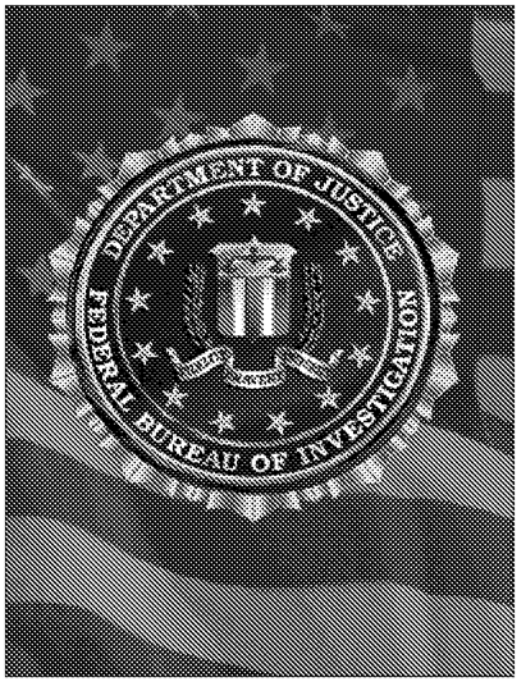
(U) Digital Evidence Policy Guide



(U) Federal Bureau of Investigation

(U) Operational Technology Division

(U) 0830PG

(U) July 31, 2016

20-cv-9284(FBI)-1

(U) General Information

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

(U) Federal Bureau of Investigation Headquarters, Operational Technology Division

(U) Division point of contact: division policy officer, [redacted]

b6 -1
b7C -1
b7E -1

(U) Supersession Information

(U) This policy guide supersedes the *Digital Evidence Policy Directive and Policy Guide*, 0639DPG.

(U) This document and its contents are the property of the FBI. If the document or its contents are provided to an outside agency, it and its contents are not to be distributed outside of that agency without the written permission of the unit listed in the contact section of this policy guide.

U) This policy guide is solely for the purpose of internal 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) DIOG Provision

(U) No policy or PG may contradict, alter or otherwise modify the standards of the *Domestic Investigations and Operations Policy Guide* (DIOG). Requests for DIOG modifications can be made to the Internal Policy office (IPO) pursuant to DIOG subsection 3.2.2, paragraphs (A), (B), (C), and (D).

(U) Law Enforcement Sensitive ~~(LES)~~

The information marked (U//~~LES~~) in this document is the property of the Federal Bureau of Investigation 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.

20-cv-9284(FBI)-2

(U) Table of Contents

1. (U) Introduction 1
1.1. (U) Purpose 1
1.2. (U) Background 1
1.3. (U) Scope 2
1.4. (U) [redacted] of Digital Evidence ..... b3 -1 b7E -2, 3, 4, 5
1.4.1. (U) Digital Evidence Searches Under [redacted] 2
1.4.2. (U) Reviews or Examinations of Digital Evidence in [redacted] Investigations 3
1.5. (U) Intended Audience 4
2. (U) Roles and Responsibilities 5
2.1. (U) Digital Evidence Roles 5
2.2. (U) Digital Evidence Responsibilities 8
2.2.1. (U) FBI Personnel Who Handle, Process, or Perform Content Reviews of Digital Evidence 8
2.2.2. (U) Federal Bureau of Investigation Headquarters 10
2.2.3. (U) FBI Field Offices 12
3. (U) Policies 14
4. (U) Procedures and Processes 15
4.1. (U//~~FOUO~~) Forensic Program Compliance Within the FBI 15
4.2. (U) Digital Evidence Handling 15
4.2.1. (U) Personnel Authorized to Handle Digital Evidence 15
4.2.2. (U) Presearch Considerations ..... 15 b7E -3, 4, 5
4.2.3. (U) Timeframe for Warrants Involving Digital Evidence 15
4.2.4. (U) Consent Searches for Digital Evidence 15
4.3. (U) Digital Evidence Processing 20
4.3.1. (U) Imaging 20
4.3.2. (U) [redacted] 20
4.3.3. (U) [redacted] 20
4.3.4. (U) Performing Content Reviews 21

20-cv-9284(FBI)-3

4.3.5. (U) Documenting Review of DE 23
4.3.6. (U) Copies 28
4.3.7. (U) Approved Tools 34
4.3.8. (U) [redacted] ..... 35 b7E -3, 4, 5
4.3.9. (U) [redacted] 35
4.3.10. (U) Reexaminations 37
4.3.11. (U) Advanced Technical Analysis 39
4.3.12. (U) Assigning Requests to Examiners and Digital Evidence Backlog Definition 40
4.4. (U) Testifying Regarding Digital Evidence Processing 40
4.4.1. (U) Computer Analysis and Response Team Forensic Examiners; Forensic Audio, Video and Image Analysis Unit Examiners; Computer Scientists-Field Office; and Operational Technology Division, Digital Forensics and Analysis Section Technical Experts 40
4.4.2. (U) Digital Extraction Technicians and Computer Analysis and Response Team Technicians 41
4.5. (U) Seeking Legal Advice 41
5. (U) Summary of Legal Authorities 42
6. (U) Recordkeeping Requirements 43
6.1. (U//~~FOUO~~) FBI Central Recordkeeping System 43
6.2. (U) Additional Information on Recordkeeping and Forms Use 43

(U) List of Appendices

Appendix A: (U) Final Approvals A-1
Appendix B: (U) Sources of Additional Information B-1
Appendix C: (U) Contact Information C-1
Appendix D: (U) Definitions and Acronyms D-1
Appendix E: (U//~~FOUO~~) Examination of FBI Evidence [redacted] ..... E-1 b7E -3, 4 , 5

20-cv-9284(FBI)-4

(U) Table of Figures

Figure 1. (U//~~FOUO~~) [redacted] ..... b7E -3, 4 , 5
Figure 2. (U//~~FOUO~~) Digital Evidence Copies 28
Figure 3. (U//~~FOUO~~) [redacted] D-1

(U) List of Tables

Table 1. (U) Roles and Responsibilities 8

20-cv-9284(FBI)-5

1. (U) Introduction

1.1. (U) Purpose

(U//~~FOUO~~) This policy guide (PG) establishes and consolidates the policies 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 stored or transmitted in binary form and is obtained with the intent to assist in proving or disproving a matter at issue in a case or an investigation. 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 (CD)/digital video discs (DVD), flash drives, random-access memory (RAM), magneto optical cartridges, Universal Serial Bus (USB) microstorage devices (commonly known as "thumb drives"), digital video recorders (DVR), 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 for establishing DE policies.

