AD - Investigations

DCP#: ECSAP 2010-02

ELECTRONIC CRIMES SPECIAL AGENT PROGRAM (ECSAP)

The U.S. Secret Service (USSS) Electronic Crimes Special Agent Program (ECSAP) provides digital evidence recovery support for USSS investigations as well as Local, State and other Federal law enforcement agencies.

Introduction

The USSS ECSAP has grown significantly since its inception in 1987. This growth has come in response to a corresponding rise in the number and types of duties (investigative and protective) that involve electronic media and emerging technologies. The investigations vary throughout the spectrum of standard USSS violations (i.e., counterfeiting, threats to USSS protectees, computer crimes, access device fraud, etc.) to network intrusions, child molestation, kidnapping and murder. In order to more effectively meet this challenge, it is essential that ECSAP agents follow an established procedure when conducting digital evidence analysis and electronic crimes investigations. This policy provides general guidance for agents conducting digital evidence recovery and analysis, and is an attempt to standardize ECSAP forensic procedures to reduce the number of procedural questions and conflicts.

Scope

The standards and procedures contained herein are evolving along with this field. Given the dynamic nature of computer forensics, not every scenario can be accounted for, nor does every exam or investigation follow the same path to resolution. Therefore, this policy should be viewed as a general guide to for conducting electronic evidence examinations.

This policy will not specifically discuss each and every type of device that may be encountered. Adequate documentation covering many types of devices already exists in the form of ECSAP Program, Computer Forensics (ECSAP-CF) training manuals and ECSAP Standard Operating Procedures (SOPs), and it would not be practical to cover each device sufficiently within the context of this document.

This policy is not intended to supersede any current or future regulations established by the USSS.

Mission

The primary mission of the ECSAP is to provide digital evidence recovery support to personnel investigating violations of laws falling under the jurisdiction of the USSS. Additionally, the ECSAP works in conjunction with local, State and Federal law enforcement agencies as deemed appropriate.

Laboratory Objectives

United States Secret Service (USSS) Computer Forensics (CF) Laboratories refer to areas in which CF examiners perform forensic analysis of devices or systems that may contain digital evidence or are of interest to the USSS.

To provide a framework of standards, quality principles, and methodologies for the detection, recovery, examination and presentation of digital evidence for forensic purposes in compliance with established USSS policy.

To encourage a consistent methodology within the USSS, and hence the production of uniform results, to facilitate the exchange of data between the program and the law enforcement community.

To facilitate a training program which encourages laboratory staff to maintain proficiency in their areas of responsibility, and keep abreast of emerging technologies.

As required, to assist Local, State and Federal agency investigations by performing forensic analysis of digital evidence.

ELECTRONIC CRIMES SPECIAL AGENT PROGRAM (ECSAP)/ELECTRONIC CRIMES TASK FORCE (ECTF) PERSONNEL

The United States Secret Service (USSS) Electronic Crimes Section (ECS) was established within the Criminal Investigative Division (CID) to ensure the successful investigation of computer-related and telecommunications crimes in the field with appropriate oversight from CID.

It is essential that open vertical, horizontal, and diagonal channels of communication exist between the USSS Headquarters laboratory, field offices, and Electronic Crimes Task Forces (ECTFs) in order to facilitate dissemination of technical information.

Positions

The Electronic Crimes Special Agent Program (ECSAP) was designed in accordance with USSS Office of Investigations standards. It was developed to support the investigative and protective missions of the USSS. This support stems from personnel assigned to USSS Headquarters offices, field offices, resident offices, resident agencies, and ECTFs. ECSAP is managed by CID.

Several assets, to include regular staff meetings and e-mail distribution lists, are utilized to facilitate communication among personnel.

Headquarters Positions

Headquarters Electronic Crimes Section (ECS) Manager

The Headquarters CID-ECS Manager/Assistant Special Agent In Charge (ASAIC), is responsible for the overall administration of the laboratory and reports to the Deputy Special Agent In Charge (DSAIC), CID. Additional responsibilities include:

- Oversight of the ECSAP, ECTF, and Information Technology (IT) sections within ECS.
- Oversight of all personnel matters, team assignments, budgeting, procurement of equipment and facilities, liaison among participating agencies and serving as the top level supervisor at the laboratory.
- Ensuring all resources are effectively utilized and the appropriate number of personnel are assigned to each task.
- Ensuring performance expectations are understood by all laboratory personnel.
- Facilitating the administration of the laboratory standards to the regional task forces and field offices.
- Assigning acting supervisors.
- Delegating assigned duties.

Headquarters ECSAP Supervisor

The Headquarters ECSAP Supervisor/Program Manager is an Assistant to the Special Agent in Charge (ATSAIC) who is responsible for procedures of the ECSAP Program, supporting the ECSAP agents in the field with equipment, resources and training, and reports directly to the ECS Manager. The ECSAP Supervisor and/or designee liaise with other agencies and professional organizations at the Headquarters level, and act as the Headquarters ECS Program Manager during extended absences of the Headquarters ECS Program Manager. The Supervisor may also act as the ECTF or the IT Supervisor during extended absences of those positions. The ECSAP Supervisor will assign forensic examination cases (including special and classified exams) to ECSAP agents assigned to CID. If it is determined that additional manpower is needed on a temporary basis, the ECSAP Supervisor will request additional examiners/personnel from outside the division. The ECSAP Supervisor is responsible for the overall direction of the ECSAP and will delegate assigned responsibilities to ECS Operations agents/personnel.

Headquarters ECTF Supervisor

The Headquarters ECTF Supervisor/Assistant to the Special Agent in Charge (ATSAIC) is responsible for the policy and procedures of the ECTF Program and the Wireless Tracking Program. The ECTF supervisor also manages ECTF personnel in the field, and reports directly to the ECS Manager.

The ECTF Supervisor reports to the Headquarters ECS Program Manager and acts as the ECSAP, the IT Supervisor, or ECS Program Manager during extended absences of those incumbents. The ECTF Supervisor provides equipment, resources and training to ECTF members in support of the ECTF mission. The ECTF Supervisor also assists in facilitating strategic partnerships and oversees ECTF standards of measurement. The ECTF Supervisor delegates assigned responsibilities to Headquarters ECTF Operations agents/personnel.

Headquarters IT Supervisor

The Headquarters IT Supervisor/Assistant to the Special Agent in Charge (ATSAIC) manages the Information Technology Section (ITS), and reports directly to the ECS Manager. ITS is responsible for the integration of information technology solutions into investigations and anticipating future needs. ITS researches, develops, and delivers information technology solutions in support of the investigative mission of the Secret Service. ITS strives to deliver cross functional solutions that promote the collection, timely analysis, collaboration, and reporting of investigative information. ITS pursues state of the art technologies which serve the best interests of the Office of Investigations, the Criminal Investigative Division, and USSS field offices. ITS focuses on: enhancement of current technical support for field investigative operations; enhancement of knowledge discovery, knowledge management and information sharing capabilities; enablement of divisional support activities which ensure continued computer system operations and management; and technology exploration.

Headquarters Operations Assistant

The Headquarters Operations Assistant is responsible for general administrative support duties at the direction of the Headquarters Electronic Crimes Section (ECS) Supervisors.

