FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1256875-0

Total Deleted Page(s) = 1
Page 24 ~ b3; b7E;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

(U) Digital Evidence Corporate Policy Directive and Policy Implementation Guide

(U) Federal Bureau of Investigation

(U) Operational Technology Division

(U) 0639DPG

(U) Published Date: January 03, 2014

(U) Review Date: January 03, 2017

(U) Note: This document incorporates the Corporate Policy Directive and the Policy Implementation Guide.

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION
CORPORATE POLICY DIRECTIVE

0639D

1. Policy Directive Title.	(U) Digital Evidence Policy Implementation Guide
2. Publication Date.	2014-01-03
3. Effective Date.	2014-01-03
4. Review Date.	2017-01-03
5. Primary Strategic Objective.	

6. Authorities:

(U) Title 28 Code of Federal Regulations (C.F.R) Section (§) 0.85

7. Purpose:

(U) To promulgate the Digital Evidence Policy Implementation Guide.

8. Policy Statement:

8.1. (U) All Federal Bureau of Investigation (FBI) employees, task force members, contractors, and other persons assigned or detailed to the FBI must comply with the policies and procedures contained in the Digital Evidence Policy Implementation Guide (PG), which are consistent with the laws, rules, and regulations governing FBI investigations, operations, programs, and activities. (See the Digital Evidence Policy Implementation Guide for these policies and procedures.)

8.2. (U) Any revisions, amendments, or updates to this PG must be coordinated through the Corporate Policy Office (CPO), the Operational Technology Division (OTD) policy officer, and other relevant stakeholders (as determined by CPO and OTD). Resulting changes must then be approved by OTD's assistant director and the executive assistant director (EAD), Science and Technology Branch, as appropriate.

9. Scope:

(U) The guidance provided by the Digital Evidence Policy Implementation Guide is intended for all FBI employees, task force members, contractors, and other persons assigned or detailed to the FBI.

10. Proponent:

(U) Operational Technology Division

11. Roles and Responsibilities:

(U) See the Digital Evidence Policy Implementation Guide.

12. Exemptions:

(U) See the Digital Evidence Policy Implementation Guide.

13. Supersession:

(U) See the Appendix C of the Digital Evidence Policy Implementation Guide.

14. References, Key Words, and Links:

(U) 14.1. See the Digital Evidence Policy Implementation Guide.

(U) 14.2. See the FBI Domestic Investigations and Operations Guide (DIOG).

15. Definitions:

(U) See the Appendix E of the Digital Evidence Policy Implementation Guide, "Definitions and Acronyms."

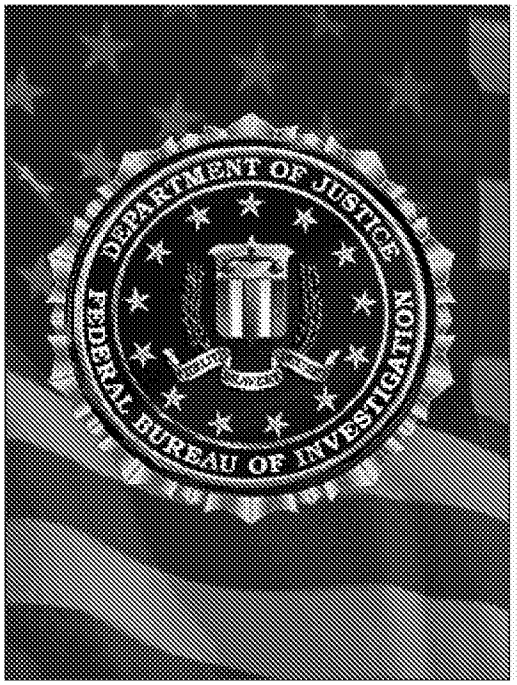
16. Appendices, Attachments, and Forms:

(U) See the Digital Evidence Policy Implementation Guide.

Sponsoring Executive Approval	
Name:	Amy S. Hess
Title:	Assistant Director, Operational Technology Division
Stakeholder Executive Approval	
Name:	Patrick W. Kelley
Title:	The General Counsel (Acting)
Final Approval	
Name:	Steven M. Martinez
Title:	Executive Assistant Director, Science and Technology Branch

UNCLASSIFIED

(U) Digital Evidence Policy Implementation Guide



(U) Federal Bureau of Investigation

(U) Operational Technology Division

(U) 0639PG

(U) January 03, 2014

(U) GENERAL INFORMATION

(U) Questions or comments pertaining to this policy implementation guide can be directed to:

(U) Federal Bureau of Investigation Headquarters (FBIHQ) /Operational Technology Division

(U~~//FOUO)~~ Division Point of Contact: Section Chief, Digital Evidence Section [redacted]

b6
b7C
b7E

(U) SUPERSESSION INFORMATION

(U) Document supersedes (See Appendix C).
(U) Document is a new publication; no previous versions available.

(U) CAVEAT

(U) This policy implementation guide is solely for the purpose of internal Federal Bureau Investigation (FBI) guidance. It is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable by law by any party in any matter, civil or criminal, nor does it place any limitation on otherwise lawful investigative and litigative prerogatives of the Department of Justice (DOJ) and the FBI.

(U) ~~LAW ENFORCEMENT SENSITIVE:~~ The information marked (U~~//LES)~~ in this document is the property of the FBI and is for internal use within the FBI only. Distribution outside the FBI without Operational Technology Division authorization is prohibited. Precautions must be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the ~~LES~~ caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked ~~LES~~ on a Web site on an unclassified network.

(U) Table of Contents

b7E

(U) List of Figures

b7E

(U) List of Appendices

b7E

1. (U) Introduction

1.1. (U) Purpose

(U//~~FOUO~~) This policy implementation guide (PG) establishes and consolidates the policy and procedures for the proper handling, reviewing, and processing of digital evidence (DE) for the Federal Bureau of Investigation (FBI), whether it is seized, received, or otherwise legally obtained. Digital evidence is data that is obtained with the intent to assist in proving or disproving a matter at issue in a case or investigation and is stored or transmitted in binary form. Digital evidence includes binary data stored on magnetic, optical or mechanical storage devices including but not limited to integrated circuits, microcontrollers, chips, tapes, computers, cell phones, compact discs/digital video discs (CDs/DVDs), flash drives, random access memory (RAM), magneto optical cartridges, USB micro storage devices (commonly known as "thumb drives"), digital video recorders (DVRs) or other electronic devices that store or process data digitally. The Operational Technology Division (OTD)/Digital Forensics and Analysis Section (DFAS) is responsible for the FBI's DE Program and establishing DE policy. b7E

(U//~~FOUO~~) Except as noted below, this PG applies to all DE obtained or acquired by the FBI in connection with an investigation.

(U//~~FOUO~~) This PG does not apply to digital evidence obtained through:

- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) Information originally obtained in a non-digital format that was later converted to digital form to facilitate storage, retrieval or search/query.
- (U//~~FOUO~~) Specialized evidentiary information or data collections regulated by another PG (e.g., digital fingerprints, digital DNA profile databases).
- (U//~~FOUO~~) Business, transactional, or other records obtained through a subpoena [redacted] that were provided in digital form.

(U//~~FOUO~~) However, if exempted records are later submitted for a forensic examination, this PG would apply to the examination of said materials.

1.2. (U) Background

(U//~~FOUO~~) As computer technology has advanced over time, digital devices have become universally used to include individuals, groups, or organizations violating federal law [redacted] DE is ever-present in FBI investigations and operations. All personnel that encounter DE must understand how to properly handle, review, and process DE to avoid damaging the integrity of the evidence or violating the Constitutional rights of a person during the course of an investigation. b7E

(U//~~FOUO~~) The FBI requires that DE be seized, searched, stored, copied, processed, reviewed, examined, analyzed, presented, and disposed of in a scientifically proven and legally defensible manner to maximize its integrity, authenticity, probative value, and

evidentiary reliability, and to facilitate the DE's admissibility at trial or other adjudicative proceeding. DE is malleable and can be easily altered or destroyed (e.g., by viewing or copying files without following the proper procedures or by variance in temperature or exposure to heat or magnetic fields). Utilizing properly trained personnel, established procedures, approved tools, and an appropriate quality assurance (QA) program maximizes the reliability and integrity of DE for the purpose of authentication and presentation in court, as well as for investigative [redacted] b7E

1.3. (U) Scope

(U//~~FOUO~~) This PG applies to all personnel working for or with the FBI, including FBI employees, contractors, detailees and task force personnel assigned to FBI field offices, FBI headquarters (FBIHQ) divisions, legal attaché (Legat) offices, regional computer forensics laboratories (RCFLs), and joint task forces (JTFs) who encounter, handle, review, or process DE.

(U//~~FOUO//LES~~) This PG addresses the handling, processing, and content review of DE. Handling includes procedures related to on-scene search and seizure, transportation and storage, evidence intake, and shipping. Processing of DE includes detailed procedures related to on-scene preview, imaging, memory capture, content review, search, extraction, report preparation, and advanced technical analysis [redacted] b7E

[redacted] Content review is the viewing of the [redacted] digital evidence container(s) in accordance with the scope of legal authority.

1.4. (U) [redacted]

(U//~~FOUO~~) Unless expressly stated otherwise, this PG applies equally to criminal [redacted] FBI personnel should coordinate questions concerning legal authority required [redacted] with their chief division counsel (CDC) or assistant division counsel (ADC) or with the Office of the General Counsel, [redacted]

1.4.1. (U) [redacted]

(U//~~FOUO~~) [redacted] b3 b7E

(U//~~FOUO~~) [redacted]

(U//~~FOUO~~ b3 b7E

1.4.2. (U) Reviews or Examinations of DE

(U~~//FOUO~~) This section discusses some of the unique areas of concern raised when the FBI

1.4.2.1. (U) b3 b7E

(U~~//FOUO~~)

(U~~//FOUO~~) However, investigative personnel may review or analyze evidence seized under the authority of a criminal warrant or consent when the evidence at issue has been determined to be within the scope of the criminal warrant or consent pursuant to which it was seized. FBI personnel should not expand the search beyond the consent or criminal warrant's scope. FBI personnel should coordinate questions concerning their authority under this scenario with their servicing CDC/ADC and OGC

(U~~//FOUO~~) In the event that the FBI need to conduct a search of criminally seized DE beyond the scope of the criminal warrant or consent, they should coordinate with their CDC/ADC and OGC to obtain additional legal authority,

1.4.2.1.1. (U) Use of Analytical Tools or Database Systems to Review or Examine DE

(U//~~FOUO~~) b3 b7E

The evidence must be tagged in some manner to permit its withdrawal from the holdings

(U//~~FOUO~~) Before uploading DE seized [redacted] b3 b7E

[redacted]

1.4.2.2. (U[redacted]

(U//~~FOUO~~) Often during reviews or examinations of DE [redacted] (when providing technical assistance to the FBI) [redacted] may be employed in accordance with the provisions of this PG. DOJ policy requires the approval of the deputy attorney general [redacted] in the furtherance of a criminal case. For more information please see [redacted]

1.4.2.2.1. (U//~~LES~~) [redacted] b3 b7E

(U//~~LES~~) During the course of [redacted]

(U//~~LES~~) [redacted]

(U//~~FOUO~~) When this circumstance applies, the case agent is responsible for notifying and coordinating with his CDC/ADC and OGC [redacted] To ensure appropriate disclosures are made, case agents must coordinate with the AUSA or DOJ Trial Attorney.