(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] b7E -3, 4, 5
- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) Information originally obtained in a nondigital 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 (deoxyribonucleic acid] profile databases).
- (U//~~FOUO~~) Business, transactional, or other records obtained through a subpoena [redacted] b7E -3, 4, 5 and 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 those 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 laws [redacted] b7E -3, 4, 5 DE is ever-present in FBI investigations and operations. All personnel who encounter DE must understand how to properly handle, review, and process it to avoid damaging the integrity of the evidence or violating the constitutional rights of a person during the course of an investigation.

(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

20-cv-9284(FBI)-6

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 purposes of authentication and presentation in court, as well as for investigative [redacted] b7E -3, 4, 5

1.3. (U) Scope

(U//~~FOUO//LES~~) This PG addresses handling, processing, and performing content reviews 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, performing a content review, search, extraction, report preparation, and advanced technical analysis [redacted] b7E -3, 4, 5

[redacted] Performing a content review involves the viewing of the [redacted] DE 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 for [redacted] of DE with their chief division counsels (CDC) or associate division counsels (ADC) or with the Office of the General Counsel (OGC), [redacted]

1.4.1. (U) [redacted]

[redacted] b3 -1

(U//~~FOUO~~) [redacted] b7E -2, 3, 4, 5, 6

[redacted]

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

[redacted]

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

[redacted]

20-cv-9284(FBI)-7

1.4.2. (U) Reviews or Examinations of Digital Evidence in

(U//~~FOUO~~) The following subsections discuss some of the unique areas of concern raised when the FBI or

b3 -1
b7E -2, 3, 4, 5

1.4.2.1. (U)

(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 must 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 CDCs/ADCs and OGC.

b3 -1
b7E -2, 3, 4, 5, 6

(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 CDCs/ADCs, OGC and must notify the AUSA to obtain additional legal authority

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

(U//~~FOUO~~) In FBI personnel may

b3 -1
b7E -2, 3, 4, 5, 6

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

(U//~~FOUO~~) Before uploading DE seized

20-cv-9284(FBI)-8

1.4.2.2. (U)

(U//~~FOUO~~) Often during reviews or examinations of DE (when providing technical assistance to the FB may be employed in accordance with the provisions of this PG. DOJ policy requires the approval of the deputy Attorney General (DAG) in the furtherance of a criminal case. See for more information.

b3 -1
b7E -2, 3, 4, 5

1.4.2.2.1. (U//~~LES~~

b3 -1
b7E -2, 3, 4, 5

(U//~~LES~~) During the course of

(U//~~LES~~)

b3 -1
b7E -2, 3, 4, 5, 6

(U//~~FOUO~~) When this circumstance applies, the case agent is responsible for notifying and coordinating with his or her CDC/ADC and OGC To ensure that appropriate disclosures are made, case agents must coordinate with the appropriate assistant United States attorney (AUSA) or DOJ trial attorney.

1.5. (U) Intended Audience

(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 (RCFL), and joint task forces (JTF) that encounter, handle, review, or process DE.

20-cv-9284(FBI)-9

2. (U) Roles and Responsibilities

2.1. (U) Digital Evidence Roles

(U//~~FOUO~~) The FBI's Digital Evidence 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 below in Figure 1 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.

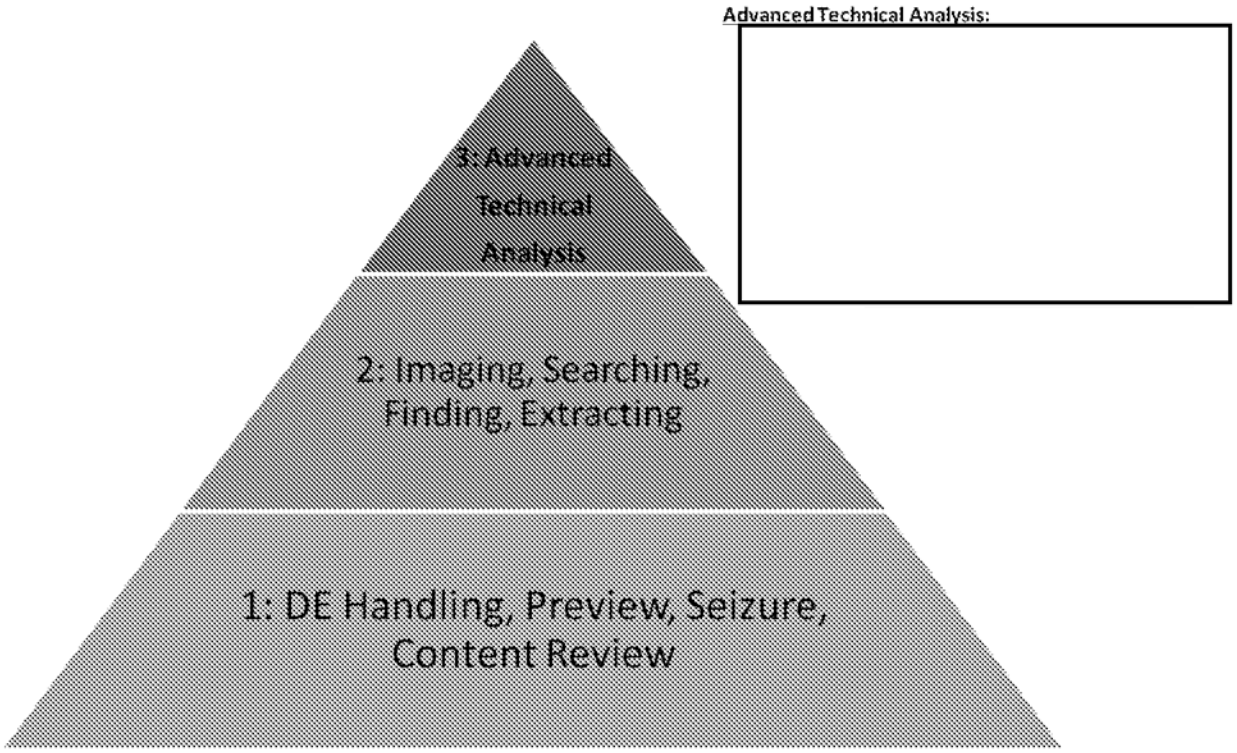


Figure 1. (U//~~FOUO~~) Functional Pyramid

(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.