Headquarters ECSAP/ECTF/IT Agents

The Headquarters ECSAP/ECTF/IT agents are computer forensic examiners who have completed the Preliminary/Basic Computer Evidence Training (PBCERT), or its equivalent as determined by the Headquarters ECSAP Supervisor. Headquarters ECSAP/ECTF/IT agents complete special or classified exams as assigned by the ECSAP Supervisor, and complete duties as assigned by their respective supervisors. Personnel assigned to the Headquarters ECS, who are not examiners, are allowed to perform administrative and field support functions as determined by the Electronic Crimes Special Agent Program (ECSAP) Manager/Assistant to the Special Agent in Charge (ATSAIC).

Regional Electronic Crimes Task Force Positions

Task Force Operations Supervisor

The Task Force Operations Supervisor is responsible for the overall administration of the Task Force Laboratory, and is responsible for all personnel matters, team assignments, budgeting, procurement of equipment and facilities for the Task Force, and liaison among participating agencies. The Task Force Operations Supervisor delegates assigned duties. The point of contact within CID for the Task Force Operations Supervisor is the Headquarters ECTF Supervisor. Assignment of forensic examination cases within the task force is done at the discretion of the Task Force Operations Supervisor. If it is determined that additional manpower is needed on a temporary basis, the Task Force Operations Supervisor may request additional examiners through the ECS.

Task Force Computer Forensic Examiner

The Task Force Computer Forensic Examiner is required to complete the PBCERT or its equivalent as determined by the Headquarters ECSAP Supervisor, prior to conducting examinations. The Computer Forensic Examiner reports to the Task Force Operations Supervisor on all forensics issues.

Task Force Operations Assistant

The Task Force Operations Assistant is responsible for general administrative support duties in support of the entire task force laboratory at the direction of the Task Force Operations Supervisor.

Field Offices, Resident Agencies, and Resident Offices

Field offices, resident agencies, and resident offices are referred to as "field offices" in the following section.

Field Office Electronic Crime Supervisor

The Field Office Electronic Crime Supervisor is responsible for daily administration of the field laboratory. The Supervisor's point of contact at CID is the Headquarters Operations Supervisor. Assignment of forensic examination cases within the field office is done at the discretion of the Supervisor. If it is determined that additional manpower is needed on a temporary basis, the Supervisor requests additional examiners through the ECSAP Supervisor.

Field ECSAP Agent

The Field ECSAP agent is required to complete the PBCERT or its equivalent as determined by the Headquarters ECSAP Supervisor prior to conducting examinations. ECSAP agents report to the Field Office Electronic Crime Supervisor for all issues and are expected to be available periodically for special/classified exams or when assistance is needed with complex cases or operations.

National Computer Forensics Institute

The National Computer Forensics Institute (NCFI), located in Hoover, Alabama is dedicated to the education and development of law enforcement professionals who investigate crimes that may contain digital evidence. The NCFI offers State and Local law enforcement officers training ranging from basic computer investigations to network investigations and the forensic recovery of digital evidence. The NCFI also offers courses to State and Local prosecutors and judges in an effort to educate and familiarize them with the investigative techniques and legal issues facing computer related investigations.

NCFI DIRECTOR

The NCFI Director is an Assistant to the Special Agent in Charge (ATSAIC) who is responsible for the management of all activities associated with the NCFI, and reports directly to the ECS Manager. The NCFI Director oversees the facility budget, class scheduling, provides guidance on nominee selections, approves all procurements for equipment and supplies, serves as the primary liaison for local contractors and vendors, and directs the activities of other NCFI personnel.

NCFI ASSISTANT DIRECTOR

The NCFI Assistant Director is a forensic examiner who acts as the daily operations supervisor. The NCFI Assistant Director oversees curriculum modifications and evaluates contract instructors. The NCFI Assistant Director is also responsible for the preparation of all invitational travel documentation and documentation related to courses offered at the NCFI. Additionally, the NCFI Assistant Director ensures all procured equipment and supplies are received, and maintains inventory of student-issued equipment.

Cell Phone Forensic Facility

U.S. Secret Service Cell Phone Forensic Facility Administrator

The U.S. Secret Service (USSS) Cell Phone Facility (CPF) Administrator is an ECSAP agent who is responsible for the daily operations of the facility. The CPF Administrator oversees the budget for the continuing operations of the CPF which includes the procurement of all equipment and items necessary for the facility's functioning. The CPF Administrator overseas USSS evidentiary compliance within the (CPF) and oversees facility research and development projects. Additionally, the CPF Administrator liaises with cell phone forensic vendors and industry experts, as well as completing forensic examinations and providing training to all areas of law enforcement.

Qualifications, Competence, Experience, and Departures

Electronic Crimes Special Agent Program (ECSAP) Program Manager

ECSAP Program Managers must be a GS-14 with managerial experience.

Operations Supervisors

Operations Supervisors must be supervisors familiar with ECSAP/ECTF operations, must have completed the USSS "Introduction to Supervision" training course, and must have reached the USSS journeyman level.

RIF

Operations Assistants

Operations Assistants must be familiar with the administrative responsibilities within the ECSAP/ECTF programs, must have completed one USSS course in administration; and must have administrative experience.

ECSAP Examiner

An ECSAP examiner must be a Special Agent GS-1811, and have completed the Preliminary/Basic Computer Evidence Training (PBCERT)., sponsored by either the Department of Treasury, the Department of Homeland Security, or its equivalent as determined by the Headquarters ECSAP Supervisor. The ECSAP Examiner should be familiar with the equipment, programs, and the USSS standard operating procedures for conducting digital evidence exams.

Each examiner must have experience in the methods used to conduct digital evidence recovery examinations and be able to testify to said methods and documentation.

ECSAP Examiner Development

The Basic Computer Evidence Recovery Training (BCERT) is used to develop and test the competency of apprentice ECSAP -CF Examiners.

New examiners must successfully complete a one-year probationary period. During this time, the examiner's immediate supervisor must review all ECSAP reports for accuracy. Upon the completion of the one-year probationary period, the Headquarters ECSAP Section will evaluate the progress of each examiner to ensure compliance with ECSAP computer forensics standards.

If examiners require assistance in the examination process, they can request assistance from the Headquarters ECSAP Section.

Departures of ECSAP Examiners from the ECSAP Program

ECSAP Examiners, who depart from any program within ECSAP, should contact the Headquarters ECSAP Section prior to their departure from either ECSAP program. ECSAP Examiners must coordinate their departures with the Headquarters ECSAP Operations Supervisor to ensure all ECSAP equipment and software in their possession has been accounted for and returned to the Headquarters ECSAP Section.

RIF

United States Secret Service
Directives System

Manual : Electronic Crimes Special Agent Program
RO : CID

Section : ECSAP-03
Date : 11/30/2011

Subject: Training and Assessment

To: All Supervisors and All Manual Holders of the Electronic Crimes Special Agent Program

Filing Instructions:

- Remove and destroy section ECSAP-03, Training and Assessment (dated 09/10/2010), in its entirety, and replace with the attached revised section.
- File this Policy Memorandum in front of this section.
- This directive is in effect until superseded.