2. (U) Roles and Responsibilities

2.1. (U) Digital Evidence Roles

(U//~~FOUO)~~ The FBI's DE Program divides DE work functions into general categories or levels based upon the type and complexity of work performed at each level, and the training and experience required of FBI personnel to competently perform the duties at each level. Each category of work depicted in Figure 1, below, has its own set of training and procedural requirements. The first tiered category requires less training and fewer procedures, while the upper two categories require more training and expertise as well as more involved procedures.

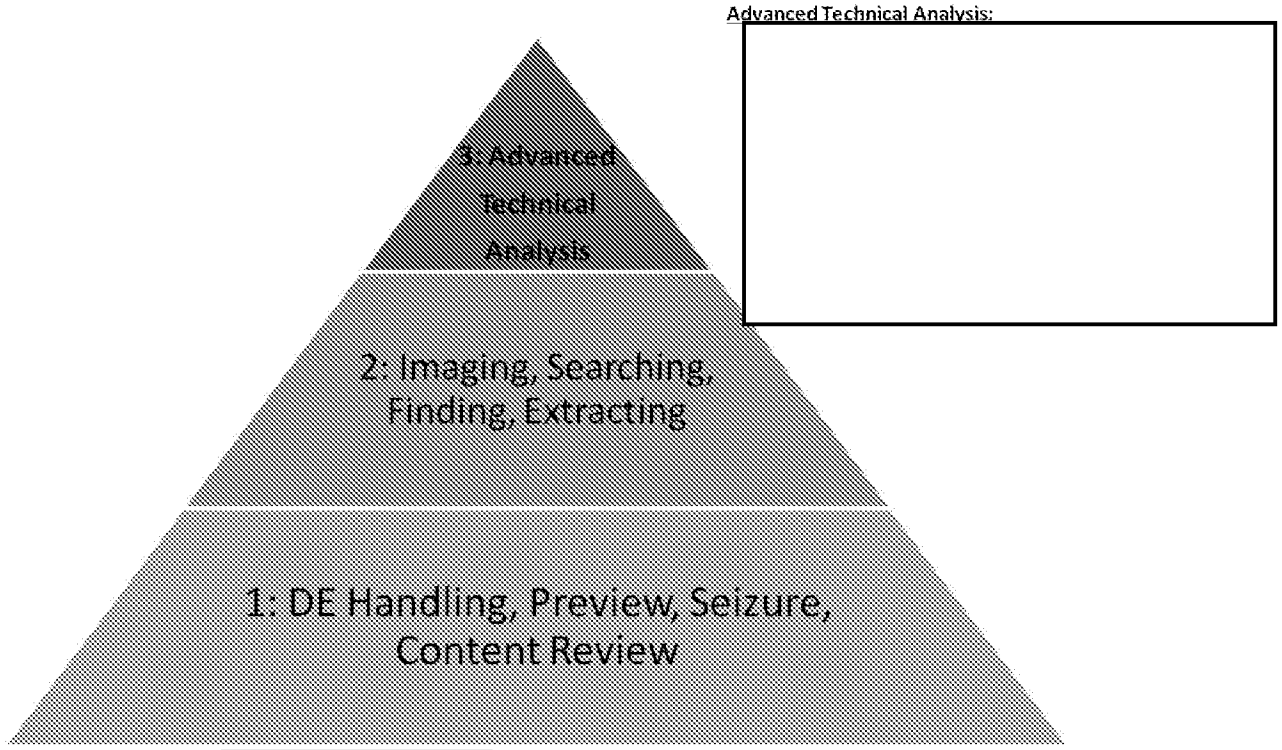


Figure 1: (U//~~FOUO~~)

(U//~~FOUO)~~ The first tiered category on the pyramid represents the broad population of FBI personnel who, with minimal training, are authorized to handle, preview, seize, and/or review DE content. The second tiered category represents a smaller population of FBI personnel who have been trained to the technician level, which allows them to image, search, find, and extract DE. The FBI considers the search and find function an investigative, as opposed to forensic, process, but the imaging and extraction remain forensic processes that require training to forensic standards. The third tiered category represents the smallest population of FBI personnel who have received extensive training and possess the requisite experience necessary to complete the most technically complex DE examinations and analysis.

(U//~~FOUO)~~ As used throughout this PG, references to training and certification refer to training and certification provided, approved, or recognized by the OTD, Digital Forensics and Analysis Section (DFAS). Similarly, unless expressly stated to the

contrary, personnel authorized in any tier must comply with the OTD/DFAS approved training, follow OTD/DFAS approved policies, procedures, and protocols, and only use tools and/or devices in accordance with this PG and OTD/DFAS policies.

(U//~~FOUO~~) Level 1: The handling of DE for seizure or evidence control purposes, and/or the preview or review of DE content for investigative [redacted] can be performed by personnel such as evidence control technicians (ECTs), special agents (SAs) and analysts with proper training and approved tools under procedures approved by OTD/DFAS. b7E

(U//~~FOUO~~) Level 2: DE technician level work can be performed by the following personnel (who can also perform Level 1 work) under procedures approved by OTD/DFAS:

- (U//~~FOUO~~) Computer Analysis and Response Team (CART) technician (CART tech): Personnel trained and certified to forensically copy or image DE.
- (U//~~FOUO~~) Digital extraction technician (DExT): Personnel trained and certified to copy or image DE and perform simple search/find/extract processes on copies of DE.
- (U//~~FOUO~~) Field Audio Video Program (FAVP) forensic analysts (FAs): Personnel trained and certified to perform basic forensic functions related to audio and video DE.

(U//~~FOUO~~) Level 3: Advanced technical analysis is conducted by the following personnel (who can also perform Level 2 and Level 1 work):

- (U//~~FOUO~~) CART forensic examiner (CART FE): Headquarters or field personnel, typically assigned full time to DE work, who are trained, equipped, and certified to copy or image DE, search/find DE, extract data from DE, and provide opinions related to DE, computer forensics, computer or electronic device operations, and other related fields, as their expertise and training permit.
- (U//~~FOUO~~) CART trainees: Prior to achieving CART FE certification, personnel seeking experience and proficiency in the CART Program are considered trainees. While in trainee status, these personnel are authorized to perform forensic tasks under the supervision of a certified CART FE:
    - (U//~~FOUO~~) CART on-the-job trainee (OJT): Personnel identified by field office management to participate in training with a commitment toward becoming certified CART FEs.
    - (U//~~FOUO~~) CART forensic examiner trainee (FET): Personnel assigned to work 100% of their time toward CART FE certification. Typically, these are trainees hired into information technology specialist – forensic examiner (ITS-FE) positions. These may also be CART OJTs who are near the end of their training and have committed 100% of their time to CART FE work.
- (U//~~FOUO~~) Regional Computer Forensics Laboratory (RCFL) associate examiner: Former certified CART FEs from an agency participating in the RCFL

program who have completed their commitment to the RCFL and returned to their home agency, and who continue a relationship with the RCFL to maintain certification and training. When serving in this role, RCFL associate examiners must continue to be impartial forensic scientists, and are prohibited from conducting investigative activities. b7E

- (U//~~FOUO~~) Computer scientist-field operations (CS-FO): The CS-FOs are experienced computer scientists who work as integral members of an investigative team supporting FBI investigations and operations. The CS-FO is responsible for providing advanced technical analysis [redacted] The CS-FO is not authorized to engage in [redacted] Additionally, because CS-FOs are part of the investigative team, they are prohibited from performing forensic examinations of DE.
- (U//~~FOUO~~) OTD/DFAS engineer/analyst/forensic examiner: DFAS [redacted] b7E

(U) Table 1 depicts the various DE personnel roles and the functions that they are authorized to perform with the proper training and certification.

Functions	Investigative Personnel	CART Tech	DExT	Field CART FEs, CS-FOs, DFAS
(U) DE Handling Preview Seizure Content Review	✓	✓	✓	✓
(U) Imaging		✓	✓	✓

(U) Search/ Find/ Extract			✓	✓
(U) Advanced Technical Analysis (U) Role-specific SOPs				✓

Table 1: (U) Roles and Responsibilities

2.2. (U) Digital Evidence Responsibilities

2.2.1. (U) All FBI Personnel Who Handle, Content Review, or Process DE

(U//~~FOUO~~) All FBI personnel who handle, content review, or process DE, in addition to the specific responsibilities delineated below due to their position, are responsible for:

- (U//F~~OUO~~) Understanding and complying with the legal authority as it relates to the DE processed, handled, or content reviewed.
- (U//~~FOUO~~) Handling, content reviewing, and processing DE and documenting those actions in accordance with this PG, other applicable OTD/DFAS policies and procedures, and applicable QA standards.
- (U//FOUO) Ensuring all DE is handled, content reviewed and marked in accordance with [redacted] b3 b7E
- (U//~~FOUO~~) Ensuring that all DE is handled, stored, content reviewed and marked in accordance with FBI dissemination marking policy (e.g., grand jury [GJ] material and tax information) and OTD/DFAS policy (e.g., child pornography materia[redacted]
- (U//FOUO) Maintaining the chain of custody of all DE.
- (U//~~FOUO~~) Disseminating DE only in accordance with this PG.
- (U//~~FOUO~~) Providing testimony, as required, in any legal proceedings in accordance with this PG.

2.2.2. (U//FOUO) Investigative Personnel and Analysts

(U//~~FOUO~~) Investigative personnel handling, processing, and performing content review of DE (typically special agents and analysts) are responsible for:

- (U//~~FOUO~~) Conducting and/or directing the preview and/or review of DE content.

- (U//~~FOUO~~) Using approved DE tools for which approved training has been completed.

2.2.2.1. (U//~~FOUO~~) CART Techs

(U//~~FOUO~~) CART techs are responsible for imaging DE using only approved tools and techniques.

2.2.2.2. (U//~~FOUO~~) DExTs

(U//~~FOUO~~) DExTs are responsible for:

- (U//~~FOUO~~) Processing images of DE to search, find, and extract items of interest from the DE within the defined scope of legal authority.
- (U//~~FOUO~~) If certified, and upon request, performing the DE functions authorized for CART techs as described above. When performing these functions, the DExT must follow the protocols and limitations prescribed for that role.

2.2.2.3. (U//~~FOUO~~) CART FEs

(U//~~FOUO~~) CART FEs are responsible for:

- (U//~~FOUO~~) Upon request, performing any DE functions authorized for a CART tech or DExT. When performing those functions, the CART FE must follow the protocols and limitations prescribed for those roles.
- (U//~~FOUO~~) Conducting and/or directing the forensic examination of DE including:
  - (U//~~FOUO~~)
  - (U//~~FOUO~~)
  - (U//~~FOUO~~)

b7E

- (U//~~FOUO~~)
- (U//~~FOUO~~) in accordance with all provisions of this PG and relevant OTD/DFAS quality assurance (QA) requirements.
- (U//~~FOUO~~) Providing execution of search warrants and preview/examinations of complex computer systems or situations.
- (U//~~FOUO~~) Providing on-scene consultation with investigators and prosecutors in the development of strategies for the seizure or on-scene imaging of digital media and equipment.