(U//~~FOUO~~) 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 performed by investigative personnel an investigative, as opposed to a forensic, process; however, imaging and extraction remain forensic processes that require training to forensic standards.

(U//~~FOUO~~) 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.

20-cv-9284(FBI)-10

(U//~~FOUO~~) As used throughout this PG, references to training and certification refer to training and certification provided, approved, or recognized by OTD/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 (ECT), special agents (SA) and other professional staff personnel who have the proper training and approved tools under procedures approved by OTD/DFAS. b7E -3, 4, 5

(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 (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 (SFE) processes on copies of DE.
- (U//~~FOUO~~) Field Audio Video Program (FAVP) forensic analysts (FA): 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 (FE): FBIHQ 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 trainees (OJT): personnel identified by field office management to participate in training with a commitment toward becoming certified CART FEs.
  - (U//~~FOUO~~) CART forensic examiner trainees (FET): personnel assigned to work 100 percent 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 percent of their time to CART FE work.
- (U//~~FOUO~~) 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 agencies, and who continue a relationship with the RCFL to maintain certification and training. When serving in this role at the RCFL, RCFL

20-cv-9284(FBI)-11

associate examiners must continue to be impartial forensic scientists and are prohibited from conducting investigative activities.

- (U//~~FOUO~~) Computer scientist-field operations (CS-FO): CS-FOs are experienced computer scientists who work as integral members of investigative teams supporting FBI investigations and operations. The CS-FO is responsible for providing advanced technical analysis, [redacted] b7E -3, 4, 5 The CS-FO is not authorized to participate in the collection of data intercept, but may 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 -3, 4, 5

(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
• DE Handling • Preview • Seizure • Perform Content Reviews	✓	✓	✓	✓
• Imaging		✓	✓	✓
• Search/Find/Extract			✓	✓

20-cv-9284(FBI)-12

Functions	Investigative Personnel	CART Tech	DExT	Field CART FEs, CS-FOs, DFAS
• Advanced Technical Analysis • Role-Specific Standard Operating Procedures (SOPs)				✓

Table 1. (U) Roles and Responsibilities

2.2. (U) Digital Evidence Responsibilities

2.2.1. (U) FBI Personnel Who Handle, Process, or Perform Content Reviews of Digital Evidence

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

- (U//~~FOUO~~) Understanding and complying with the legal authority as it relates to the DE that has been processed, handled, or has had a content review performed.
- (U//~~FOUO~~) Handling, processing, and performing content reviews on DE and documenting those actions in accordance with this PG, other applicable OTD/DFAS policies and procedures, and applicable QA standards.
- (U//~~FOUO~~) Ensuring that all DE is handled, marked, and has a content review performed in accordance with the [redacted] b3 -1 b7E -2, 3, 4, 5
- (U//~~FOUO~~) Ensuring that all DE is handled, stored, marked, and has a content review performed, in accordance with FBI dissemination marking policies and OTD/DFAS policies.
- (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.

2.2.1.1. (U) Investigative Personnel and Analysts

(U//~~FOUO~~) Investigative personnel handling, processing, and performing content reviews of DE (typically special agents [SA] 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.

20-cv-9284(FBI)-13

2.2.1.2. (U) Computer Analysis and Response Team Technicians

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

2.2.1.3. (U) Digital Extraction Technicians

(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~~) Performing the DE functions authorized for CART techs as described above, if certified, and upon request. When performing these functions, the DExT must follow the protocols and limitations prescribed for that role.

2.2.1.4. (U) Computer Analysis and Response Team Forensic Examiners

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

- (U//~~FOUO~~) Performing any DE functions authorized for a CART tech or a DExT, upon request. 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:
  - o (U//~~FOUO~~) [redacted]
  - o (U//~~FOUO~~) [redacted]
  - o (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) [redacted] b7E -3, 4, 5
- (U//~~FOUO~~) [redacted] in accordance with all provisions of this PG and relevant OTD/DFAS QA requirements.
- (U//~~FOUO~~) Providing [redacted] the execution of search warrants and previews/examinations of complex computer systems or situations.
- (U//~~FOUO~~) Providing on-scene consultations with investigators and prosecutors in the development of strategies for the seizure or on-scene imaging of digital media and equipment.

2.2.1.5. (U//~~FOUO~~) Field Audio Video Program Forensic Analysts

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

- (U//~~FOUO~~) Conducting and/or directing the content review of audio and video DE.
- (U//~~FOUO~~) [redacted] b7E -3, 4, 5
- (U//~~FOUO~~) [redacted]

20-cv-9284(FBI)-14

- (U//~~FOUO~~) b7E -3, 4, 5
- (U//~~FOUO~~)

2.2.1.6. (U//~~FOUO~~) Computer Scientists-Field Operations

(U) CS-FOs are responsible for:

- (U//~~FOUO~~) Performing any function related to DE that is carried out by a CART tech or DExT. When performing those functions, CS-FOs must follow the protocols and limitations prescribed for those roles.
- (U//~~FOUO~~) Supporting investigative and personnel with computer science expertise in support of cases or investigations (e.g., assistance with interviews and searches), as authorized by this PG. b7E -3, 4, 5
- (U//~~FOUO~~) Using for all activities.

2.2.1.7. (U) Regional Computer Forensics Laboratories Personnel

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

2.2.2. (U) Federal Bureau of Investigation Headquarters

2.2.2.1. (U) Federal Bureau of Investigation Headquarters 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 areas by posting a link to this PG on their respective division Intranet sites.
- (U//~~FOUO~~) Ensuring compliance with all matters identified in this PG.
- (U//~~FOUO~~) Monitoring compliance and reporting noncompliance in their respective mission areas in accordance with the guidance found in the *Domestic Investigations and Operations Guide* (DIOG).