Impact Statement: This directive advises of implementation of the standardization plan for development of Electronic Crimes Special Agent Program, Computer Forensics (ECSAP-CF) examiners. More specifically, a new section has been added entitled "Development of ECSAP-CF Examiners" which outlines the CF examiner selection process, and developmental requirements.

Mandatory Review: The Responsible Office will review all policy contained in this section in its entirety by or before November 2014.

Questions regarding this policy should be directed to the Office of Investigations, Criminal Investigative Division at 202-406-9330.

A.T. Smith
AD - Investigations

DCP#: ECSAP 2011-02

TRAINING AND ASSESSMENT

United States Secret Service (USSS) field office supervisors are responsible for managing the developmental and operational assignment of those Computer Forensic (CF) examiners under their supervision. Ideally, CF examiners must strive to conduct no less than 30 forensic examinations per year. If the workload of a CF examiner's office does not provide the opportunity to conduct this number of exams, supervisors should strongly encourage their examiners' participation when solicitations for CF examiners are made by the Criminal Investigative Division (CID), Electronic Crimes Special Agent Program (ECSAP) Manager. CF examiners who repeatedly fail to produce a sufficient number of CF examinations will be referred to the ECSAP Manager for a performance review. This review will consider the overall productivity of the CF examiner as compared to his/her peers, and will result in recommendation as to whether or not the examiner should remain in the CF program.

Development of ECSAP-CF Examiners

ECSAP-CF Examiner Selection Process

Agents interested in becoming ECSAP-CF examiners must meet the following selection criteria:

- Understanding of computers as determined by the completion of a Competency Assessment;
- Willingness to complete a four year assignment in the ECSAP Computer Forensics (ECSAP-CF) program;
- Acknowledgement of specialization requirements as outlined within this section; and
- Successful completion of a phone interview given by members of CID-ECSAP, that tests the candidate's understanding of computers, his/her willingness to complete a four year assignment to the ECSAP-CF program, and the acknowledgment of prescribed specialization requirements.

ECSAP-CF Examiner Training/Developmental Requirements

- Year one will consist of the selectee's successful completion of the Preliminary Basic Computer Evidence Recovery Training (PBCERT).

- Year two will consist of the CF examiner's successful completion of:
  - a. 30 or more total Computer Exam credits (and/or);
  - b. Advanced Computer Evidence Recovery Training (ACERT); and
  - c. Established Memory Acquisition and Analysis Training

- Year three will consist of the CF examiner's successful completion of:
  - d. 60 or more total Computer Exam credits (and/or)
  - e. Specialization Training in one or more of the following areas:
    - i. Cell Phone and other Mobile Device Forensics;
    - ii. Network Forensics;
    - iii. Macintosh Forensics;
    - iv. Linux; and/or
    - v. Advanced Windows Operating System (OS) Forensics – This will be the standard area of specialization of all CF examiners who do not specialize in another area of specialization.

- Year four will consist of advanced training selected within Year three.

Maintenance of Competency

CF examiners are provided professional development through an annual training conference, designated courses throughout the year, and continuing approved online courses. It is each examiner's responsibility to ensure that all training is updated within the Learning Management System (LMS).

Annual Certification

CF examiners will be given an annual proficiency exam. The Computer Forensics Research and Development Branch (CFRDB), formerly the Electronic Crimes Section (ECS), is responsible for preparing, administering, and evaluating the examination. ECSAP agents failing to demonstrate proficiency resulting from the examination will be required to attend remedial training. At the completion of remedial training, ECSAP agents must successfully demonstrate proficiency by completing an additional examination.

ECSAP examiners should attend the annual USSS ECSAP In-Service Training and participate in the online LMS, or similar training, to meet a minimum requirement of at least 40 or more hours of continuing education. Additional courses and training are available, and ECSAP-CF examiners are encouraged to request additional training through their immediate supervisors. ECSAP-CF agents who are unable to attend the annual USSS ECSAP-CF In-Service Training will be required to obtain an additional 40 hours of continuing education credits during that year.

ECSAP-CF agents are specialists in the examination of digital evidence. They provide expertise in the investigations of network intrusions and electronic evidence recovery in numerous types of cases. ECSAP agents located at Headquarters perform case management and provide support to ECSAP field agents and Electronic Crimes Task Forces (ECTFs), in addition to assisting with internal lab processing tasks (i.e., providing ECSAP agents and Regional Task Forces with lab supplies, hardware, and software).

Professional Certifications

In addition to the Treasury Computer Forensics Training Program (TCFTP) certification that each ECSAP-CF examiner receives upon completion of PBCERT and ACERT; each examiner is required to achieve both the Guidance Software's EnCE certification, and Access Data's ACE certification within one year of TCFTP certification. If the above certifications are not obtained within one year, ECSAP-CF examiners will face remedial action.

Quality Assurance/Peer Review

A review system will be employed throughout the ECSAP-CF program to ensure the quality of the CF examination process. This program will consist of the following components:

- Review of Exams – Every exam an ECSAP-CF agent creates will be administratively peer reviewed.
- Field Investigative Reporting System (FIRS)/Peer Review - FIRS will be used to coordinate the implementation of the Peer Review system.
- Technical Review of Reports – A random selection of open ECSAP exams will be conducted routinely. A second examiner will use the notes of the first examiner to repeat the examination process. A successful review will offer the same conclusions as the original exam.
- Peer Reviewers – Peer Reviewers will consist of senior ECSAP-CF examiners as determined by ECSAP/CID.

State/Local Examiners

State and local sworn law enforcement officers who have completed Preliminary Basic Computer Evidence Recovery Training (PBCERT), and work in an ECTF office, are authorized to conduct digital examinations for USSS cases and for other state and local agencies as deemed appropriate by the ECTF supervisor. Any such examinations must be done in accordance with any existing Memorandum of Understanding between their agency/department and the USSS.

Both Electronic Crimes State and Local Program (ECSLP) members, and state and local CF examiners who received their initial training at the National Computer Forensics Institute (NCFI) are requested to attend the annual ECSAP Conference, if sufficient funding is available.

Invitational Travel for State and Local Examiners

State and local CF examiners are occasionally requested to travel to attend training or assist with electronic crime investigations, exams, and projects. In addition to the guidelines set forth in the Administrative Manual, section FMD-08(02), Travel Authority, it is requested the submitting offices also follow the guidelines listed below relating to state and local examiners:

1. Submit an SSF 4000, Invitational Travel Request/Authorization for Non-Employees, to the CID/ECSAP, or CID/ECTF (if it is an ECTF office). CID will forward the SSF 4000 to the Office of Investigations (INV).

2. Once the SSF 4000 is approved by the Office of Investigations, and an authorization number has been issued, the approved form will be forwarded to the submitting office.

3. It will be incumbent on the submitting office to make hotel and flight reservations for the state and local examiner unless otherwise specified on the travel Official Message.

4. Upon completion of travel, the submitting office will assist the state and local examiner in completing a Travel Voucher Worksheet (SSF 3200), as well as an ACH Electronic Funds Transfer Form (SF 3881).

5. Submit the completed SSF 3200 and SF 3881 to the CID/ECSAP, or CID/ECTF along with all receipts and a copy of the approved SSF 4000. The packet will be approved in CID, and forwarded to the Financial Management Division (FMD) for reimbursement.