2.2.2.3.1. (U//~~FOUO~~) Field Audio Video Program (FAVP) Forensic Analysts (FA)

(U//~~FOUO~~) FAVP FAs are responsible for:

- (U//~~FOUO~~) Conducting and/or directing the content review of audio and video DE.
- (U//~~FOUO~~)
- (U//~~FOUO~~)
- (U//~~FOUO~~)

2.2.2.4. (U//~~FOUO~~) Computer Scientists-Field Operations (CS-FOs)

(U) CS-FOs are responsible for:

- (U//~~FOUO~~) Performing any function carried out by a CART tech or DExT related to DE. When performing those functions, the CS-FO must follow the protocols and limitations prescribed for those roles.
- (U//~~FOUO~~) Supporting investigative personnel with computer science expertise in support of cases or investigations (e.g., assistance with interviews and searches), as authorized by this PG. b7E
- (U//~~FOUO~~) Using for all activities.

2.2.2.5. (U) RCFL Personnel

(U//~~FOUO~~) RCFL personnel are responsible for performing duties as outlined in the MOU between their agency and the FBI.

2.2.3. (U) FBI Headquarters (FBIHQ)

2.2.3.1. (U) FBIHQ Operational Divisions

(U//~~FOUO~~) The executive management of FBIHQ operational divisions is responsible for:

- (U//~~FOUO~~) Communicating the DE policies, procedures, and guidance set forth in this PG to personnel within their mission area by posting a link to this PG on their respective division websites.
- (U//~~FOUO~~) Ensuring compliance with all matters identified in this PG.
- (U//~~FOUO~~) Monitoring compliance and reporting non-compliance in their respective mission areas in accordance with DIOG guidance on compliance and non-compliance.

2.2.3.1.1. (U) FBIHQ Operational Divisions Routinely Handling DE

2.2.3.1.1.1. (U//~~FOUO~~) b7E

(U//~~FOUO~~) DExT personnel who are responsible for:

- (U//~~FOUO~~) Serving as

- (U//~~FOUO~~) b3 b7E

- (U//~~FOUO~~) Following FBI DE protocols applicable to DExTs, as specified in this PG.
- (U//~~FOUO~~)
- (U//~~FOUO~~) At the request of the case agent or headquarters program management unit and with the approval of OGC
- (U//~~FOUO~~) At the request of the case agent or headquarters program management unit and with the approval of
- (U//~~FOUO~~)

2.2.3.1.1.2. (U//~~FOUO~~) CID/Violent Crimes Against Children (VCAC) Section

(U//~~FOUO~~) Criminal Investigative Division/Violent Crimes Against Children (VCAC) Section provides b7E abuse and exploitation to children which may be investigated under the jurisdiction and authority of the FBI. The OTD/DFAS/Digital Analysis and Research Center (DARC)

(U//~~FOUO~~) VCAC manages several programs including the Innocent Images National Initiative (IINI).

(U//~~FOUO~~) VCAC is responsible for establishing guidance for the handling of child pornography contraband for the IINI program.

2.2.3.1.1.3. (U//~~FOUO~~) OTD/Digital Forensics and Analysis Section b7E

(U//~~FOUO~~) The Operational Technology Division (OTD)/Digital Forensics and Analysis Section (DFAS), in coordination with other FBI divisions, is responsible for:

- (U//~~FOUO~~) Creating and maintaining policy and procedures for the FBI's DE Program, wherein such policy and procedures ensure compliance with governing legal authorities, with regard to the manner in which DE is searched, processed, stored, accessed, used, and disseminated, to maintain the integrity of the evidence and to ensure adherence to applicable privacy and civil liberties laws, policies, and regulations.

- (U//~~FOUO~~) Overseeing the FBI DE field subprograms, which include:
  - (U//~~FOUO~~) Computer Analysis Response Team (CART) Forensic Examiner (FE) subprogram.
  - (U//~~FOUO~~) Digital Extraction Technician (DExT) subprogram.
  - (U//~~FOUO~~) Computer Scientist - Field Operations (CS-FO) subprogram.
  - (U//~~FOUO~~) Field Audio Video Program (FAVP) subprogram.
  - (U//~~FOUO~~) FBI Digital Evidence Laboratory (DEL) and Quality Assurance Program for DE.
  - (U//~~FOUO~~) Regional Computer Forensics Laboratory (RCFL) subprogram.
- (U//~~FOUO~~) Providing the following capabilities and resources:
  - (U//~~FOUO~~) Trained examiners who provide DE acquisition, preservation, processing, review, examination, presentation, and testimony.
  - (U//~~FOUO~~) Trained personnel to provide advanced analysis capabilities for DE including:
    - (U//~~FOUO~~)
    - (U//~~FOUO~~)
    - (U//~~FOUO~~)
    - (U//~~FOUO~~)
    - (U//~~FOUO~~)
    - (U//~~FOUO~~)

    b7E
  - (U//~~FOUO~~) Training, certification, and proficiency testing for personnel who process DE.
  - (U//~~FOUO~~)

    b7E
  - (U//~~FOUO~~)
  - (U//~~FOUO~~)
  - (U//~~FOUO~~)

2.2.4. (U) FBI Field Offices

2.2.4.1. (U) FBI Field Office Management

(U//~~FOUO~~) FBI field office management (i.e., Assistant Director in Charge (ADIC), Special Agent in Charge (SAC), Assistant Special Agent in Charge (ASAC), and Supervisory Special Agent (SSA)) is responsible for:

- (U//~~FOUO~~) Promoting and communicating DE policy.
- (U//~~FOUO~~) Ensuring compliance with this PG.

- (U//~~FOUO~~) Monitoring compliance and reporting non-compliance in their respective mission area in accordance with the DIOG.

2.2.4.2. (U//~~FOUO~~) Evidence Control Technicians

(U//~~FOUO~~) With regard to DE, evidence control technicians (ECTs) are responsible for:

- (U//~~FOUO~~) Properly storing, protecting, and tracking DE, as described below in section 3.
- (U//~~FOUO~~) Properly packaging and shipping DE, as necessary, as described below in Section 3.1.

3. (U) Policies and Procedures

3.1. (U//~~FOUO~~) Forensic Program Compliance within the FBI

(U//~~FOUO~~) All DE forensic programs conducted in FBI space must fully comply with FBI forensic policies, procedures and requirements as set by OTD/DFAS, and must be under the direct and immediate control and supervision of the OTD/DFAS unless prior written concurrence of the AD, OTD or his/her designee is obtained.

3.2. (U) Digital Evidence Handling

b7E

(U//~~FOUO~~) This section sets forth policy related to the handling of DE for all personnel working for or with the FBI, including investigative and technical personnel, ECTs, CART techs, DExTs, CART FEs, CSs, DFAS technical experts, FAVP FAs, RCFL personnel, and other personnel who encounter DE.

3.2.1. (U) Personnel Authorized to Handle DE

(U//~~FOUO~~) FBI personnel must handle DE for seizure, transportation, and storage, as with any evidence, pursuant to requirements specified in the [redacted] FBI personnel must also be trained and/or certified in accordance with OTD/DFAS policy and procedures and follow all applicable protocols before processing DE, including making copies or images of DE.

3.2.2. (U) Pre-Search Considerations

3.2.2.1. (U//~~FOUO~~) Legal Review

(U//~~FOUO~~) FBIHQ and field office personnel must ensure that the seizure and examination of DE strictly adheres to the procedures listed in this PG. Personnel handling DE may request chief division counsel (CDC) or Office of the General Counsel (OGC) legal review of DE-related search warrants and subpoenas as applicable [redacted] Field office CDCs or OGC are also available to provide assistance in drafting search warrants or subpoenas for seizing or searching DE.

b3
b7E

3.2.2.2. (U) Timeframe for Warrants Involving DE

(U//~~FOUO~~) Although Rule 41(e)(2)(A) does not place a specific time limit on off-site copying or review of electronic storage media, some judicial districts place specific limits on the amount of time permitted for off-site review. The case agent should consult with the CDC or OGC [redacted] if there are questions pertaining to time permitted for examination.

b7E

3.2.2.3. (U) Consent Searches for DE

(U//~~FOUO~~) Whenever possible, written consent must be obtained from the consenting party and documented on a form FD-26, *Consent to Search* or FD-941, *Consent to Search Computers*. However, this does not mean that oral consent is not valid. The case agent must, when relying on oral consent, appropriately document the oral consent on an FD-302.

(U//~~FOUO~~) In consent cases, case agents should ensure that [redacted] b7E

[redacted]

(U//~~FOUO~~) If consent is terminated, the case agent must immediately contact personnel processing the DE and notify them of the revocation of consent. Once consent is withdrawn, any imaging not completed must be terminated. The case agent should also promptly contact the CDC or OGC for advice on how to proceed with searching any completed or partial images made prior to revocation.

3.2.2.4. (U) Requesting Local Field Office Assistance

(U//~~FOUO~~) DExT personnel may provide on-scene support for routine DE handling and processing in accordance with the procedures outlined in this PG. DExT support should be requested by coordinating with the appropriate squad supervisor(s).

(U//~~FOUO~~) FBI case agents who require search and seizure assistance and/or examination of DE must contact their field office CART supervisor, CART coordinator, or other CART personnel.

(U//~~FOUO~~) Case agents must submit service requests for DE assistance within field offices via electronic communication (EC) to CART personnel. All service requests must include:

- (U//~~FOUO~~) Case ID – the universal case file number (UCFN)
- (U//~~FOUO~~) Case title
- (U//~~FOUO~~) Specific request
- (U//~~FOUO~~) Description of legal authority
- (U//~~FOUO~~) "CART Operations" in the synopsis field of ECs

3.2.2.5. (U) Requests Involving Multiple Locations

(U//~~FOUO~~) Case agents must coordinate in advance any DE service requests involving multiple field offices with the CART supervisor or coordinator in their division as well as with the other applicable divisions. If further assistance is required, the CART supervisor or coordinator should coordinate with the OTD/DFAS/Forensic Operations Unit (FOU). b7E

3.2.2.5.1. (U) Providing [redacted] Technical Assistance in DE Cases

(U//~~FOUO~~) The FBI provides DE forensic services through [redacted]

[redacted]

(U//~~FOUO~~) Pursuant to 28 CFR § 0.85(g) and the DIOG, the FBI Digital Evidence Laboratory (DEL) and RCFLs are authorized to provide, without cost, technical and scientific assistance, including expert testimony in federal or local courts, to all duly constituted law enforcement agencies, other organizational units of the Department of Justice, and other federal agencies. Under this authority, the FBI DEL and RCFLs may

also provide technical and scientific assistance, including expert testimony [redacted] b7E

[redacted]

(U//~~FOUO~~) The FBI DEL consists of the following units, all of which are components of the OTD/DFAS: Forensic Operations Unit (FOU), Forensic Analysis Unit (FAU), Forensic Support Unit (FSU), the RCFL National Program Office (RCFL NPO) and the Forensic Audio, Video and Image Analysis Unit (FAVIAU). The DFAS forensic examiners (see Section 2.1, Digital Evidence Roles) that comprise the DEL consist of CART-FEs, CART-FETs and FAVIAU examiners.

(U//~~FOUO~~) The following OTD/DFAS units are not components of the FBI DEL: the [redacted] Field office CART assets and laboratories are not part of the FBI DEL. Although the RCFLS follow the FBI DEL's quality program, each RCFL is an individually accredited lab independent from each other and the FBI DEL.