2.2.2.1.1. (U) FBIHQ Operational Divisions Routinely Handling Digital Evidence

2.2.2.1.1.1. (U//~~FOUO~~)

(U//~~FOUO~~) DExT personnel who are responsible for: b7E -3, 4, 5, 6

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

20-cv-9284(FBI)-15

- (U//~~FOUO~~) Following FBI DE protocols applicable to DExTs, as specified in this PG.
- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) Providing copies of seized or otherwise legally obtained DE for upload into the [redacted] at the request of the case agent or FBIHQ program management unit and with the approval of OGC/[redacted] b3 -1 b7E -2, 3, 4, 5, 6
- (U//~~FOUO~~) Providing copies of DE to IC partners, at the request of the case agent or FBIHQ program management unit and with the approval of [redacted]
- (U//~~FOUO~~) [redacted]

2.2.2.1.1.2. (U//~~FOUO~~) Criminal Investigative Division (CID), Violent Crimes Against Children (VCAC) Section

(U//~~FOUO~~) CID's VCAC Section provides [redacted] b7E -3, 4, 5 abuse and exploitation of children that may be investigated under the jurisdiction and authority of the FBI. The OTD/DFAS/Digital Analysis and Research Center (DARC) [redacted]

(U//~~FOUO~~) VCAC manages several programs, including the Innocent Images National Initiative (IINI) and is responsible for establishing guidance for the handling of child pornography contraband for the IINI program.

2.2.2.1.1.3. (U//~~FOUO~~) Operations Technology Division Digital Forensics and Analysis Section

(U//~~FOUO~~) OTD's DFAS, in coordination with other FBI divisions, is responsible for:

- (U//~~FOUO~~) Creating and maintaining policies and procedures for the FBI's DE program, wherein such policies and procedures ensure compliance with governing legal authorities, regarding 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~~) The Computer Analysis Response Team Forensic Examiner Subprogram.
  - (U//~~FOUO~~) The Digital Extraction Technician Subprogram.
  - (U//~~FOUO~~) The Computer Scientist-Field Operations Subprogram.
  - (U//~~FOUO~~) The Field Audio Video Program Subprogram.
  - (U//~~FOUO~~) The FBI Digital Evidence Laboratory (DEL) and Quality Assurance Program for DE.

20-cv-9284(FBI)-16

- o (U//~~FOUO~~) The RCFL Subprogram.

- (U//~~FOUO~~) Providing the following capabilities and resources:
  - o (U//~~FOUO~~) Trained examiners who provide DE acquisition, preservation, processing, review, examination, presentation, and testimony.
  - o (U//~~FOUO~~) Trained personnel who provide advanced analysis capabilities for DE, including:
    - (U//~~FOUO~~)
    - (U//~~FOUO~~)
    - (U//~~FOUO~~)
    - (U//~~FOUO~~)
    - (U//~~FOUO~~)
    - (U//~~FOUO~~)

    b7E -3, 4, 5
  - o (U//~~FOUO~~) Training, certification, and proficiency testing for personnel who process DE.
  - o (U//~~FOUO~~)
  - o (U//~~FOUO~~)

    b7E -3, 4, 5
  - o (U//~~FOUO~~)
  - o (U//~~FOUO~~) DE Help Desk

2.2.2.2. (U//~~FOUO~~) Office of the General Counsel

(U//~~FOUO~~) An associate general counsel (AGC) from the Science and Technology Law Section (STLS) or an OGC supervisory attorney must, upon request, provide:

- Legal guidance to FBIHQ personnel on the handling, processing, and performing of content reviews of DE, in accordance with this PG.
- Legal policy guidance regarding the interpretation or application of this PG to FBIHQ, field office, and RCFL personnel.
  - o Some RCFLs have

    b7E -3, 4, 5

2.2.3. (U) FBI Field Offices

2.2.3.1. (U) FBI Field Office Management

(U//~~FOUO~~) FBI field office management (i.e., assistant directors in charge [ADIC], special agents in charge [SAC], assistant special agents in charge [ASAC], and supervisory special agents [SSA]) are responsible for:

20-cv-9284(FBI)-17

- (U//~~FOUO~~) Promoting and communicating DE polices.
- (U//~~FOUO~~) Ensuring compliance with this PG.
- (U//~~FOUO~~) Monitoring compliance and reporting noncompliance in their respective mission areas, in accordance with the DIOG.

2.2.3.2. (U//~~FOUO~~) Evidence Control Technicians (ECT)

(U//~~FOUO~~) Regarding DE, ECTs are responsible for:

- (U//~~FOUO~~) Properly storing, protecting, and tracking DE, as described in subsection 4.2.4.5. of this PG.
- (U//~~FOUO~~) Properly packaging and shipping DE, as necessary, as described in subsections 4.2.4.6. and 4.2.4.6.1. of this PG.

2.2.3.3. (U) Chief Division Counsels

CDCs must, upon request, provide legal guidance regarding the handling, processing, and the performing of content reviews of DE, in accordance with this PG. CDCs' responsibilities with regard to evidence may be delegated to an ADC or an LA.

20-cv-9284(FBI)-18

3. (U) Policies

(U//~~FOUO~~) This PG establishes and consolidates the policies and procedures for the proper handling, reviewing, and processing of DE for the FBI, whether it is seized, received, or otherwise legally obtained. DE is data that is stored or transmitted in binary form and is obtained with the intent to assist in proving or disproving a matter at issue in a case or an investigation. 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, CDs/DVDs, flash drives, RAM, magneto optical cartridges, USB micro storage devices (commonly known as "thumb drives"), DVRs, or other electronic devices that store or process data digitally. The OTD DFAS is responsible for the FBI's Digital Evidence Program and establishing DE policies.

20-cv-9284(FBI)-19

4. (U) Procedures and Processes

4.1. (U//~~FOUO~~) Forensic Program Compliance Within the FBI

(U//~~FOUO~~) All DE forensic programs and subprograms 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 assistant director (AD), OTD or his or her designee is obtained.

4.2. (U) Digital Evidence Handling

(U//~~FOUO~~) This section sets forth policies and procedures 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.

4.2.1. (U) Personnel Authorized to Handle Digital Evidence

(U//~~FOUO~~) Level one and above personnel (as defined in Figure 1) are authorized to seize, image, and transport DE, provided that they act within the scope of their training and certifications. FBI personnel must also be trained and/or certified in accordance with OTD/DFAS policies and procedures and follow all applicable protocols before processing DE, including making copies or images of DE.