6. A database of all invitational travel will be maintained by the CID/ECSAP/ECTF.

EQUIPMENT

Requesting Equipment

Equipment Under $3000.00

When requesting equipment under $3000.00, the requesting agent must contact the Criminal Investigative Division/Electronic Crimes Section (CID/ECS), and provide the following information:

- Agent's name;
- Electronic Crimes Special Agent Program (ECSAP) Supervisor's Approval;
- Date of Request;
- Date Needed;
- Requesting agent's place of duty;
- Requesting agent's office phone number;
- Agent who was contacted about the request;
- Part #, property #, etc. if available;
- Description: A complete description of the needed item (brand, model, size, color, etc). Include the price of the item; and
- Vendor Information: This needs to be as complete as possible, to include vendor address, telephone number, Web site (if any), etc.

Prior to the purchasing the equipment, the CID-ECSAP Supervisor/ATSAIC must provide written approval. Once approved, the item may be purchased using the Purchase Card. Refer to the Administrative Manual sections FMD-18(03) and FMD-15(04) for information regarding use of the Purchase Card.

Equipment Over $3000.00

Any purchases over $3000.00 must be processed through the standard procurement process. Delivery and receipt of these purchases will be based on the dollar value and complexity of the procurement. Refer to the Administrative Manual, sections PRO-05, FMD-06(03), and FMD-06(04) for additional information regarding competition, and the handling of invoices for contracts and purchase orders respectively.

Accountability of Equipment

A Secret Service Property Number (SSPN) shall be assigned to all ECSAP equipment valued at $300 or more. Information pertaining to accountable property is located in the Administrative Manual, sections AOD-02, Property Charged to Employees, and AOD-03, Property Charged to Offices.

An agent departing the Electronic Crimes Special Agent Program is responsible for contacting the ECS for instructions on how to return or dispose of ECSAP issued property.

Lost or Stolen ECSAP Equipment

The CID – ECSAP Supervisor/ATSAIC shall be notified of incidents pertaining to lost/stolen/damaged ECSAP equipment. Information pertaining to lost/stolen/damaged equipment can be located in the Administrative Manual, section AOD-06, Lost, Stolen and Damaged Property. (See Administrative Manual, section AOD-06(01)) for detailed information regarding lost, stolen, and damaged property.)

Shipping ECSAP Equipment

When shipping ECSAP equipment and media, the shipping office must make certain that all shipments are properly packaged to ensure safe transportation with ordinary care in handling. Shipping costs are the responsibility of the shipping office unless prior approval has been obtained by ECS. Information pertaining to the shipping of items can be located in the Administrative Manual, section AOD-07(02), Official Mail Services and Protective Research Manual, section IRM-03(07).

Turning-In ECSAP Equipment

When ECSAP equipment is being turned-in or returned to the ECS, agents are responsible for ensuring that case information does not remain on their forensic computers, and that their hard drive(s) have been adequately wiped. Agents who have ECSAP equipment that is damaged or inoperable should contact the CID–ECSAP Supervisor/ATSAIC to determine its final disposition (whether the equipment can be excessed or has to be returned to the ECS).

Maintenance of Equipment

It is the responsibility of examiners to maintain their equipment in a serviceable condition and to treat the equipment in manner consistent with the applicable manufacturer's guidelines (ECSAP-06) and the Protective Research Manual, section IRM-03(07).

ASSESSMENT

The Electronic Crimes Special Agent Program (ECSAP) maintains an aggressive quality assurance program through the use of standardized training and peer reviews (see ECSAP-08).

Senior Examiners

If the workload of an examiner's office does not provide the opportunity to conduct **30 examinations** per year, it is incumbent upon the senior examiner to request opportunities to conduct additional exams through the Criminal Investigative Division (CID), ECSAP Supervisor/Assistant to the Special Agent In Charge (ATSAIC).

Journeyman Examiner

If the workload of an examiner's office does not provide the opportunity to conduct **30 examinations** per year, it is incumbent upon the journeyman examiner to request opportunities to conduct additional exams through the Senior Examiner or the ECSAP Supervisor/ATSAIC.

Apprentice Examiners

Competency testing for the Apprentice ECSAP agent is the "Basic Computer Evidence Recovery Training" (BCERT) final examination. Upon completion of the first year after graduating from BCERT, a review of the examiner's progress will be evaluated by the program manager for continuation within the program. Examiners who fail any portion of BCERT may be removed from the ECSAP, Computer Forensics program at the discretion of the ECSAP Supervisor /ATSAIC.

LABORATORY REQUIREMENTS

Physical Environment

Digital examination laboratories located in United States Secret Service (USSS) controlled facilities will provide security in accordance with the local field office. Reference is made to the Administrative Manual; section ADM-08(03), Office Security. In addition, every USSS laboratory **conducting digital examinations is required to have a securable storage area for the temporary storage of evidence** during examinations, as per Investigative Manual, section INV-13, Evidence. A separate locking system shall be used to ensure that only authorized personnel have access to the laboratory.

Equipment

It is the responsibility of each examiner to maintain the equipment in a serviceable condition, and to treat the equipment in the proper manner, according to the following guidelines:

- Maintain inventory and control of equipment and instruments
- Maintain control of materials and supplies
- Perform calibration of equipment and instruments
- Store "clean" hard drives in a secure location
- Obtain the latest software patches/updates
- Obtain the latest virus definition updates

Inventory and Control of Equipment and Instruments

Each laboratory is responsible for maintaining control and inventory of equipment and instruments used for forensic examination. This inventory is maintained in the Sunflower Asset Management System (SAMS) and includes, but is not limited to, forensic computers, hard disk drives, and software. Each item is inventoried and identified by Secret Service Property Number (SSPN), description, and responsible party. If an item is not assigned an SSPN, the item should be inventoried by serial number. "Clean" hard drives shall be stored in a secure location.

When previously used hard drives are to be utilized for the purpose of imaging, the drives must be wiped using issued wiping utilities (NIST Special Publication 800-88 requires one complete over-write using said utility) before the imaging takes place, unless a secure hash function is used (such as the MD5 algorithm) to ensure data validation.

Control of Materials and Supplies

Each laboratory is responsible for maintaining a stockpile of materials and supplies sufficient to support digital evidence recovery operations for approximately two months. Additional materials and supplies are available from the Electronic Crimes Special Agent Program (ECSAP) Section on an "as needed" basis. Regional Task Forces are responsible for maintaining sufficient supplies through allocated funds.

Calibration of Equipment and Instruments

The computer forensic machines maintained in the laboratories will be provided with software and hardware updates from Headquarters as needed. Additionally, forensic examiners are required to update their anti-virus software definitions, and obtain the latest software patches/updates prior to each new examination.

Software

Each examiner is responsible for ensuring his/her forensic software is current. Additionally, examiners must contact the Criminal Investigative Division, Computer Forensics and Research Development Branch, for authorization to purchase needed software and to coordinate its delivery.

Questions regarding the purchase of additional software should be addressed to the ECSAP – Assistant to the Special Agent In Charge.