(U//~~FOUO~~) In accordance with the DIOG, the provision of routine forensic analysis and examination of submitted evidence is considered technical and scientific support. Routine forensic analysis and examination of evidence performed by the FBI DEL, RCFLs, or CART personnel in field offices is not considered expert investigative assistance (as defined in the DIOG), even if those components are providing expert witness testimony in connection with the support.

3.2.2.5.2. (U) Expert Investigative Assistance in DE Cases

(U//~~FOUO~~) FBI personnel, particularly approving officials, must be careful to review requests for assistance with DE [redacted] see the DIOG.

(U//~~FOUO~~) During the course of providing either [redacted] b3 b7E

3.2.2.5.3. (U) Requests for [redacted] the DEL or RCFLs

(U//~~FOUO~~) FBI components that are not part of the FBI DEL or RCFLs, may only provide technical assistance pursuant to Attorney General Order 2954-2008 and the DIOG.

(U//~~FOUO~~) Requests fo [redacted] than the FBI DEL or RCFLs must be processed and handled in accordance with the DIOG [redacted] as applicable.

(U//~~FOUO~~) Requests for RCFL DE support from [redacted] will be handled in accordance with the applicable MOU governing the RCFL concerned, provided the MOU is not inconsistent with this PG. b7E

(U//~~FOUO~~) Because the authority to provide this support is under 28 CFR § 0.85(g), a federal nexus is not required, and such services must be provided at no cost to the requesting agency. RCFLs may not provide [redacted] All such requests must be referred to the FBI DEL.

(U//~~FOUO~~) [redacted] b3 b7E

(U//~~FOUO~~) The processing of the DE and dissemination of materials and information pertaining to the technical assistance by the RCFLs must be in accordance with this PG.

(U//~~FOUO~~) RCFLs will track all service requests, and disseminate information to [redacted]

3.2.2.5.5. (U//~~FOUO~~) Requests for the Use of [redacted]

(U//~~FOUO~~) Requests for the use of FBI or other [redacted] in criminal cases require the review and recommendation of OGC [redacted] and the DOJ's Criminal Division, as well as approval by the Deputy Attorney General. See Deputy Attorney General Memorandum [redacted]

(U//~~FOUO~~) Requests for the use of [redacted] b7E

(U//~~FOUO~~) The dissemination of [redacted]

(U//~~FOUO~~) Prior to approval of a request, assurances must be obtained from the requesting agency, as well as the chief prosecutor for the applicable jurisdiction, that representatives of the requesting agency will not disclose [redacted] in court, through pre-trial motions, discovery, or other means, or through any federal or state freedom of information legislation or similar law, or otherwise disclose to the media or public, without the prior written consent of the Director, FBI, or his designee. The requesting agency and the chief prosecutorial official will also acknowledge they are receiving the requested technical assistance expressly conditioned on the fact that they are subject to the nondisclosure provisions governing FBI information as set forth in 28 CFR § 16.22, 16.24, and 16.26, as well FBI policy on the protection, use, and

b7E

[redacted]

3.2.2.6. (U) DE and Evidence Control Facilities (ECFs)

(U//~~FOUO~~) The original DE seized at a search site must be securely transported to the FBI field office or RCFL site and, after processing and examination, placed, as appropriate, in an FBI or RCFL evidence control facility (ECF). [redacted] provides additional guidance and requirements.

3.2.2.7. (U) DE Storage

(U//~~FOUO~~) DE must be stored and secured and/or sealed to prevent data or evidentiary loss, cross-transfer contamination, or other deleterious change (e.g., DE must be sealed and protected from heat and light for preservation).

3.2.2.8. (U) Shipping DE

(U//~~FOUO~~) Shipping of DE from field offices to FBIHQ or RCFLs must be handled through an FBI ECF.

3.2.2.9. (U) Shipping DE to CART

b7E

(U//~~FOUO~~) When it has been determined that DE needs to be shipped either to another field office CART FE or to the OTD/DFAS, the DE must be processed through the field office's ECT. The ECT must ensure that the DE is packaged securely and that proper chain-of-custody procedures are followed. For assistance in packing DE for shipping, the case agent should contact the ECT in his or her field office.

(U//~~FOUO~~) The DE must be accompanied by an EC requesting examination as described in th[redacted]

3.2.2.10. (U) Transferring a Working Copy of FBI DE [redacted]

b7E

(U//~~FOUO~~) Case agents may submit working copies [redacted] Submission may be accomplished by completing a transmission request EC in the FBI's Central Recordkeeping System, and providing a working copy of the DE [redacted]

3.3. (U) Digital Evidence Processing

b7E

3.3.1. (U) Imaging

(U//~~FOUO~~) Imaging is the act of making [redacted] copy of the original DE to serve as an accurate reproduction of the original DE. Imaging must only be performed by certified DE personnel. Certified DE personnel (i.e., CART FEs, CART techs, DExTs, and FAVP FAs) must follow standard CART procedures and QA requirements when imaging DE.

Specific procedures for imaging digital media are detailed in the

3.3.2. (U)

(U//~~FOUO~~)

b7E

3.3.3. (U)

(U//~~FOUO~~)

b7E

3.3.3.1. (U)

(U//~~FOUO~~)

b7E

3.3.4. (U) Content Review

(U//~~FOUO~~) Investigative personnel can review DE for content

3.3.4.1. (U) Scope and the Content Review

(U//~~FOUO~~) When searching DE pursuant to legal authority, an agent is authorized to seize only items specified in and responsive to the authority, absent an independent legal basis under which materials can be seized or retained.[1]

[1] (U//~~FOUO~~)

b7E

(U//~~FOUO~~) When searching DE pursuant to a criminal warrant, the warrant permits only a search for evidence of a specific, enumerated crime or crimes. Therefore, agents may only seize items that are within the bounds of the warrant, commonly known as the "scope" of the warrant.

(U//~~FOUO~~) When searching DE [redacted] b7E

government must not exceed the scope authorized in the order. Questions regarding the authorized scope of a search should be directed to the servicing legal counsel (CDC/ADC or OGC).

3.3.4.2. (U//~~FOUO~~) Scope Issues in Consent Cases

(U//~~FOUO~~) Where consent is the legal authority for a search of DE, the ability of FBI personnel to review the digital evidence is bound by the terms of the consent provided. Consenting individuals may impose binding limitations on the areas or items that may be searched (e.g., specific rooms of a house, specific files or folders on a computer), either orally or on the written consent form.

3.3.4.3. (U//~~FOUO~~) Search Protocols for DE

(U//~~FOUO~~) All FBI personnel should observe all restrictions written into warrants, including local protocols attached to any warrants, when examining or reviewing DE. Questions regarding such provisions should be directed to the servicing legal counsel (CDC/ADC or OGC).

3.3.4.4. (U) Self-service Kiosks

(U//~~FOUO~~) Self-service kiosks are provided in most field offices. In addition, portable kiosk kits are available in many FBI resident agencies (RAs). When reasonably available, investigative personnel must use the kiosks to automatically process supported DE types.

(U//~~FOUO~~) [redacted] self-paced or hands on training is required. b7E

(U//~~FOUO~~) [redacted] self-paced or hands on training is required.

3.3.4.5. (U) When Content Review Is Authorized

(U//~~FOUO~~) Content review is authorized only after DE is processed by authorized personnel (i.e., CART FEs, CART techs, DExTs, FAVP FAs), with the following exceptions:

- (U//~~FOUO~~) [redacted] approved by OTD/DFAS are utilized.

- (U//~~FOUO~~) Preview [redacted] OTD/DFAS policy. b7E
- (U//~~FOUO~~) Preview by RCFLs or CART field office facilities in accordance with OTD/DFAS policy.
- (U//~~FOUO~~) The use of self-service kiosks for [redacted]

(U//~~FOUO~~) Content review of original DE is prohibited by those not trained and authorized by OTD.

3.3.4.6. (U//~~FOUO~~ [redacted]

(U//~~FOUO~~ [redacted] within the scope of the legal authority. The information obtained through [redacted]

3.3.4.7. (U [redacted]

(U//~~FOUO~~) [redacted] b7E

3.3.4.8. (U) Content Review Tools

(U//~~FOUO~~) All DE content review tools used by personnel working for or with the FBI or RCFL in their investigations must be legally obtained and used in accordance with the limitations in the licensing agreement, unless a legal exception applies (e.g., fair use or specific guidance in the legal authority) and the reviewer has coordinated with his or her CDC or OGC. If proprietary software is seized with the data, it may be used to view the data from the investigation.

3.3.5. (U) Documenting Review of DE

(U//~~FOUO~~) FBI personnel must document in a report all reviews and searches of DE from the point of the receipt of DE through completion of the search, including any identification of evidence that falls within the scope of the warrant [redacted] b3 b7E [redacted] The documentation must be serialized to the investigative case file. Such documentation should identify, at a minimum, the general nature and manner in which the search of the media was conducted, major steps taken during the search, and forensic tools employed during the search.

(U//~~FOUO~~) Undocumented, "off-the-record" searches or reviews of DE are not permitted. The above documentation requirement does not apply to searches of results copies (see Section 3.2.6 for definition o[redacted]

(U//~~FOUO~~) The four categories of reports are:

1. (U//~~FOUO~~) **Content Review Report:** Reports factual information resulting from the review of DE.
2. (U//~~FOUO~~) **DExT Report:** Reports factual information [redacted] b3 b7E
3. (U//~~FOUO~~) **Report of Examination:** Reports the results of an examination performed by a certified examiner or other technical expert, usually with information regarding advanced analysis or opinions.
4. (U//~~FOUO~~) [redacted]

3.3.5.1. (U) Content Review Report

(U//~~FOUO~~) A content review report is a factual report of investigative findings resulting from the review of original, master [redacted] of the DE. [redacted] The report details who performed the review, when it was performed, what was reviewed and found, and where it was found. A content review report may be documented by completing an FD-302. Content review reports must be serialized into the investigative file. A content review report must contain, at a minimum, the following information:

- (U//~~FOUO~~) Name and contact information of the reviewer.
- (U//~~FOUO~~) Description of the working copy reviewed, including case number and original DE description.
- (U//~~FOUO~~) The physical location of where the review was completed (i.e., location of the reviewer).
- (U//~~FOUO~~) The date of the report.
- (U//~~FOUO~~) The methodology and basis for their conclusion [redacted] b7E
- (U//~~FOUO~~) Report of the responsive content found. [redacted]

(U//~~FOUO~~) All FBI personnel must also fully and officially document in the content review report any other individuals who provide substantive assistance (as opposed to purely technical assistance) [redacted]

[redacted]

(U//~~FOUO~~) A content review report must contain only factual information and must not contain expert opinions related to the DE, other than those expressly permitted in this section and considered to be advanced technical analysis (see Section 2.1, figure 1). b7E

3.3.5.2. (U) DExT Report

(U//~~FOUO~~) A DExT report is a factual report [redacted] details who performed the work, when it was performed, what was reviewed and found, and where it was found. A DExT report may be documented by completing an FD-302 in accordance wit[redacted] prescribed by OTD/DFAS. DExT reports must be serialized into the investigative case file and must contain a minimum of the following information:

- (U//~~FOUO~~) Name and contact information of the DExT.
- (U//~~FOUO~~) Case identification.
- (U//~~FOUO~~) Name of requestor and specifically what they requested.
- (U//~~FOUO~~) Description of the working copy processed, including case number and original DE description.
- (U//~~FOUO~~) The physical location of where the review was completed (i.e., location of the reviewer).
- (U//~~FOUO~~) The date of the report.
- (U//~~FOUO~~) List of procedures performed.
- (U//~~FOUO~~) What was searched for and items found of investigative importance.
- (U//~~FOUO~~) Where the DExT is a case agent or investigator, and is reviewing or conducting [redacted] on his/her own case evidence, the methodology and basis for his/her conclusion [redacted] b7E
- (U//~~FOUO~~) Report of the responsive content found, including [redacted]
- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) [redacted]

- (U//~~FOUO~~)

b7E

- (U//~~FOUO~~) What was targeted during the search and, if applicable, the order in which items were targeted

(U//~~FOUO~~) All DExTs must also fully and officially document in the DExT report any other individuals who provide substantive assistance

(U//~~FOUO~~) A DExT report must contain only factual information and must not contain expert opinions related to the DE, other than those expressly permitted in this section and considered to be advanced technical analysis (see section 2.1, figure 1).