4.2.2. (U) Presearch Considerations

4.2.2.1. (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 CDC or OGC legal review of DE-related search warrants and subpoenas, as applicable [redacted] b3 -1 b7E -2, 3, 4, 5, 6

Field office CDCs and OGC are also available to provide assistance in drafting search warrants or subpoenas for seizing or searching DE.

4.2.3. (U) Timeframe for Warrants Involving Digital Evidence

(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. Case agents should consult with their CDCs or OGC [redacted] b7E -3, 4, 5, 6 there are questions pertaining to time permitted for examination.

4.2.4. (U) Consent Searches for Digital Evidence

(U//~~FOUO~~) Whenever possible, written consent must be obtained from the consenting party and documented on an FD-26, "Consent to Search" or an FD-941, "Consent to Search Computer(s)." 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, "Form for Reporting Information That May Become the Subject of Testimony."

(U//~~FOUO~~) In consent cases, case agents should ensure that [redacted] b7E -3, 4, 5

20-cv-9284(FBI)-20

(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 the revocation.

4.2.4.1. (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 may be requested through, and in coordination with, the appropriate squad supervisor(s).

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

(U//~~FOUO~~) Case agents must submit requests for DE assistance to CART personnel via electronic communication (EC) or, where available, an automated request through the approved OTD/DFAS Intranet site or an RCFL service request form. All service requests must include:

- (U//~~FOUO~~) The universal case file number (UCFN) (case identification number [ID]).
- (U//~~FOUO~~) The case title.
- (U//~~FOUO~~) The specific request.
- (U//~~FOUO~~) The description of legal authority.

4.2.4.2. (U) Requests Involving Multiple Locations

(U//~~FOUO~~) Case agents must coordinate, in advance, any DE service requests involving multiple field offices with the CART supervisors or coordinators in their divisions, as well as with the other applicable divisions. If further assistance is required, CART supervisors or coordinators should work with the OTD/DFAS/Digital Evidence Field Operations Unit (DEFOU).

4.2.4.3. (U) Providing [redacted] Technical Assistance in Digital Evidence Cases

b7E -3, 4, 5

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

(U//~~FOUO~~) Pursuant to Title 28 Code of Federal Regulations (CFR) Section (§) 0.85(g) and the DIOG, the FBI 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 -3, 4, 5

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

20-cv-9284(FBI)-21

(U//~~FOUO~~) The following OTD/DFAS units are not components of the FBI DEL: (1) the [redacted] b7E -3, 4, 5, 6 [redacted] Field office CART assets and laboratories are not part of the FBI DEL. Although RCFLs follow the FBI DEL's Quality Assurance Program, each RCFL is an individually accredited lab, independent from other RCFLs 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.

4.2.4.3.1. (U) Expert Investigative Assistance in Digital Evidence Cases

(U//~~FOUO~~) FBI personnel, particularly approving officials, must be careful to review [redacted] b3 -1 b7E -2, 3, 4, 5 [redacted] see the DIOG.

(U//~~FOUO~~) During the course of providing either [redacted] b3 -1 b7E -2, 3, 4, 5, 6 [redacted]

4.2.4.3.2. (U) Requests for [redacted] the Digital Evidence Laboratory or Regional Computer Forensics Laboratories

(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 for [redacted] than the FBI DEL or RCFLs must be processed and handled in accordance with the DIOG and the [redacted], as applicable.

(U//~~FOUO~~) [redacted] b3 -1 b7E -2, 3, 4, 5 [redacted]

4.2.4.3.3. (U) [redacted]

20-cv-9284(FBI)-22

4.2.4.3.3.1. (U) Requests to the FBI Digital Evidence Laboratory

(U//~~FOUO~~) Requests submitted to the DEL for [redacted] b3 -1 b7E -2, 3, 4, 5

(U//~~FOUO~~) [redacted] b3 -1 b7E -2, 3, 4, 5

(U//~~FOUO~~) [redacted] b3 -1 b7E -2, 3, 4, 5

(U//~~FOUO~~) [redacted] b3 -1 b7E -2, 3, 4, 5

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

(U//~~FOUO~~) [redacted] b3 -1 b7E -2, 3, 4, 5

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

4.2.4.3.3.2. (U) Requests for Regional Computer Forensic Laboratory Support

(U//~~FOUO~~) Requests for RCFL DE support from [redacted] will be handled in accordance with the applicable MOU governing the RCFL concerned, provided that the MOU is consistent with this PG. b7E -3, 4, 5

(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. b3 -1 b7E -2, 3, 4, 5

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

20-cv-9284(FBI)-23

[redacted] b3 -1 b7E -2, 3, 4, 5

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

(U//~~FOUO~~) RCFLs will track all service requests and disseminate information to [redacted] b3 -1 b7E -2, 3, 4, 5

4.2.4.3.4. (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 b3 -1 b7E -2, 3, 4, 5, 6 approval by the DAG. See the DAG memorandum entitled "[redacted]"

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

(U//~~FOUO~~) The dissemination of protected information must be in accordance with the DIOG.

(U//~~FOUO~~) Prior to the approval of a request, assurances must be obtained from the requesting agency and the chief prosecutor for the applicable jurisdiction that representatives of the requesting agency will not disclose [redacted] in court, through pretrial motions, b7E -3, 4, 5 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 or her designee. The requesting agency and the chief prosecutorial official will also acknowledge that 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 policies on the protection, use, and [redacted]

4.2.4.4. (U) Digital Evidence and Evidence Control Facilities (ECF)

(U//~~FOUO~~) The original DE seized at a search site must be transported securely to the FBI field office or RCFL site and, after processing and examination, be placed, as appropriate, in an FBI or RCFL ECF.

4.2.4.5. (U) Digital Evidence Storage

(U//~~FOUO~~) DE must be stored and secured and/or sealed to prevent data or evidentiary loss, cross-transfer contamination, or other deleterious changes.

20-cv-9284(FBI)-24

4.2.4.6. (U) Shipping Digital Evidence

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

4.2.4.6.1. (U) Shipping Digital Evidence to the Computer Analysis and Response Team

(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. The DE must be accompanied by an EC explaining the shipment.