RIF

EVIDENCE

Processing of Classified Material

Classified materials are processed by U.S. Secret Service (USSS), Electronic Crimes Special Agent Program, Computer Forensics (ECSAP/CF) laboratories throughout the field, on a case-by-case basis. Any requests for service that includes processing of classified material must be brought to the attention of the Headquarters ECSAP/Assistant to the Special Agent In Charge (ATSAIC), prior to the evidence being accepted in the laboratory.

Classified material is processed only within areas approved for the handling of classified material, by ECSAP examiners with the proper clearance.

Cases involving classified material may be handled offsite only at the direction of the submitting agency, and with the approval from the Headquarters ECSAP – ATSAIC.

Custodians of classified information should refer to the procedures listed in the Human Resources and Training Manual, section SCD-03(01), Handling and Safeguarding of National Security and Officially Limited Information.

Handling and Preserving the Integrity of Evidence

Special care must be taken when securing electronic equipment and when handling, transporting, and storing evidence. Information pertaining to the handling of evidence, specifically the chain of custody, and itemized proper documentation, is contained within the Investigative Manual, section INV-13, Evidence.

Proper USSS forms must be utilized in the identification, sealing, and storage of evidence. Specific procedures for the handling of digital evidence are documented in the "USSS Best Practices Guide for Seizing Electronic Evidence (Version 3)," and the "USSS Forward Edge 2" CD-ROM.

Examiners should review documentation provided by the requestor in order to determine the processes necessary to complete the examination, and ascertain the appropriate legal authority to perform the requested examination. Examples of such authorities include: consent to search by owner, search warrant, or other legal authority. When in doubt, contact the USSS Headquarters ECSAP Supervisor/ATSAIC for guidance regarding legal authority.

RIF

ECSAP agents conducting forensic examinations for outside Federal, State, and local law enforcement agencies will use approved USSS evidence intake and chain of custody procedures, regardless of whether a USSS investigative case is expected to be opened. For non-USSS cases, ECSAP agents must open an 866 case and document the evidence in the ECSAP "On-line Reporting System." An 866 case number should be generated upon receipt of the evidence in order for the agent to open the case in the "On-line Reporting System." With this documentation, outside Federal and State/local evidence can be tracked by the field office's name or number within the on-line reporting system. The SSF 1544, Certified Inventory of Evidence, will no longer be needed (Outside Agency Request ONLY). This will simplify the evidence intake procedure, minimizing administrative tasks required by examiners in the field, as well as provide for an evidentiary control backup available in Headquarters for non-USSS cases. Examiners are reminded to include proper SSF 1544 information in the available database field for USSS cases.

Exam Assistance Requests from the Department of Homeland Security, Office of Inspector General

When examiners are requested to assist with any analysis originating from the Department of Homeland Security (DHS), Office of Inspector General (OIG), including imaging previews and/or analysis, the examiner must contact the Headquarters ECSAP Program Manager for approval. The examiner should also notify the requesting DHS/OIG authority that they must make an official request to the USSS Office of Professional Responsibility requesting assistance from the USSS and provide a synopsis of the investigation. The case number will be generated in CID and assigned to the examiner (i.e., 178-866-xxxxx). The examiner will then follow normal procedures regarding the completion of the on-line exam reports and other documentation.

One or more of the following forms must be utilized in the identification, sealing, and storage of evidence received from DHS/OIG:

- The SSF 3160, Evidence Envelope;
- The SSF 3160A, Evidence Label;
- The SSF 1544, Certified Inventory of Evidence;
- The SSF 3051, Certified Inventory of Personal Property; or
- State/local evidence or property forms.

The shipping of electronic evidence will be facilitated through use of the government contract carrier. Every package will be shipped with the appropriate packaging materials, in a manner that will minimize the possibility of damage, and with the appropriate documentation as described in the Investigative Manual, section INV-13.

If it is necessary to return the original media held as evidence, it is mandatory that images of that media be listed on a SSF 1544 and placed in the evidence vault.

Marking of Evidence

In addition to the procedures outlined in the Investigative Manual, section INV-13, USSS forensic examiners are required to mark all evidence included in the forensic examination, including hard drives and removable media, to facilitate positive identification.

Sealing Evidence

Evidence presented to the USSS forensic examiner must be sealed with evidence tape and accompanied by one or more of the following forms:

- The SSF 1544, Certified Inventory of Evidence;
- The SSF 3051, Certified Inventory of Personal Property; or
- State/local Evidence or Property Form.

Furthermore, evidence must also be accompanied by one or more of the following documents:

- The SSF 1922, Consent to Search, or
- A0 93, Written and signed Search Warrant for the item(s) seized.

(b)(7)(E)

R I F

Write Blocking

The acquisition of all digital forensic evidence should be obtained with the assistance of "Write Blockers" and/or in "Read Only" mode so as to not contaminate the evidence during acquisition.

Storage of Evidence

The USSS provides for overnight and short-term storage through the local field office laboratories and specified evidence vaults, as described in the Investigative Manual, section INV-13, Evidence.

Disposition of Evidence

In all Federal cases, authorization shall be obtained from the United States Attorney's Office prior to the destruction of evidence and images.

Securing Computer Systems Containing Evidence

Physical access to evidence is restricted to the main evidence vault which is provided by the field office or the requesting agency; in addition to this, temporary storage is made available within the Computer Forensics laboratory.

All USSS forensic computers are restricted from being connected to the Internet/Intranet. Forensic machines are allowed to be networked via a local area network (LAN) that does not have access to the Internet/Intranet. LANs that use a server are required to have the server password protected, with limited access to its files. Additionally, the server must be housed in a limited access area with the same appropriate physical security measures as the storage of physical evidence. Updates and patches shall be applied via removable media only, and will not be directly downloaded on-line. Software that has been downloaded via a non-forensic machine must be screened for viruses prior to it being loaded on a forensic computer.

R I F

Removal of Evidence/Contraband from Secure Digital Evidence Storage

Upon the exhaustion of appellate review, all evidence maintained via Secure Digital Evidence Storage (SDES) or other Electronic Storage media should be destroyed. Exceptions are cases where the evidence has been identified as being of interest to the Assistant United States Attorney's office beyond the scope of the case adjudicated, or if a USSS supervisor directs the agent to preserve the evidence. When in doubt, contact the Headquarters ECSAP – ATSAIC for further guidance.

Authorization for the destruction will be in standard Official Memorandum format. The destruction of the evidence pertaining to the case will be accomplished by means of an issued wiping software utility that complies with the Department of Defense standard (seven overwrites). Documentation of the evidence destruction will be in writing and maintained in the case file.

DIGITAL EXAMINATION PROCESS

The digital examination process will vary according to the system. A hardware or software write block will be implemented during the acquisition process. All examinations must include a minimum of one (1) verified image.

Quality Assurance

A vital component of the forensic process is quality assurance. The Criminal Investigative Division (CID), Electronic Crimes Special Agent Program (ECSAP) maintains an aggressive quality assurance program through the use of standardized training and peer reviews.

It is mandated that all ECSAP agents complete the requisite certified digital examiner training provided by the United States Secret Service (USSS), or if the applicant has received training and/or experience in computer forensics, a review of the agent's qualifications will be completed to determine if the agent can "test-out" or be admitted into the ECSAP program based on their qualifications. The review of the agent's previous training will be overseen and directed by the ECSAP program manager. Such qualifications to enter the program based on previous experience can include experience as a computer forensic examiner for a State/local police department or within the private sector.