(U//~~FOUO~~) If the DExT is an FBI investigative asset (agent or IA) and is conducting a content review and DExT review simultaneously in his or her own case, only a DExT report is required.

3.3.5.3. (U) Report of Examination

(U//~~FOUO~~) A report of examination is used to report the results must be serialized into the investigative file. For CART FEs and forensic audio, video, and image examiners, the report of examination is required to be documented by completing all fields in an FBI by OTD/DFAS. Reports of examination must be serialized into the investigative case file and must contain a minimum of the following information:

b7E

- (U//~~FOUO~~) Name and contact information of the examiner.
- (U//~~FOUO~~) Case identification.
- (U//~~FOUO~~) Name of requestor and specifically what they requested.
- (U//~~FOUO~~) Description of the working copy processed, including case number and original DE description.
- (U//~~FOUO~~) The physical location of where the review was completed (i.e., location of the reviewer).

- (U//~~FOUO~~) The date of the report.
- (U//~~FOUO~~) List of procedures performed.
- (U//~~FOUO~~) Items searched for and items found of investigative importance.
- (U//~~FOUO~~) Report of the content found and,
- (U//~~FOUO~~)
- (U//~~FOUO~~) What was targeted during the search, and, if applicable, the order in which items were targeted

b7E

(U//~~FOUO~~) All FBI personnel must also fully and officially document in the report of examination whenever they receive substantive assistance from another individual during the examination or review process (not including "help desk" type assistance).

(U//~~FOUO~~) Frequently, in the course of the investigation or during trial preparation, an examiner is asked to perform additional analysis of the DE. If this occurs, the examiner must file a supplemental report of examination, in accordance with the requirements above, to fully document the additional analysis requested in accordance with the Federal Rules of Criminal Procedure Rule 16.

3.3.5.4. (U Report

(U//~~FOUO~~)

b7E

reports must be serialized into the investigative case file and must contain the following information, if applicable:

- (U//~~FOUO~~) Case identification.
- (U//~~FOUO~~) Name of requestor and specifically what they requested.

- (U//~~FOUO~~) Description of the working copy processed, including case number and original DE description.
- (U//~~FOUO~~) The physical location of where the review was completed (i.e., location of the reviewer).
- (U//~~FOUO~~) The date of the report.
- (U//~~FOUO~~) List of procedures performed.
- (U//~~FOUO~~) What was searched for and items found of investigative importance.
- (U//~~FOUO~~) Report of the responsive content found, including
- (U//~~FOUO~~)
- (U//~~FOUO~~) What was targeted during the search, and, if applicable, the order in which items were targeted

b7E

(U//~~FOUO~~)
report any other individuals who provide substantive assistance with the search/find/extraction (not including "help desk" type assistance) They must, at a minimum, include who assisted them during the processing, and if applicable,

(U//~~FOUO~~ report must contain only factual information and must not contain expert opinions related to the DE that would fall within the description of advanced technical analysis (see Section 2.1, figure 1).

3.3.5.5. (U) Testifying Regarding Review of DE

(U//~~FOUO~~) All personnel who handle DE must be prepared to testify concerning their findings and actions when seizing, handling, previewing, processing or reviewing DE. To facilitate accurate and complete testimony, documentation should be as detailed and extensive as necessary to recall all key aspects of their activity.

3.3.5.6. (U) Retaining Results of Review

(U//~~FOUO~~) After the DE is reviewed and/or examined, the set of data that is determined to be within the scope of the legal authority, relevant, and probative or exculpatory

(U//~~FOUO~~) The results of a content review or examination

b7E

b7E

(U//~~FOUO~~) may be charged out by the case agent or any other party authorized by the case agent or case agent's chain of command.

3.3.6. (U) Copies

3.3.6.1. U) Original DE vs. Master Copy vs. Working Copy

(U//~~FOUO~~) Digital evidence is unique in that it can, in many cases, be duplicated, or imaged.

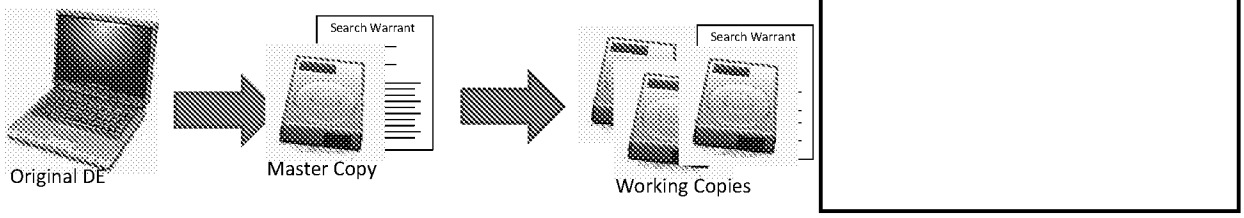


Table 2: (U//~~FOUO~~) DE Copies

(U//~~FOUO~~) **~~Original~~ Original DE**: DE seized at a search scene or otherwise legally obtained and stored in an ECF. If another agency transmits image copies on digital media without the original device accompanying it, the original copy received is the original DE copy.

(U//~~FOUO~~) With the exception of contraband, items subject to statutory forfeiture, or instrumentalities of a crime, original DE may be returned to its rightful owners when all criminal proceedings have terminated and the CDC and AUSA/prosecutor have concurred. FBI personnel who are directed to return original DE prior to the conclusion of the trial should contact their CDC/ADC and OGC to ensure the proper stipulations are entered into to prevent challenges to authenticity after return of the media. b7E

(U//~~FOUO~~) If the original DE contains contraband and the device was not forfeited, FBI personnel should not destroy the entire computer. Instead, the hard drive with the contraband should be removed and physically destroyed or contents removed in a manner that would preclude recovery.

(U//~~FOUO~~) **~~Master~~ Master Copy**: The one required copy of DE that is stored on media to be retained and logged on a chain of custody

(U//~~FOUO~~) **Working Copy**:

b7E

(U//~~FOUO~~)

(U//~~FOUO~~) Restrictions on the tracking, dissemination and copying

(U//~~FOUO~~) A copy of the original legal authority should be maintained with each working copy of the DE

(U//~~FOUO~~)

(U//~~FOUO~~) It is impossible to guarantee that

3.3.6.2. (U) Controlling Master Copies

(U//~~FOUO~~) All master copies must be saved

The original legal authority should be maintained with the master copy of the DE.

(U//~~FOUO~~) Master Copies may be in two forms:

1. (U//~~FOUO~~) [redacted] b7E

2. (U//~~FOUO~~) [redacted]

(U//~~FOUO~~) DE received in an ECF marked "master copy" must be assigned a new 1B number and given a new bar code (as applicable). In the description field, the ECT must include the original 1B number from which the DE was derived.

(U//~~FOUO~~) To ensure the integrity of the master copy and to prevent unauthorized copies from being disseminated, a master copy may only be charged out by DE personnel (i.e., CART FEs, CART techs, DExTs, and FAVP FAs).

3.3.6.3. (U) Protecting Original Evidence or Master Copies

(U//~~FOUO~~) Examinations or reviews of DE [redacted]

3.3.6.4. (U) Previews of Original Evidence

(U//~~FOUO~~) In accordance with this PG, FBI personnel may conduct previews of original DE. In these cases, personnel may only conduct previews in accordance with procedures approved by OTD/DFAS [redacted] b7E

3.3.6.5. (U) Disseminating [redacted]

(U//~~FOUO~~) [redacted] b3 b7E

(U//~~FOUO~~) All FBI personnel receiving requests fo [redacted] must first look to the language of the relevant legal authority to determine whether dissemination of images or copies of DE is authorized by the court order for the stated purpose [redacted] FBI personnel may [redacted] of that legal authority is included in the investigative case file and the provision o [redacted] is documented as outlined in this section.

(U//~~FOUO~~) [redacted] FBI personnel may, with OGC approval, disseminate [redacted] Such dissemination must be documented in the case file, as outlined in this section.

(U//~~FOUO~~) Only certified DE personnel (i.e., CART FEs, CART techs, DExTs, FAVP FAs, and OTD/DFAS Technical Experts) are allowed to make working copies. All copies made after (or from) the master copy [redacted] are required to be labeled as working copies. b7E

(U//~~FOUO~~) Case agents must document the dissemination of working copies for tracking purposes in the case file. The case agent is required to document the case agent name, the number of working copies provided, recipient [redacted] UCFN or file number, evidence number, who requested the working copy, date, time, and the purpose for the working copy.

(U//~~FOUO~~) At the discretion of the case agent or case agent's supervisor, working copies may be submitted to an ECF for chain of custody tracking. In addition, the creation of the copy must be documented by the certified DE personnel in the examination file or DExT report, as applicable.

(U//~~FOUO~~) The case agent or FBIHQ program manager may disseminate working copies of DE [redacted]

(U//~~FOUO~~) Because DE may contain contraband, personally identifiable information (PII), privileged or other legally protected information, [redacted] must be appropriately marked [redacted]

3.3.6.5.1. (U) Copies of DE for US Attorneys

(U//~~FOUO~~) Only [redacted] DE shall be provided to USAOs, unless otherwise authorized by this section. To obtain a working copy of DE, the USAO must request the copy in writing and explain the purpose of obtaining an image or working copy of the media. The request must include whether the USAO intends to further disseminate the media and, if so, to whom and for what purpose (e.g., to facilitate an examination or review by non-FBI personnel). In this event, the request should be handled [redacted] request or re-examination request (as outlined below). When reviewing such a request, FBI personnel may only comply when the following requirements have been met:

- (U//~~FOUO~~) The court order clearly authorizes such a dissemination under the relevant circumstances.
- (U//~~FOUO~~) The affiant advised the court that such dissemination would occur under the relevant circumstances in the underlying application for the legal authority.
- (U//~~FOUO~~) The case agent, in consultation with his or her CDC and OGC [redacted] determines such a dissemination is otherwise authorized. b7E

(U//~~FOUO~~) Statements in search warrant affidavits or other applications or orders ambiguously authorizing the search and seizure of media by "government personnel," or similar language, are insufficient to meet the above requirements. For purposes of this section, “government personnel” does not include assistant United States attorneys, paralegals, or other personnel in a United States Attorney’s Office, or trial attorneys, paralegals or other personnel in the Department of Justice that do not meet the definition

of a "federal law enforcement officer" authorized to execute a search warrant in Rule 41(a)(2)(C), Federal Rules of Criminal Procedure.