4.2.4.7. (U) Transferring a Working Copy of FBI Digital Evidence to [redacted] b7E -3, 4, 5, 6

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

4.3. (U) Digital Evidence Processing

4.3.1. (U) Imaging

(U//~~FOUO~~) Imaging is the act of making a [redacted] copy of the original DE to serve as an accurate reproduction of the original DE. Only certified DE personnel must perform imaging. 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 [redacted] b7E -3, 4, 5

4.3.2. (U) [redacted] b7E -3, 4, 5

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

4.3.3. (U) [redacted] b7E -3, 4, 5, 6

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

20-cv-9284(FBI)-25

[redacted] b7E -3, 4, 5, 6

4.3.3.1. (U) [redacted]

(U//~~FOUO~~) [redacted] b7E -3, 4, 5, 6

4.3.4. (U) Performing Content Reviews

(U//~~FOUO~~) Investigative personnel can review DE for content after the DE has been processed by an authorized method. This review may be conducted using such methods as [redacted] b7E -3, 4, 5

4.3.4.1. (U) Scope and the Performing 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]

(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] b3 -1 b7E -2, 3, 4, 5 the 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).

4.3.4.2. (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 or specific files or folders on a computer), either orally or on the written consent form.

---

[1] (U//~~FOUO~~) [redacted] b7E -3, 4, 5

20-cv-9284(FBI)-26

4.3.4.3. (U//~~FOUO~~) Search Protocols for Digital Evidence

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

4.3.4.4. (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 (RA). Investigative personnel must use the kiosks, when reasonably available, to automatically process supported DE types, unless otherwise directed by CART personnel.

(U//~~FOUO~~) [redacted] b7E -3, 4, 5
[redacted] self-paced or hands-on training is required.

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

4.3.4.5. (U) Authorization for Performing Content Reviews

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

- (U//~~FOUO~~) [redacted] approved by OTD/DFAS are utilized
- (U//~~FOUO~~) Preview [redacted] OTD/DFAS policies
- (U//~~FOUO~~) Preview by RCFLs or CART field office facilities, in accordance with OTD/DFAS policies b7E -3, 4, 5
- (U//~~FOUO~~) The use of self-service kiosks for [redacted]

(U//~~FOUO~~) Performing content reviews of original DE is prohibited by those not trained and authorized by OTD

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

(U//~~FOUO~~) [redacted] within the scope of the legal authority. The information obtained through [redacted] b7E -3, 4, 5

4.3.4.7. (U) [redacted] b7E -3, 4, 5

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

[redacted] b7E -3, 4, 5

4.3.4.8. (U) Content Review Tools

(U//~~FOUO~~) All DE content review tools used by personnel working for or with the FBI or RCFL 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.

4.3.5. (U) Documenting Review of DE

(U//~~FOUO~~) FBI personnel must document 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 or is identified as [redacted] The documentation must be serialized to the investigative case file. Such documentation must 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. b3 -1 b7E -2, 3, 4, 5

(U//~~FOUO~~) Undocumented, "off-the-record" searches or reviews of DE are not permitted. The above documentation requirement does not apply to searches of [redacted] (see subsection 4.3.5.6. of this PG for a definition of a [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 resulting from the [redacted] b7E -3, 4, 5
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] b3 -1 b7E -2, 3, 4, 5

4.3.5.1. (U) Content Review Report

(U//~~FOUO~~) A content review report is a factual report of investigative findings resulting from the review of original, master, or [redacted] of the DE. Because [redacted] b7E -3, 4, 5

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, "Form for Reporting Information That May Become the Subject of Testimony." 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.

20-cv-9284(FBI)-28

- (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 that the [redacted] b7E -3, 4, 5
- (U//~~FOUO~~) Report of the responsive content found, including [redacted] b7E -3, 4, 5

(U//~~FOUO~~) All FBI personnel must fully and officially document in the content review report any other individuals who provided substantive assistance (as opposed to purely technical assistance, [redacted] b7E -3, 4, 5

(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 subsection 2.1., Figure 1).

4.3.5.2. (U) Digital Extraction Technician Report

(U//~~FOUO~~) A DExT report is a factual report of [redacted] details who performed the work, when it was performed, what was reviewed and found, and where it was found. DExT work may be documented by completing an FD-302, "Form for Reporting Information That May Become the Subject of Testimony," in accordance with the [redacted] prescribed by OTD/DFAS. DExT reports must be serialized into the investigative case file and must contain a minimum of the following information or provide a reference to where the information may be found: b7E -3, 4, 5

- (U//~~FOUO~~) Name and contact information of the DExT.
- (U//~~FOUO~~) Case identification.
- (U//~~FOUO~~) Name of requestor and specifically what was requested.
- (U//~~FOUO~~) Description of the working copy processed, including case number and original DE description.

20-cv-9284(FBI)-29

- (U//~~FOUO~~) Physical location of where the review was completed (i.e., location/address of the reviewer).
- (U//~~FOUO~~) Date of the report.
- (U//~~FOUO~~) List of procedures performed.
- (U//~~FOUO~~) What was searched for and what items of investigative importance were found (including negative search results, when applicable).
- (U//~~FOUO~~) Where the DExT is a case agent or investigator and is reviewing or conducting an [redacted] on his or her own case evidence, the methodology and basis for his or her conclusion that the [redacted] b7E -3, 4, 5
- (U//~~FOUO~~) Report of the responsive content found, including [redacted]
- (U//~~FOUO~~) [redacted] b7E -3, 4, 5
- (U//~~FOUO~~) [redacted] b7E -3, 4, 5
- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) What was targeted during the search and, if applicable, the order in which items were targeted [redacted] b7E -3, 4, 5

(U//~~FOUO~~) All DExTs must fully and officially document in the DExT report any other individuals who provided substantive assistance with the [redacted] b7E -3, 4, 5

(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 subsection 2.1, Figure 1).

(U//~~FOUO~~) If the DExT is an FBI investigative asset (e.g., an SA or an intelligence analyst [IA]) and is performing a content review and DExT review simultaneously in his or her own case, only a DExT report is required.