Another qualification that could allow for an agent to enter the program would is a peer review. A peer review consists of a review of a completed computer forensics (CF) exam by a senior CF examiner.

A peer review of every CF exam is conducted at the end of an examination. It is incumbent upon the forensic examiner to ensure a peer review is accomplished. The peer review must be accomplished prior to the final approval process which is conducted by the Electronic Crimes Section (ECS).

Examinations

When conducting an examination, the following guidelines must be applied:

- Perform an electrical safety check prior to any examination of equipment;
- Remove covers of personal computers (PCs) to check for hidden items, disconnected drives, etc;
- Carry out pre-processing checks (system date/time, port settings, BIOS geometry, etc.) and complete the required documentation;
- Secure items produced from the processes and identify with labeling;
- Maintain notes/photos as necessary and complete all required paperwork;

R I F

- Photographs shall be taken of all media being examined. The photographs should include the associated serial numbers of the media when applicable;

- All media being examined shall be initialed and dated by the examiner;; and

- Images of examined media shall be scanned for viruses using the most recent definitions available at the time of the exam. The examiner shall document the date/time of the virus scan, anti-virus software utilized, and the definition release date.

Files relating to each case should be organized under a folder titled with the case name and/or case number. This folder can contain all files/folders relating to the case including: Export/Temp/E01 files/Evidence/ Report/Case File, etc.

State and Local Exams

For exams performed for State/Local agencies, copies of images shall be provided to the appropriate State/local agency for final retention.

Special Exams

If an examiner receives a request to perform a "sensitive" exam, (i.e., for the Office of Professional Responsibility,; the Office of the Inspector General or a "Classified" exam), these exams should be coordinated through the Inspection Division prior to examination. These types of exams shall be completed, or designated by the CID/ECSAP for completion by the applicable field office.

The Inspection Division shall also be notified of any requests to perform exams for any OIG, including the Department of Homeland Security (DHS/OIG)

Macintosh/Linux Exams

Examiners who have not received training on "Macintosh" or "Linux" systems should contact the Macintosh/Linux Coordinator, or the Headquarters CID/ECSAP Manager for assistance.

All Macintosh exams should be completed by ECSAP agents who have received training in performing a Macintosh exam. Macintosh specific hardware and software should be used to perform the exam when applicable.

R I F

Forensic Library

A forensic library is maintained in the Headquarters CID/ECSAP. The forensic examiner should also maintain appropriate references locally.

Information Resources

The USSS provides an informal informational online router (ECSAP router) to assist forensic examiners in keeping abreast of new technologies and trends. The USSS also provides, on a case-by-case basis, additional funding for locally requested courses. In addition, the USSS allocates funds to cover one-half of the annual membership fees for the High Technology Crime Investigation Association (HTCIA) for its forensic examiners. The USSS provides information on future training opportunities, seminars, courses and classes. These resources provide the examiners with a vast quantity of information spanning this field.

From: INV
Sent: Wednesday, June 03, 2015 12:52 PM
To: USA
Cc: INV
Subject: Establishment of New FIRS-ECSAP, and Global Positioning System (GPS) Secondary Case Classification

//ROUTINE//

FROM: Headquarters (AD - Investigations)

TO: All Supervisors and Holders of the Investigative Manual

SUBJECT: Establishment of New FIRS-ECSAP, and Global Positioning System (GPS) Secondary Case Classification Codes

This directive should be reproduced locally and filed in front of the following Secret Service manual sections:

Master File Classification Code (MFCC) Manual:	
(Front)	DCP#: MFCC 2015-03
Investigative Manual:	
ECSAP-09, Case Records and Reports	DCP#: ECSAP 2015-02

This directive is in effect until superseded.

The creation of the following secondary case types will be used in the Field Investigative Reporting System, Electronic Crimes Special Agent Program (FIRS-ECSAP) application for better statistical tracking:

866.940 - Tablets, E-Readers, Hybrids

866.941 - Secret Service Case
866.942 - Federal Government Case
866.943 - State and Local Government Case

866.950 - Electronic Gaming Systems

866.951 - Secret Service Case
866.952 - Federal Government Case
866.953 - State and Local Government Case

866.960 - Wearable Technology

866.961 - Secret Service Case
866.962 - Federal Government Case
866.963 - State and Local Government Case

866.970 - Global Positioning System

866.971 - Secret Service Case
866.972 - Federal Government Case
866.973 - State and Local Government Case

876.150 - NETWORK INTRUSION AND FORENSIC EVALUTION PROGRAM (NIFE)

876.151 - Secret Service Case
876.152 - Federal Government Case
876.153 - State/Local Government Case

As technology changes and new electronic devices emerge, criminals often leverage these new devices to conduct their criminal activity. ECSAP Agents are tasked with conducting forensic examinations pursuant to ongoing criminal investigations.

Questions regarding this policy should be directed to the Criminal Investigative Division Regions Section at 202-406-9330.

Headquarters (AD - Investigations) Jenkins

CASE RECORDS AND REPORTS

Laboratory Management Information System

Support of digital analysis conducted by an Electronic Crimes Special Agent Program (ECSAP) agent is controlled by the Criminal Investigative Division (CID), Electronic Crimes Section (ECS), or by their controlling Electronic Crimes Task Force (ECTF). The ECS is responsible for supporting all digital laboratories throughout the USSS with the exception of the ECTF. The ECTF laboratory managers and supervisors control the operations for their respective laboratories.

The information system used by the digital laboratories consists of the investigative supervisor's case tracking database, MCI database, and the managerial and financial policies as dictated by the local field office supervisor. Refer to the Investigative Manual, section INV-35, Case Management for further information.

Retention of Files

For each exam, an electronic copy of the ECSAP examination report, along with digital evidence photographs, and notable files located during the exam, shall be placed on a CD or DVD and kept with the master case file.

All records of the USSS are Government property and are destroyed in accordance with the procedures of a records disposition program. This program establishes specific retention periods that must be followed in the disposal of each category of record. (See Administrative Manual, section MNO-07, Records Disposition Schedules, for specific details regarding any and all of the most current additions and/or revisions to the following guidelines). Retention periods for case files are listed in the following table:

Type of Case	Field Office Retention	Headquarters Retention
Criminal Judicial	30 years	30 years after close of case
Criminal Non-Judicial (except forgery)	10 years	30 years after close of case
Criminal Non-Judicial (except forgery)	5 years	30 years after close of case
Non-Criminal	5 years	30 years after close of case
PI Judicial and PI Non-Judicial (formerly Class III)	30 days (or 2 years at SAIC's discretion)	20 years after close of case
PI Non-Judicial	30 days (or 2 years at SAIC's discretion)	5 years
Personnel Security	N/A	20 years after date of last action

**Any case containing protected Internal Revenue Service information has a minimum retention period of 8 years.

Case Numbering

For non-USSS cases the original case is opened with an 866.xxx or 876.xxx primary case type (i.e. 866.010, 866.020, 876.112, etc.). Information pertaining to case types can be located in the Master File Classification Code Manual.

The case number format for non-USSS cases should be as follows: CFO-866.XXXXX (note CFO is Controlling Field Office) or CFO-876.XXXXX and the appropriate case type suffix (-S, -ICR, -NC, etc.).