(U//~~FOUO~~) The above restriction applies in circumstances where the judicial order authorizes the ultimate seizure of only a subset of data that exists on the media initially seized [redacted] b7E

[redacted]

(U//~~FOUO~~) If FBI personnel are requested to provide such copies or otherwise facilitate such a transfer, they should inform the unit chief, Forensic Operations Unit, their squad supervisor, and their CDC. When personnel comply with such a request pursuant to the procedures described above, they must clearly document the details of the request and compliance with the above requirements in the agent's investigative case file and, if applicable, any digital evidence examination file. FBI personnel also must comply with any other relevant policy or procedures, such as the need to obtain the approval of the assistant director of OTD for a second examination of digital evidence.

3.3.6.5.2. (U) Discovery Requests

(U//~~FOUO~~) FBI personnel handling DE must comply with defense demands for discovery.

(U//~~FOUO~~) The dissemination of working copies of DE to the defense to facilitate a discovery request is the case agent's responsibility. Prior to disseminating working copies for discovery, the case agent must protect PII, such as social security numbers, telephone numbers, bank account numbers, and medical records in accordance with federal law. The case agent must document the provision of discovery copies in the investigative case file.

3.3.6.5.2.1. (U) Providing DE with No Contraband

(U//~~FOUO~~) The party requesting discovery must either supply suitable (size, quantity, and type) media for duplication of the data subject to disclosure or make arrangements for replacement of expended media.

(U//~~FOUO~~) Copies prepared pursuant to a discovery request are typically [redacted] b7E [redacted] and must be verified as appropriate for disclosure by the case agent in consultation with the AUSA prior to release as discovery. In accordance with DOJ e-discovery guidance, the FBI is under no obligation to create [redacted] for discovery. The FBI does not provide this service due to the administrative burden and the inability [redacted]

b7E

3.3.6.5.2.2. (U) Requests for DE Containing Contraband

(U//~~FOUO~~) When discovery is requested of material containing contraband (e.g., child pornography), the FBI must follow the procedures outlined in 18 U.S.C. § 3509(m) the "Adam Walsh Child Protection and Safety Act" (the Act). Pursuant to the Act, the FBI is required to make reasonable accommodations for the defense to have access to such material in an FBI facility specifically configured for these types of reviews, frequently called Adam Walsh rooms. Reasonable accommodations include access to the government-controlled facility during normal business hours, access to telephones, the Internet, and printers. Defense experts may make special, advanced arrangements to use the facility outside normal business hours. However, this must be based on a compelling need and will not be done as a matter of routine practice due to the fiscal and manpower expense to the FBI.

(U//~~FOUO~~) Defense experts may use their own computers and tools to conduct an analysis. However, they must be notified in advance that any digital media entering the government facility must be forensically wiped prior to departure in order to ensure FBI compliance with the requirements of the Adam Walsh Act. If the field office does not have a segregated Adam Walsh room, the chief security officer (CSO) must be notified in advance that defense experts may have laptops or other portable electronic devices to support the discovery. The case agent must coordinate with the CSO for appropriate access. If the defense expert requires more than one session to complete the exam, reasonable accommodation may also include that the FBI provide either a lockable, private space within the government-controlled facility or a locking safe, in which the defense expert may store his or her tools and equipment when away from the room. These measures ensure attorney-client privilege and work products are not accidentally exposed to the government.

(U//~~FOUO~~) If a defense expert requests to take any materials generated during the examination from the government-controlled facility, all materials must be reviewed to ensure that no contraband, law enforcement sensitive (LES), or classified materials are included. If the defense expert objects to this review, CART personnel should notify their supervisor(s) and CDC/ADC or OGC [redacted] r input and assistance in resolving the issue. If those parties are not able to negotiate a resolution, the prosecutor on the case must be notified to obtain his or her assistance in securing a protective order from the court handling the case. It is recommended that the order include, at a minimum, a direction to each member of the defense team to individually certify, under oath and in writing, that they have taken no materials which are considered contraband under federal law away from the government-controlled facility upon completion of the defense examination, and that they have not caused any contraband to be sent offsite.

b7E

(U//~~FOUO~~) If a defense expert represents to the court that it is not feasible to bring his or her tools and equipment to the government facility, the FBI may supply forensic tools and equipment, including appropriate forensic tool licenses, limited to the forensic tools and equipment currently used by the FBI at the time of the request.

b7E

3.3.6.5.2.2.1. (U) Special Guidelines for RCFLs in State or Local Cases

(U//~~FOUO~~) For purposes of handling DE reasonably believed to contain contraband in state and local cases, RCFLs should follow the guidelines listed above whenever possible to prevent the contraband from being redistributed and the victims re-victimized. However, with respect to purely state or local cases, RCFLs are obligated to follow state or local court orders governing discovery.

3.3.6.6. (U)

3.3.6.6.1. (U) Disseminating

(U//~~FOUO~~) Case agents may, with the supervisor's approval, provide copies of the to authorized law enforcement, prosecutors in furtherance of a lawful purpose and consistent with the terms of the search warrant or other legal authority.

(U//~~FOUO~~) All personnel who handle DE must document dissemination of copy in the case notes, case report, and CART database, if applicable

(U//~~FOUO~~) Once submitted to the ECF, the case agent may copy and disseminate copies and associated reports. If the case agent makes copies he or she is required to label the media in the same manner as the original (e.g., classification markings, banners, file number, and handling caveats).

3.3.7. (U) Approved Tools

b7E

(U//~~FOUO~~) Approved tools must be used by all DE personnel during

(U//~~FOUO~~) Approved tools for processing DE are listed of many approved tools requires successful completion of OTD/DFAS-approved training.

(U//~~FOUO~~) In addition to tools listed on the approved tool list,

(U//~~FOUO~~) For each approved version of each tool, the approved tool list provides information about the forensic processes for which the tool is approved, as well as the

known limitations of the tool. DE personnel are responsible for understanding these limitations prior to the use of the tool on DE.

3.3.7.1. (U) Adding Approved Tools

(U//~~FOUO~~) OTD/DFAS must approve tools in accordance with OTD/DFAS test and validation protocol and based upon appropriate scientific and evidentiary criteria.

(U//~~FOUO~~) Recommendations to add tools to the approved tool list may be submitted to the OTD/DFAS/Forensic Support Unit (FSU). Tool testing, validation, and verification must be coordinated through OTD/DFAS/FSU, although actual testing may be performed by personnel from other divisions or agencies as approved by OTD/DFAS.

3.3.8. (U)

(U//~~FOUO~~) Case agents should coordinate with OTD

Case agents should be aware that the use of unapproved is discouraged

(U//~~FOUO~~) When using b7E

3.3.9. (U) Requests for

3.3.9.1. (U) Examinations of Digital Evidence in FBI Cases

(U//~~FOUO~~) Except as authorized in this PG (see Appendix E, Examination of FBI Evidenc, all evidence generated by FBI criminal must be submitted for forensic examination or forensic analysis to an FBI laboratory or forensic program authorized by the FBI Science and Technology Branch (STB). "Forensic examination(s)" or "forensic analysis (es)" are either:

- (U//~~FOUO~~) Generated as part of a process applied by a recognized forensic discipline of the American Society of Crime Laboratory Directors (ASCLD) or the ASCLD-Laboratory Accreditation Board (ASCLD-LAB), or the International Standards Organization (ISO). b7E
- (U//~~FOUO~~) Commonly described or recognized as "forensic" or otherwise relating to the analysis of evidence by scientific or technical means or manner of evidence by or through an expert witness, as defined by the Federal Rules of Evidence (or their applicable equivalent) or as pronounced by rule or ruling of any court or tribunal.

(U//~~FOUO~~)

3.3.9.1.1. (U) Transfer of Evidence

3.3.9.1.1.1. (U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

3.3.9.1.1.2. (U) Chain of Custody

(U//~~FOUO~~) In criminal investigations, once FBI evidence has been b7E is responsible for maintaining any chain of custody on all original and derivative evidence created through the examination process until the completion of all trials and appeals. FBI personnel may not retain duplicate evidence or samples of evidence without the prior written concurrence of the AD, OTD.

3.3.9.1.2. (U) Non-Circumvention of FBI Policy

(U) A referral authorized by this PG may not be used, in whole or in part, to purposefully effectuate or passively benefit from activity that would otherwise violate FBI policy, including:

- (U) b7E
- (U

3.3.10. (U) Service Requests in Support of Administrative or Civil Matters

(U//~~FOUO~~) FBI personnel and facilities s) may not accept service requests to provide DE services in administrative or civil matters. The AD, OTD, may grant exceptions after consultation with OGC In considering requests for exceptions, the AD, OTD must consider:

- (U) Whether such support would constitute an acceptable use of appropriated funds.
- (U) The impact on the FBI of using available examiner and equipment resources in support
- (U) The cost to the FBI in having to provide personnel to testify in a civil matter, as well as be deposed and complete other civil discovery.

- (U) Other relevant factors presented by particular situations.

(U//~~FOUO~~) These limitations do not preclude providing DE support for FBI internal investigation matters, or for RCFLs to provide DE suppor [redacted] b7E

[redacted]

(U//~~FOUO~~) If the FBI receives civil or administrative legal process (e.g., a subpoena) in connection with DE services performed for a criminal [redacted], the individual served must coordinate with his or her CDC/ADC or OGC counsel for guidance, as applicable. b3 b7E

3.3.11. (U) Re-examinations

3.3.11.1. (U) Definition of Examination

(U//~~FOUO~~) An examination is defined as a forensic process whereby a forensic examiner reviews digital evidence [redacted]

[redacted] b7E

(U//~~FOUO~~) Examination of data previously reviewed by a DExT is not considered a re-examination.

3.3.11.2. (U) Overview of Re-examinations

(U//~~FOUO~~) Unless approved by the AD, OTD as outlined below, examinations are not conducted on any evidence that has been previously subjected to the same type of technical examination (hereafter referred to as a "re-examination.")

(U//~~FOUO~~) A re-examination occurs when evidence, already subjected to a technical examination [redacted]

(U//~~FOUO~~) This requirement is intended to:

- (U//~~FOUO~~) Eliminate duplication of effort.
- (U//~~FOUO~~) Ensure that the integrity of the evidence is maintained. b7E
- (U//~~FOUO~~) [redacted]
  - (U//~~FOUO~~) [redacted]

- (U//~~FOUO~~)
- (U//~~FOUO~~)

b7E

3.3.11.3. Requesting a Re-examination

(U//~~FOUO~~) Within the FBI, re-examinations may only be requested by an EC approved by the requesting field office's division head. ECs should be addressed to the AD, OTD, and be routed through the chief, CART-FOU and the appropriate CART Field Operations Program manager

(U//~~FOUO~~) The request should include a letter from the United States Attorney (or District Attorney if a state or local case), containing:

- (U//~~FOUO~~) The extraordinary circumstances compelling the requested re-examination.
- (U//~~FOUO~~) A detailed explanation of the facts and circumstances surrounding the request.
- (U//~~FOUO~~) All existing service requests.
- (U//~~FOUO~~) All existing legal authorities.
- (U//~~FOUO~~) All prior examination results, notes, and reports pertaining to the previous examinations or reviews, or an explanation as to why this material is not available.

(U//~~FOUO~~) In the event of exigent circumstances

b7E

3.3.11.4. Approval of Re-examination Requests

(U//~~FOUO~~) Upon receipt of a request for re-examination, the chief, CART-FOU will review the request and supporting materials to determine if a particular examination request is a re-examination for the purpose of seeking the AD, OTD's approval.