20-cv-9284(FBI)-30

4.3.5.3. (U) Report of Examination

(U//~~FOUO~~) A report of examination is used to document the results of [redacted] and 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 a [redacted] may use other reporting formats approved by OTD/DFAS. Reports of examination must be serialized into the investigative case file and must contain a minimum of the following information or provide a reference to where the information may be found. If relying on the reference provision, all references must accompany the report of examination provided to the defendant during discovery. b7E -3, 4, 5

- (U//~~FOUO~~) Name and contact information of the examiner
- (U//~~FOUO~~) Case identification
- (U//~~FOUO~~) Name of requestor and specifically what was requested
- (U//~~FOUO~~) Description of the working copy processed, including case number and original DE description
- (U//~~FOUO~~) Physical location of where the review was completed (i.e., location/address of the reviewer)
- (U//~~FOUO~~) Date of the report
- (U//~~FOUO~~) Procedures performed, which may include the following:
  - o [redacted]
  - o Types of files targeted ([redacted]) b7E -3, 4, 5
  - o The order in which items were searched (if applicable)
- (U//~~FOUO~~) Items searched for and items found of investigative importance, including negative search results, when applicable
- (U//~~FOUO~~) Report of the content found, [redacted] b7E -3, 4, 5
- (U//~~FOUO~~) [redacted]

(U//~~FOUO~~) All FBI personnel must also fully and officially document in the report of examination whenever they received substantive assistance from another individual during the examination or review process (not including help-desk-type assistance), including [redacted] b7E -3, 4, 5

20-cv-9284(FBI)-31

[redacted] b7E -3, 4, 5

(U//~~FOUO~~) Frequently, in the course of the investigation or during trial preparation, an examiner will be 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 document fully the additional analysis requested, in accordance with the Federal Rules of Criminal Procedure Rule 16.

4.3.5.4. (U) [redacted] Reports b7E 3, 4, 5, 6

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

[redacted] Intelligence 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 he or she requested
- (U//~~FOUO~~) Description of the working copy processed, including case number and original DE description
- (U//~~FOUO~~) Physical location of where the review was completed (i.e., location of the reviewer)
- (U//~~FOUO~~) Date of the report
- (U//~~FOUO~~) List of procedures performed
- (U//~~FOUO~~) What was searched for and what items of investigative importance were found
- (U//~~FOUO~~) Report of the responsive content found, including identifying the [redacted] b7E -3, 4, 5
- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) What was targeted during the search and, if applicable, the order in which items were targeted [redacted]

(U//~~FOUO~~) [redacted]
report, any other individuals who provided substantive assistance with the [redacted] (not including help desk-type assistance) [redacted] Th b7E -3, 4, 5, 6
must, at a minimum, include who assisted them during the processing and, if applicable, who
[redacted]

20-cv-9284(FBI)-32

(U//~~FOUO~~) [redacted] 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 subsection 2.1, Figure 1). b7E -3, 4, 5

4.3.5.5. (U) Testifying Regarding Review of Digital Evidence

(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 must be as detailed and extensive as necessary to recall all key aspects of their activities.

4.3.5.6. (U) Retaining Results of Review

(U//~~FOUO~~) After the DE is reviewed and/or examined, the set of data that (1) is determined to be within the scope of the legal authority, (2) is relevant, and (3) is probative or exculpatory must be [redacted] b7E -3, 4, 5

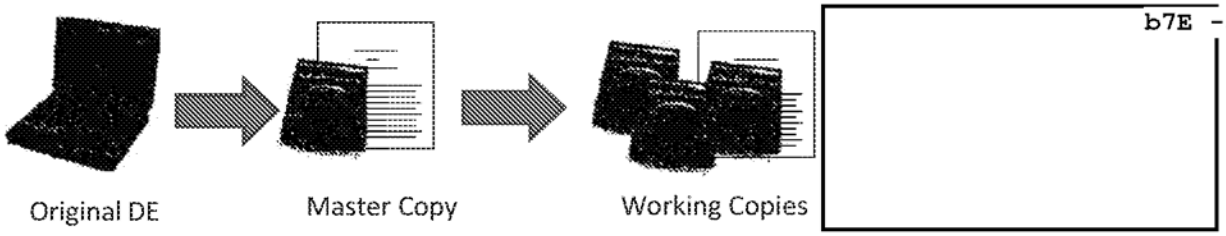
(U//~~FOUO~~) The results of a content review or an examination must be [redacted]

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

4.3.6. (U) Copies

4.3.6.1. (U) Original Digital Evidence vs. Master Copy vs. Working Copy vs. [redacted] b7E -3, 4, 5

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



b7E -3, 4, 5

Figure 2. (U//~~FOUO~~) Digital Evidence Copies

(U//~~FOUO~~) Original DE: DE seized at a search scene or otherwise lawfully 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

CDCs/ADCs and OGC [redacted] to ensure that the proper stipulations are entered into to prevent challenges to authenticity after return of the media. b7E -3, 4, 5, 6

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

(U//~~FOUO~~) Master copy: the one required copy of DE that is stored on media to be retained and logged on an FD-1004, "Federal Bureau of Investigation Evidence Chain of Custody" form. [redacted] b7E -3, 4, 5

[redacted]

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

[redacted]

(U//~~FOUO~~) Working copies [redacted] b7E -3, 4, 5

[redacted]

(U//~~FOUO~~) Restrictions on the tracking, dissemination, and copying of [redacted] b7E -3, 4, 5

[redacted]

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

[redacted] b7E -3, 4, 5

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

[redacted]

(U//~~FOUO~~) It is impossible to guarantee that [redacted] b7E -3, 4, 5

[redacted]

20-cv-9284(FBI)-34

[redacted] b7E -3, 4, 5

4.3.6.2. (U) Controlling Master Copies

(U//~~FOUO~~) All master copies must be saved [redacted] The original legal authority must be reviewed prior to making any copies [redacted] b3 -1 b7E -2, 3, 4, 5

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

1. (U//~~FOUO~~) [redacted] b7E -3, 4, 5
2. (U//~~FOUO~~) [redacted]

(U//~~FOUO~~) DE that is received in an ECF and is 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).

4.3.6.3. (U) Protecting Original Evidence or Master Copies

(U//~~FOUO~~) Unless it is not technically possible, examinations or reviews of DE [redacted] b7E -3, 4, 5

4.3.6.4. (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, 4, 5

4.3.6.5. (U) Disseminating [redacted]

(U//~~FOUO~~) [redacted] b7E -3, 4, 5

[redacted] b7E -3, 4, 5

(U//~~FOUO~~) All FBI personnel receiving requests for [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 provide a [redacted] of that legal authority is included in the investigative case file and if the provision of [redacted] is documented as outlined in this section.