The case title for non-USSS cases should be the name of the requesting agency.

For non-USSS cases that consist of cellular telephones only, PDAs only, skimmers only, or a combination of all three, (but lacking a hard drive, CD, floppy or other media type) the exam report will be opened with an 866.9xx primary case type (i.e., 866.9xl Secret Service Cases, 866.9x2 Federal Government Cases, and 866.9x3 State and local Government Cases). SIM cards will be classified under the Cellular Telephone classification, whether they are recovered in an actual phone or by themselves.

For example, a local police department requests that an examination be performed on a cellular telephone. The examiner would open the case with the primary case type of 866.913. The 866.010 (Liaison State/local Government) would not need to be included, as the 866.913 specifically addresses State and Local government cellular phones. However, if the examination includes a laptop and a cellular phone, the examiner may open an 866.010 as long as the 866.913 is included as a secondary case type. The same will apply for PDAs and Skimmers. The purpose of the new 866.9xx series case types is to track the number of specific devices encountered by examiners, so it is essential these devices be documented via the appropriate case type

Case control credit will be given to the office requesting the ECSAP examination, but exam credit will be given to the ECSAP agent performing the exam.

For existing USSS cases, the ECSAP exam should be entered into the "On-line Reporting System" as an 866 or 876 report under the existing USSS case number and existing case title with an index attached which would be in numerical order for that fiscal year (i.e. first exam for an USSS office in 2009 would be 2009-01 John Doe, second exam 2009-02 John Doe). This index will apply to the case, not to the examiner or to the office. For example, the Kansas City Field Office receives a laptop and a cellular telephone and requests that a Washington Field Office agent perform the cellular telephone exam. The Kansas City report will be 2007 01 case title, and the report opened by Washington under Kansas City's case will be 2007 02 case title.

File Naming

Electronic files associated with exams shall be named by the case number associated with the exam. If there are multiple exams for one case, the case number and number of exam in sequence should be used (e.g., 320-866-12345Exam1.., 320-866-12345Exam2.., etc.).

Exam Credits

An examination is defined as the forensic analysis of any hard drive, cellular telephone, PDA, skimmer or any collective number of removable media (i.e. CDs floppy diskettes, SIM cards, etc.). For example, an examination involving three (3) hard drives, four (4) CDs and twelve floppy diskettes will total five (5) exams in the on-line reporting system. One credit will be given for each hard drive regardless of size and one (1) for each additional type of media. An examination with a PDA, skimmer, cellular telephone with SIM card in the phone, and one (1) additional SIM card, will total four (4) exams in the on-line reporting system; one (1) for the PDA, one (1) for the skimmer, one (1) for the cellular telephone with SIM card and one (1) for the additional SIM card.

Clean Rooms

In order for an office to request data extraction from electronic media via a clean room, and for the office conducting the clean room data extraction to receive credit, the following steps must be taken.

- The office that is requesting a clean room data extraction must have an open case with a case number. That office would send the electronic media to one of the offices with clean room capabilities via an Investigations Other District (IOD) request.
- Once the electronic media is received, the office conducting the clean room data extraction needs to open an 876.1xx on-line report under the office that is requesting the clean room data extraction (similar to any other IOD request). When completed, the clean room office would return the electronic media and any applicable extracted data to the requesting office.
- Once the requesting office receives the electronic media, that office will conduct the forensic exam and receive 866 credit(s). If the clean room office conducting the data extraction was not able to successfully extract the data from or otherwise repair the electronic media, then the requesting office would only claim credit on any other electronic media that was forensically examined by the ECSAP agent.
- If the office requesting the clean room data extraction is the same office as the clean room office, that office needs to complete an 866 report AND an 876 report.
- Each recoverable piece of media which is examined by the requesting office will receive exam credit per the standard protocol mentioned earlier in this section and will be represented within the on-line report.
- For each piece of media which has data extracted by the clean room office, that office/agent will be given one clean room credit and will be represented within the 876 report.
- If the evidence is unrecoverable, then the clean room office conducting the data extraction will report the evidence and exam credit under 876. The office that requested the clean room data extraction will report the evidence request in 876.1xx (any 866 reports that were opened would need to be removed as no analysis took place).

RIF

Preview Exam

Preview is defined as viewing electronic media with a software/hardware tool for evidence in which no forensic image or files have been stored on a secured electronic media for the electronic media in question.

Offices which conduct exams for other agencies and do not have the possibility of becoming an established USSS case will be allowed to receive credit for previews. The previews can be the only method used for locating evidence. An 876.14x report must be established in the on-line reporting system in order to receive exam credit.

When conducting a preview on an established USSS case, if the examiner discovers evidence, a complete forensic exam must be completed. An 866 report must be established in the on-line reporting system for exam credit. If an 876.14x is already established it must be removed from the on-line reporting system prior to opening an 866 control card.

Image Exam

Imaging credit may be received for either USSS cases or other agency cases. An 876.13x report must be established in the on-line reporting system in order to receive exam credit. An 866 report can only be opened if a complete forensic exam is conducted on the imaged electronic media. If an 866 control card is established then the 876.13x must be removed from the on-line reporting system.

On-Line Reporting

In order to receive exam, image, preview, or clean room credit, all work must be documented in the on-line reporting system.

Please follow the below instructions when creating, assigning, completing, and submitting your on-line reports.

RIF

RIF

United States Secret Service
Directives System

Manual : Electronic Crimes Special Agent Program
RO : CID

Section : ECSAP-10
Date : 10/09/2014

Subject: Network Intrusion Responder (NITRO) Program

To: All Supervisors and All Manual Holders of the Electronic Crimes Special Agent Program

Filing Instructions:

- Remove and destroy the Electronic Crimes Special Agent Program Table of Contents (dated 09/10/2010), and replace with the attached revised Table of Contents.

- Remove and destroy section ECSAP-10, Conducting Network Intrusion Investigations (dated 09/10/2010), in its entirety, and replace with the attached revised section.

- File this Policy Memorandum in front of this section.

- This directive is in effect until superseded.

Impact Statement: This directive has been updated to reflect current policy and procedures governing agent roles, responsibilities, qualifications, and investigative procedures applicable to the Network Intrusion Responders (NITRO) Program. This directive also establishes the new SSF 4358, "Electronic Crimes Special Agent Program (ECSAP) Service Agreement," to be completed by agents entering into the NITRO Program. Additional changes to this policy are as follows:

- Section **title** has been changed to "Network Intrusion Responder (NITRO) Program."

- Language has been incorporated advising of the roles and responsibilities of NITRO agents.

- **New SSF 4358**, Electronic Crimes Special Agent Program (ECSAP) Service Agreement, has been established to standardize the commitment procedure for agents entering the NITRO Program.

RIF

- Language has been included regarding the introduction of the Network Intrusion Action Center (NIAC), and the responsibility of NITRO agents to update the NIAC regarding network-based investigative information, and all network-based response scenarios.

- Language has been incorporated describing the appropriate use of Subject Matter Expert (SME) hours.

- Procedures requesting Internet Protocol (IP) Captures from the Technical Security Division has been included.