(U//~~FOUO~~) After the chief, CART-FOU determines that the requested examination is a re-examination, he or she prepares a recommendation of approval or denial for the AD, OTD that considers the following factors:

- (U//~~FOUO~~) Scope of the requested re-examination.
- (U//~~FOUO~~) Responsiveness of the prior examination to previous and current service requests or legal authorities.
- (U//~~FOUO~~) Type of tools used in the prior examination or review (e.g., generally accepted forensic tools).

- (U//~~FOUO~~) Location of agency and type of facility that performed the prior examination or review [redacted] b7E
- (U//~~FOUO~~) Nature of prior review or examination (including whether prior examination substantially followed or were analogous to FBI CART SOPs).
- (U//~~FOUO~~) Whether documentation of prior examination or review provides sufficient detail (including whether there are indicia of a completed examination, [redacted]
- (U//~~FOUO~~) Background and certification of previous examiner.
- (U//~~FOUO~~) Purpose of previous review or examination.

(U//~~FOUO~~) The AD, OTD will consider the request for re-examination and, after coordination with OGC [redacted] as needed, approve or disapprove the request. Notice of approval or disapproval of the re-examination request will be transmitted via EC (to FBI field offices or headquarters divisions [redacted] If approved and if required by the circumstances, the approval document may also outline any conditions or limitations placed on the re-examination. The approval documentation will be maintained in the examination file.

(U//~~FOUO~~) Questions regarding whether a service request constitutes a re-examination should be directed to the appropriate DFAS unit.

(U//~~FOUO~~) The case agent must make all necessary notifications to the prosecutor concerning potential [redacted] that is or may be created as a result of the re-examination.

3.3.12. (U) Advanced Technical Analysis

(U//~~FOUO~~) Advanced technical analysis of DE may only be performed by [redacted]

3.3.12.1.1. (U [redacted] b7E

(U//~~FOUO~~) Requests for advanced analysis must be made via a service request. All service requests must be documented via EC or, where available, an automated request through the approved OTD/ [redacted], using an open FBI case file, or by a request for assistance from [redacted] to the field office or RCFL.

3.3.12.2. (U//~~FOUO//LES~~) [redacted]

(U//~~FOUO//LES~~) [redacted]

3.3.12.3. (U) Forensic Audio Video Image Analysis [redacted] b7E

(U//~~FOUO~~) All requests for advanced forensic [redacted] must be submitted to OTD/FAVIAU via EC or other appropriate documentation identified by FAVIAU.

3.3.12.3.1. (U//~~FOUO//LES~~) [redacted]

(U//~~FOUO//LES~~) All requests for [redacted]

3.3.12.3.2. (U//~~FOUO//LES~~) [redacted]

(U//~~FOUO//LES~~) All requests for [redacted]

3.3.13. (U) Assigning Requests to Examiners and DE Backlog Definition

(U//~~FOUO~~) In order to more accurately assess backlog of DE requests, the backlog is defined as "any unassigned request that is over 30 days old." To ensure an effective and efficient workflow, supervisors should assign service requests as examiners become available to actively address the request. At no time should a service request be assigned to avoid being identified as backlog.

(U//~~FOUO~~) The goal is to more accurately track digital forensic backlog by identifying requests that the field office does not have the resources to address. To further facilitate an accurate accounting of backlog, service requests should be limited to no more than ten unique items. The case agent or requestor should list out the items in the service request and rank them in order of priority to their investigation. [redacted] b7E

(U//~~FOUO~~) Service requests can be entered directly into the CART database by the case agent or by CART personnel on behalf of the case agent. Service requests entered by CART personnel into the CART database must be inputted within one business day of receipt, regardless of other proprietary software/databases used to manage service requests in individual field offices and RCFLs.

5. (U) Recordkeeping Requirements

5.1. (U//~~FOUO)~~ FBI Central Recordkeeping System

(U//~~FOUO)~~ DE must not be serialized into the FBI's central recordkeeping system or any other FBI administrative or records management system (e.g., The FBI's central recordkeeping system (current) is the FBI's official recordkeeping system for all case file management. Non-record materials, per the legal definition of federal records, must not be placed in the case file or case file system. Non-record materials include any copies preserved for convenience or reference. Though the FBI's central recordkeeping system has the ability to accept many documents and file types as either a serial or an attachment to both electronic communications (ECs) and forms, current policies dictate the guidelines for what material is authorized to be placed in the FBI's central recordkeeping system. All original digital evidence (1B) and ELSUR evidence (1D) must be maintained and handled per evidence procedures and guidelines, and as such, original digital and ELSUR evidence must not be serialized, attached to any document, maintained, or stored in the FBI's central recordkeeping system. b7E

b7E

should be retained in the 1A or 1C section of the case file and thus may be serialized into the FBI's central recordkeeping system. Under no exception should contraband material be serialized into the FBI's central recordkeeping system.

5.2. (U) Additional Guidance on Recordkeeping and Forms Use

- (U) ~~FOU~~ Intranet web site: b7E
- (U) DEL Quality Assurance Intranet web site:
- (U) DEL Training Intranet web site:
- (U) Domestic Investigations and Operations Guide (DIOG):
- (U)

Appendix A: (U) Sources of Additional Information

(U) Please review the following Intranet web sites for additional information:

(U//~~FOUO~~) All of the below are to be marked (U//~~FOUO~~), [redacted] b7E

[redacted]

They are not to be identified to the public.

- [redacted]

Appendix D (U): Definitions and Acronyms

(U) Defined Concepts

(U) Seizure vs. On-scene Imaging vs. Processing

(U//~~FOUO~~) There is often a great deal of digital media at a search site. Because processing and reviewing this media consumes valuable FBI resources, it is important to

(U//~~FOUO~~) On-scene, digital media may either be

b7E

Otherwise, based on legal authority, there may be a decision as to whether to

It is important to know that imaging is a time-consuming process that may take hours or days depending upon on the amount of data to be copied.

(U//~~FOUO~~) Once seized DE and images made on-scene are back at an FBI facility, they may be processed using kiosks or preview methods

U//~~FOUO~~.

b7E

Figure 3: (U//~~FOUO~~)

(U) Imaging (Copying) DE b7E

(U//~~FOUO~~) DE is an unusual kind of evidence in that, in most cases, it can be copied many times without degrading the original evidence. Most computer users are familiar with copying files

(U//~~FOUO~~) In order to preserve and maintain the original evidence as it was found

(U//~~FOUO~~) To prevent cross contamination

(U//~~FOUO~~) The above processes related to described in the CART standard operating procedures (SOPs).

(U) Definitions

(U//~~FOUO~~) **Approved Tools –** Tools that have been successfully tested and validated for processing DE or are native applications and utilities necessary for viewing files with proprietary formatting. Approved tools are listed on the OTD Intranet website.

(U//~~FOUO~~) **Computer Analysis Response Team –Technician (CART tech)** – Personnel trained and certified to forensically copy or image DE.

(U//~~FOUO~~) **Computer Analysis Response Team Forensic Examiner (CART FE)** – FBIHQ or field personnel, typically assigned full-time to DE work, who are trained, equipped, and certified to copy or image DE, search DE, extract data from DE, and who are authorized to provide opinions related to DE in court.

(U//~~FOUO~~) **CART On-the-Job Trainee (OJT)** – Personnel identified by field office management to participate in training with a commitment toward becoming certified CART FEs.

(U//~~FOUO~~) **CART Forensic Examiner Trainee (FET)** – Personnel assigned to work toward CART FE certification 100% of their time. Typically, these are trainees hired into ITS-FE positions. These may also be CART OJTs who are near the end of their training and have committed 100% of their time to CART FE work.

(U//~~FOUO~~) **Content Review Report** – Factual report of search/find/extract information that details who performed the work, when it was performed, what was reviewed and found, and where it was found.

(U//~~FOUO~~) **Computer Scientist - Field Operations (CS-FO) –** The CS-FO works as an integral member of an investigative team supporting FBI investigations and operations. The CS-FO is responsible for providing advanced technical analysis, exploiting data

b7E

(U//~~FOUO//LES~~) **DFAS Technical Experts** – DFAS

(U//~~FOUO~~) **Digital Evidence** – Data stored digitally on integrated circuits, micro controllers, chips, tapes, magnetic media, optical media or other devices that assist in proving or disproving a matter at issue in a case or investigation.

(U//~~FOUO~~) **Digital Evidence Extraction Technician (DExT)** – Personnel trained to copy or image DE and perform simple search/find/extract processes on copies of DE.

(U//~~FOUO~~) **Report of Examination** – The official report of examination used by CART FEs and Forensic Audio Video Image examiners and other DE technical experts to report the results of advanced technical analysis and/or document opinions formed as a result of that analysis (e.g., Digital Evidence Laboratory

(U//~~FOUO~~) **Digital Evidence/Media Handling** – Physical treatment of digital media beginning with the initial identification, seizure, packaging, transport, shipment, storage, and control.

(U//~~FOUO~~) **Digital Evidence Personnel** – Personnel who are authorized upon completion of FBI approved training in the handling and processing of digital evidence/media (i.e., DExT, CART personnel, and FAVP FA).

b7E

(U//~~FOUO//~~LES) **Digital Evidence Processing –** Processing of DE applies to personnel who are trained and tested to process DE and includes procedures related to on-scene preview, imaging, memory capture, content review, DE search, extraction, preparing reports, and advanced technical analysis

(U//~~FOUO~~) **Examination** – Forensic process whereby a forensic examiner reviews digital evidence Examinations have a specific scope as defined by the supporting legal authority and the service request pertaining to the evidence submitted for examination. The legal authority and service request may define the scope of the examination

(U//~~FOUO~~) Examination of data previously reviewed by a DExT is not considered a re-examination.

(U//~~FOUO~~) **Expert Opinion** – Judgment regarding certain facts or data either acquired by an expert's own investigation, testing, or observations and based on his knowledge,

skill, experience, training, or education in a certain scientific, technical, or other specialized field.

(U//~~FOUO~~) **Expert Testimony** – Testimony of a witness qualified as an expert (scientific, technical or specialized field) by knowledge, skill, experience, training, or education, in the form of an opinion or otherwise. This testimony is based on sufficient facts or data, is the product of reliable principles and methods, and is grounded upon principles and methods that have been applied reliably to the facts.

(U//~~FOUO~~) **Extraction** – DE that has been [redacted] b7E
[redacted] and provided for investigative purposes.

(U//~~FOUO~~) **Fact Witness** – A fact witness has personal knowledge of events pertaining to a case and can only testify to things he personally has observed. A fact witness cannot offer opinion.

(U//~~FOUO~~) **Field Audio Video Personnel (FAVP) Forensic Analyst (FA) –** Personnel trained to perform basic forensic functions related to audio and video DE.

(U [redacted]

(U//~~FOUO~~) **Master Copy** – The required copy of DE that is stored on media to be retained and logged on a chain of custody. This is [redacted] copy of the original DE or a logical copy that contains selected files and artifacts from the original DE, such as relevant files from a business server. It is important that the original legal authority be maintained with the master copy of the DE. If there is a question of whether a copy of the legal authority documents can be retained and/or forwarded, contact OGC or local CDC.