Forms Instructions: New SSF 4358 may be accessed via the Management and Organization Division's home page under MNO Keywords: Forms.

Mandatory Review: The Responsible Office will review all policy contained in this section in its entirety by or before October 2017.

Questions regarding this policy should be directed to the Office of Investigations, Criminal Investigative Division at 202-406-9330.

Paul S. Morrissey
AD - Investigations

DCP#: ECSAP 2014-02

NETWORK INTRUSION RESPONDER (NITRO) PROGRAM

Authority and Management

Title 18 of United States Code, section 1030 provides the United States Secret Service (USSS) authority to investigate unauthorized access to computer systems, commonly referred to as network intrusions. The USSS Electronic Crimes Special Agent Program (ECSAP) manages the Network Intrusion Responder (NITRO) Program by coordinating initial and ongoing NITRO training, distributing hardware and software resources to NITRO agents, and supporting USSS offices in the field undertaking network-based investigations.

Types of Network Intrusions

- Denial of Service (DoS) – An attack that renders the computer resource unable to communicate on the network.
- Malicious Code – A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.
- Unauthorized Access – A person gains logical or physical access without permission to a network, system, application, data, or other Information Technology (IT) resource.
- Inappropriate Usage – A person violates acceptable use of any network or computer policies.
- Multiple Component – A single incident that encompasses two or more types of intrusions; for example, a malicious code infection leads to unauthorized access to a host, which is then used to gain unauthorized access to additional hosts.

NITRO Agents

Personnel interested in the NITRO Program must complete the Network+ certification course in the Learning Management System (LMS) prior to being considered for basic NITRO training. The Criminal Investigative Division (CID) NITRO Program Manager or his/her representative will send out an Official Message soliciting candidates for Basic NITRO (BNITRO) training. Field offices interested in nominating agents for participation in BNITRO training will email the NITRO Program Manager or the ECSAP Supervisor with the prospective agent's name(s). Field offices should contact the NITRO Program Manager or the ECSAP Supervisor if they feel that they have an exceptional need of additional NITRO agents. The selection for subsequent network-based training will be based upon the NITRO agent's performance within the NITRO Program and adherence to the NITRO reporting guidelines. The Criminal Investigative Division (CID) will also consider candidates by assessing the field office's demand for network intrusion investigations, and the office's historical reporting activity in the Network Intrusion Action Center (NIAC).

All agents must complete the NITRO basic course prior to entering the NITRO Program. During the basic NITRO course, agents will receive a NITRO computer and various software and hardware tools to be used during NITRO investigations. Upon completion of basic NITRO training, all NITRO agents will become a part of the NITRO e-mail group, and will be added to the Network Intrusion Action Center (NIAC). As a member of the NIAC, agents will receive e-mail updates of network intrusion reports submitted by members of the NIAC.

Agents who become a part of NITRO will incur a 36 month commitment to the NITRO Program. Agents must sign the SSF 4358, Electronic Crimes Special Agent Program (ECSAP) Service Agreement, upon entrance to the NITRO Program; a copy of this signed document will be maintained in CID. Additionally, candidates should be aware that NITRO agents may be required to travel out of district for various CID/ECSAP assignments to include investigative assistance, presentations, classroom instruction, and projects associated with research and development. NITRO agents subject to internal field office squad rotations, or temporary protection-related assignments should attempt to maintain their NITRO proficiency for the duration of their 36 month commitment to the NITRO program. Field office SAICs should make every effort to ensure that the 36 month commitment is adhered to.

Equipment

It is the responsibility of each NITRO agent to maintain the issued equipment in a serviceable condition, and to treat the equipment in the proper manner, according to the following guidelines:

- Inventory and Control of Equipment and Instruments;
- Control of Materials and Supplies;
- Calibration of Equipment and Instruments;
- Store "clean" hard drives in a secure location;
- Obtain the latest software patches/updates; and
- Obtain the latest virus definition updates.

Network Intrusion Investigations

NITRO agents conducting complex network intrusion investigations will have access to various Subject Matter Experts (SME) to assist in their investigations. The use of SME assistance must be coordinated through CID/ECSAP, to assure that accounting of billable SME hours is properly recorded. Questions regarding the adequate utilization of this service should be immediately addressed with the NITRO project manager or the ECSAP supervisor.

NITRO agents who have authorization via Court Order to conduct an Internet Protocol (IP) intercept, should contact the Technical Security Division (TSD)/Investigative Support Branch (ISB)/Telephone Intercept Section (TIS), and use the following procedure.

- Contact TSD/ISB/TIS by phone to notify them of your intent to conduct an IP intercept and provide the following information:
    - Case Agent;
    - Who needs access to the collected data;
    - Case Number;
    - Data Source; and
    - Copy of the signed Court Order authorizing the IP intercept.

- Send an Official Message from the SAIC of your office to the SAIC of CID; with "Info: to the AD Investigations, the SAIC of ISD, and the SAIC of TSD, that details your request for an IP intercept.

- Provide a billing contact and address for charges incurred by TSD for providing the IP intercept.

Reporting System

All NITRO-related responses and run-outs should be documented in the Network Intrusion Action Center (NIAC) within 24 to 48 hours. NITRO agents are required to update the NIAC whenever they respond to a network intrusion or receive information related to malicious or unauthorized network activity. Due to the nature of network intrusions, it is paramount to update this system as soon as investigative information is received.

Information regarding discovered malware and indicators of compromise (IOC) should be entered in the NIAC; these entries should not include the actual malware or malicious software. All malware and IOCs should be submitted for analysis to US-CERT. NITRO agents who have obtained either new malware or a variant of known malware should contact the NITRO program manager immediately. The NITRO Program Manager will contact the USSS/CID advisor to the National Cybersecurity Communications and Integration Center (NCCIC), and will coordinate this submission of the malware to the NCCIC.

NITRO-related metrics will be gleaned from the information contained within the NIAC. This information will be used to quantify the various indicators within the NITRO Program, making its accuracy extremely important in determining the utilization and dissemination of investigative resources.

The NIAC is contained within the Field Investigative Reporting System (FIRS); access to FIRS is described in the Investigative Manual, section ECSAP-09, Case Records and Reports.

Case Management/Case Types

Network intrusion-based categorization may be the primary or secondary case type for a network-based investigation. Reference the Master File Classification Code Manual, section CT-700, Investigations – General, for case types used in network-based investigations.

(b)(7)(E)

(b)(7)(E)

Case Opening/Case Closing

NITRO cases should be opened when the following criteria are present: a search warrant or a subpoena has been issued, and/or items with evidentiary value are taken into custody by the Secret Service. Investigative responses that do not generate sufficient investigative leads to open a case, should be entered in the NIAC within 24 to 48 hours, along with investigative responses that lead to cases being opened. A NIAC entry may develop into a network intrusion case subsequent to its initial entry. When this occurs, the initial entry should be updated within the respective "Report-Summary" in the NIAC.

Before a NITRO investigation is closed, contact the Cyber Intelligence Section (CIS) to ensure that media or copies of media that remain from the investigation, is not destroyed. CIS may choose to add this media to their investigative database to enhance their investigative efforts. All NITRO cases that require the handling of digital evidence should be in compliance with Investigative Manual, section ECSAP-07, Evidence.