(U//~~FOUO~~) **Original DE** – DE seized at a search scene or otherwise legally obtained and stored in an ECF.

(U) **Random Access Memory (RAM) –** A computer system's memory which contains contents of recent applications and data so they can be accessed quickly when needed by the computer's processor.

(U//~~FOUO~~) **Regional Computer Forensics Laboratory (RCFL) Associate Examiner** – Former certified CART FE from an agency participating in the RCFL program who has completed their commitment to the RCFL, returns to their home agency, and continues a relationship with the RCFL to maintain certification and training.

(U//~~FOUO~~) **Re-examination** – A re-examination of DE occurs when data/evidence, [redacted] b7E

(U//~~FOUO~~) [redacted] – Less than a full copy of the original DE [redacted]

(U) **Volatile Memory** – Memory that is not retained when power is lost to a device.

(U//~~FOUO~~) **Working Copy** – Additional full copies of DE derived from the Master copy to allow review by personnel working for or with the FBI in its investigations [redacted]

Appendix E (U//~~FOUO~~): Examination of FBI Evidence [redacted] b7E

[redacted]

(U//~~FOUO~~) As discussed above in section 3.2.9.1., all evidence generated by FBI criminal and [redacted] investigations (including joint investigations) must be submitted for forensic examination or forensic analysis to a laboratory or authorized forensic program of the FBI Science & Technology Branch (STB), unless an exception to policy is approved in accordance with this Appendix.

(U//~~FOUO~~) In rare instances, the unique demands of a particular case may prompt a USAO, DOJ entity, or other prosecutorial or investigative agency to have FBI evidence processed, examined or analyzed [redacted] b7E

[redacted]

(U//~~FOUO~~) This procedure is separate and distinct from re-examination (as defined in section 3.2.11.2. above). A re-examination occurs when evidence, already subjected to a technical examination, is reviewed for the same probative data of its content, source, origin, and manner of creation, alteration, or destruction.

(U//~~FOUO~~) Further [redacted] FBI personnel shall follow the guidance in section 3.2.9.1.1 regarding the transfer of evidence.

(U//~~FOUO~~) Subject to the referral prohibitions described below (section entitled Mandatory Prerequisites and Discretionary Referral Factors), the SC, DFAS, after consultation as desired with an assistant general counsel (AGC [redacted] (OGC [redacted] may authorize [redacted] transfer of FBI evidence [redacted] certified forensic examiner or laboratory only under the following conditions: b7E

- (U//~~FOUO~~) After a determination of the existence of the mandatory prerequisites and due consideration and evaluation of the discretionary referral factors described below.
- (U//~~FOUO~~) After consultation as may be deemed appropriate with the appropriate prosecutor and the applicable CDC or OGC supervisor.
- (U//~~FOUO~~) After compliance with the administrative requirements below (section entitled Administrative Requirements).

(U//~~FOUO~~) [redacted]

(U//~~FOUO~~) Within the FBI [redacted] may only be requested via an EC approved by the requesting field office's division head. ECs should be addressed to the AD, OTD, and be routed through the chief, CART-FOU and the appropriate CART Field Operations Program manager. b7E

[redacted]

(U//~~FOUO~~) The case agent must ensure that the request EC is serialized to the relevant investigative case file. This EC must include:

- (U) The FBI case ID or universal case file number (UCFN).
- (U) The FBI field office, telephone number and fax number.
- (U) The FBI case agent's name.
- (U) The applicable case prosecutor's name, if known.
- (U) A description of the original evidence to be released.
- (U) The full name, address and telephone number of [redacted] b7E
- (U) A certification that a supervisory prosecutor and CDC have concurred in the request, and that the supervisory prosecutor has read and understands the FBI's policy [redacted]
- (U) The full name and position title of the case agent's Supervisory Special Agent (SSA).
- (U) An acknowledgement from the case agent that he/she understands it is the case agent's responsibility to make all required notifications to the prosecutor concerning [redacted]

(U//~~FOUO~~) [redacted] request should include a letter from the United States Attorney, or District Attorney if a state or local case, [redacted] b7E

(U//~~FOUO~~) [redacted]

(U//~~FOUO~~) Approving [redacted]

(U//~~FOUO~~) Mandatory Prerequisites and Discretionary [redacted]

(U//~~FOUO~~) The SC, DFAS must not authorize [redacted] unless the SC affirmatively determines that either of the following prerequisites is met:

(U//~~FOUO~~) [redacted] b7E

Directors -Laboratory Accreditation Board (ASCLD-LAB), or International Standards Organization (ISO). forensic examiner must possess at the time of referral and, thereafter, maintain competency certifications(s) and meet proficiency requirements applicable to the recognized discipline or sub-discipline that has accredited b7E

(U//~~FOUO~~)

- (U//~~FOUO~~)
- (U//~~FOUO~~) In the judgment of the SC, DFAS, otherwise be objectively suitable after considering and weighing each

(U//~~FOUO~~)

(U//~~FOUO~~) Assuming that the prerequisites described in the section above are met, the SC, at his or her discretion, may authorize an

- (U//~~FOUO~~) Breadth of experience: the number and complexity of forensic examinations/analyses conducted
- (U//~~FOUO~~) Testimonial experience: the experience
- (U//~~FOUO~~) Report quality: the quantity and quality of written reports produced b7E
- (U//~~FOUO~~) Equipment acceptance:
- (U//~~FOUO~~) Testing and evaluation documentation: whether there exists sufficient test and validation documentation on the equipment, tools or materials
- (U//~~FOUO~~) Written protocols

documentation adequate to facilitate the repeatability of results by an equally qualified examiner.

- (U//~~FOUO~~) Applied quality assurance system [redacted] b7E
  - (U//~~FOUO~~) Annual, impartial, testing-based, proficiency examinations.
  - (U//~~FOUO~~) Peer review of examination results and reports.
  - (U//~~FOUO~~) Random and/or regular external compliance audits.
- (U//~~FOUO~~) Legal requirements [redacted] the examiner is employed or conducting forensic examinations has an affirmative procedure to evaluate, determine and monitor the ability of the examiner to testify in federal court relative to [redacted] or whether there exists a process for evaluating the existence of exculpatory information, which, as a matter of law, must be affirmatively disclosed, with or without request. [redacted]
- (U//~~FOUO~~) Law enforcement authority: whether there is a requirement that examinations are conducted by personnel employed by federal, state or local law enforcement agencies as may be required by law or under the direct supervision of a sworn law enforcement officer (see e.g., United States v Shrake, 515 F.3d U.S. 743 (7th Cir. 2008)) or whether the examination processes are conducted by an examiner who is a federal law enforcement officer or who is working at the direction of a federally sworn officer pursuant to 18 U.S.C. § 3105, if applicable.
- (U//~~FOUO~~) Space restrictions: whether the department, agency, or entity under which the examiner operates has an affirmative process in place requiring that examinations of contraband are conducted in law enforcement controlled space as required under the Adam Walsh Child Protection and Safety Act.
- (U//~~FOUO~~) Contraband: whether adequate controls exist to prevent unauthorized access or distribution of contraband pursuant to law (see e.g., child pornography at 28 U.S.C. § 2252, et seq. or controlled substances pursuant to 21 U.S.C. § 881, et seq.).
- (U//~~FOUO~~) Criminal history/indices check: [redacted] b7E
- (U//~~FOUO~~) Security requirements: the maintenance of an appropriate security level clearance relative to the FBI evidence being examined or analyzed in conformity with FBI security policy, as well as the facility and IT system in which the evidence will be stored and reviewed that is compliant with FBI security policy and [redacted] b3 b7E

- (U//~~FOUO~~) Occupational safeguard services: whether there is available [redacted] b7E
- (U//~~FOUO~~) Depth/adequacy of examination: whether all necessary examinations, routines, and procedures will be conducted [redacted] (federal violations frequently require different elements of proof than do state or local violations of the same or similar nature).
- (U//~~FOUO~~) Preservation of original/best evidence: whether the examination process [redacted]
- (U//~~FOUO~~) Cost: [redacted]

(U//~~FOUO~~) Administrative Requirements

(U//~~FOUO~~) Prior to initiating a request [redacted]

- (U//~~FOUO~~) Conduct the examination(s) as well as testify as required at all proceedings associated with the case.
- (U//~~FOUO~~) Conduct all necessary examinations in light of the fact that violations of federal law often require different elements of proof than the same or similar state or local violations.
- (U//~~FOUO~~) Not destroy or impair the admissibility of the evidentiary material
- (U//~~FOUO~~) Consult either the FBI Laboratory or OTD DEL, as applicable, on scientific and technical aspects for the examination, if needed
- (U//~~FOUO~~) Notify either the FBI Laboratory or OTD DEL if examination will consume the evidentiary material.
- (U//~~FOUO~~) Promptly provide a copy of the examination report to either the FBI Laboratory or OTD DEL after the examination is completed.

(U//~~FOUO~~) The OTD DEL must notify the case agent of any prior knowledge regarding the proposed [redacted] concerning the examiner's ability to meet the basic standards of practice of the scientific discipline involved in the examination, or the use of practices that may call into question the ability to use the evidence and examination results at or administrative results at any judicial or administrative proceedings. This contact will be documented by the case agent via EC in the investigative case file. b7E

(U//~~FOUO~~) Referral Prohibitions

(U//~~FOUO~~) Disqualified b7E

(U//~~FOUO~~)

- (U//~~FOUO~~)
- (U//~~FOUO~~)

- (U//~~FOUO~~) The FBI has information to believe
- (U//~~FOUO~~)

(U//~~FOUO~~) Second Opinion Examinations

(U//~~FOUO~~) may not be used, in whole or in part, to seek or obtain second b7E opinions regarding or re-examinations of a forensic examination/analysis or variations of an examination/analysis already commenced or completed by an FBI STB laboratory without obtaining re-examination authority as described in section 3.2.11 of this PG. If authority is sought for a second opinion or re-examination, the case agent must notify the prosecutor that no testimony should be provided on the same technical subject or area, or regarding the initial examination (testimony will be provided for the defense if required by law). The case agent must make all required notifications to the prosecutor concerning material that is created as a result of the second opinion or re-examination.

(U//~~FOUO~~) "Curbstone" or Informal Evaluations or Advice

(U//~~FOUO~~) may not be used, in whole or in part, to seek or obtain "curbstone," ad hoc, or informal opinions or advice by or from non-FBI scientific or technical personnel to assess the potential value of FBI evidence prior to submitting it to FBI STB laboratories (e.g., FBI personnel may not provide FBI evidence to a non-FBI scientific or technical person to obtain an informal, undocumented or "off the record" opinion on whether it should be submitted to an FBI STB laboratory, or what type of examination should be requested).

(U//~~FOUO~~) Investigations Prohibited. b3 b7E

(U//~~FOUO~~)

- (U//~~FOUO~~)

- (U//~~FOUO~~) [redacted] b3 b7E
- (U//~~FOUO~~) [redacted].
- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) [redacted]

(U//~~FOUO~~) Documentation Requirements.

(U//~~FOUO~~) The SC, DFAS must prepare an EC containing the approval or denial [redacted] b7E request and the case agent must ensure that the EC is serialized to the relevant investigative case file. This EC must include:

- (U//~~FOUO~~) The date the request was either approved or denied.
- (U//~~FOUO~~) In the case of an approved [redacted] referral, a certification by the SC, DFAS that he/she has determined that the proposed [redacted]