(U//~~FOUO~~) [redacted] FBI personnel may b3 -1
disseminate, with OGC's approval, [redacted] b7E -2, 3, 4, 5
[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 create media of working copies. All copies made after (or from) the master copy, [redacted] are required to be labeled as working copies, except as noted.

b7E -3, 4, 5

(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 his or her name, the number of working copies provided, the recipient [redacted] the UCFN or file number, the evidence number, who requested the working copy on what date and at what time, and the purpose for the working copy.

(U//~~FOUO~~) At the discretion of the case agent or the 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 to [redacted] b7E -3, 4, 5

(U//~~FOUO~~) Because DE may contain contraband, personally identifiable information (PII), privileged files or other legally protected information, [redacted] b7E -3, 4, 5
[redacted] must be appropriately marked [redacted]

4.3.6.5.1. (U) Copies of Digital Evidence for the United States Attorney's Office

(U//~~FOUO~~) Only [redacted] of DE may be provided to USAOs, unless otherwise b7E -3, 4, 5
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 a 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 must be handled as [redacted] request or reexamination request (as

20-cv-9284(FBI)-36

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 would occur under the relevant circumstances in the underlying application for the legal authority.
- (U//~~FOUO~~) The affiant advised the court that such a 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] b7E -3, 4, 5, 6 determines that such a dissemination is otherwise authorized.

(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 the purposes of this section, "government personnel" does not include AUSAs, paralegals, or other personnel in a USAO, nor does it include trial attorneys, paralegals, or other personnel in DOJ who 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 -3, 4, 5

[redacted]

(U//~~FOUO~~) If FBI personnel are requested to provide such copies or otherwise facilitate such a transfer, they should inform the UC of the Forensic Support Unit, their squad supervisors, and their CDCs. 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 must also comply with any other relevant policies or procedures, such as the need to obtain the approval of the AD of OTD for a second examination of digital evidence.

4.3.6.5.2. (U) Discovery Requests

(U//~~FOUO~~) Discovery requests must be accommodated following applicable laws.

(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 (e.g., 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.

4.3.6.5.2.1. (U) Providing Digital Evidence with No Contraband

20-cv-9284(FBI)-37

(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 -3, 4, 5 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 that results and the inability [redacted]

4.3.6.5.2.2. (U) Requests for Digital Evidence Containing Contraband

(U//~~FOUO~~) When discovery is requested of material containing contraband (e.g., child pornography), the FBI must follow the procedures outlined in Title18 United States Code (U.S.C.) Section (§) 3509(m), the Adam Walsh Child Protection and Safety Act (the Act). Pursuant to the Act, the FBI is required to make reasonable accommodations, frequently called Adam Walsh rooms, specifically configured for these types of reviews, for the defense to have access to such material in an FBI facility. Reasonable accommodations include access to the government-controlled facility during normal business hours, access to telephones, access to the Internet, and access to printers. Defense experts may make special, advance arrangements to use the facility outside of 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 workforce expenses 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 their 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 exposed accidentally 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 have been included. If the defense expert objects to this review, CART personnel must notify their supervisor(s) and CDCs/ADCs or OGC [redacted] for input and assistance in resolving the issue. If those parties ar b7E -3, 4, 5, 6 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 he or she has taken no materials that are considered

contraband under federal law away from the government-controlled facility upon completion of the defense examination, and that he or she has not caused any contraband to be sent off site.

(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.

4.3.6.5.2.3. (U) Special Guidelines for Regional Computer Forensic Laboratories 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 revictimized. However, with respect to purely state or local cases, RCFLs are obligated to follow state or local court orders governing discovery.

4.3.6.6. (U) [redacted]

4.3.6.6.1. (U) Disseminating [redacted]

(U//~~FOUO~~) Case agents may, with the supervisor's approval, provide copies of the [redacted] to authorized law enforcement, prosecutors, and [redacted] in furtherance of a lawful purpose and consistent with the terms of the search warrant or other legal authority. b7E -3, 4, 5

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

(U//FOUO) Once the DE has been submitted to the ECF, the case agent may copy and disseminate copies of the [redacted] and associated reports. If the case agent makes copies of the [redacted] 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).

4.3.7. (U) Approved Tools

(U//~~FOUO~~) Approved tools must be used by all DE personnel during the [redacted] b7E 3, 4, 5

[redacted]

(U//~~FOUO~~) Approved tools for processing DE are listed on the [redacted] Use of many approved tools requires successful completion of OTD/DFAS-approved training. b7E -3, 4, 5

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

20-cv-9284(FBI)-39

[redacted] b7E -3, 4, 5

(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.

4.3.7.1. (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/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.

4.3.8. (U) [redacted]

(U//~~FOUO~~) Case agents should coordinate with OTD [redacted] Case agents should be aware b7E -3, 4, 5, 6
that the use of unapproved [redacted] is discouraged, [redacted]

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

4.3.9. (U) Requests for [redacted]

4.3.9.1. (U) Examinations of Digital Evidence in FBI Cases b7E -3, 4, 5

(U//~~FOUO~~) Except as authorized in this PG (see Appendix E, "Examination of FBI Evidence by [redacted]), all evidence generated by FBI criminal and [redacted] must be submitted for forensic examination or forensic analysis to an FBI laboratory or a forensic program authorized by the FBI Science and Technology Branch (STB). "Forensic examination(s)" or "forensic analysis[es]" is 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).
- (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~~) [redacted] b7E -3, 4, 5

20-cv-9284(FBI)-40

4.3.9.2. (U) Transfer of Evidence

4.3.9.2.1. (U//~~FOUO~~) [redacted] b7E -3, 4, 5

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

(U//~~FOUO~~) [redacted] b7E -3, 4, 5

4.3.9.3. (U) Chain of Custody

(U//~~FOUO~~) In criminal investigations, once FBI evidence has been [redacted] b7E -3, 4, 5 is responsible for maintaining any chain of custody on all original and derivative evidence [redacted] created through the examination process until the completion of all trials and appeals. FBI personnel may not retain duplicate evidence or samples of evidence [redacted] without the prior written concurrence of the AD, OTD.

4.3.9.4. (U) Noncircumvention of FBI Policies

(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 policies, including:

- (U) [redacted] b7E -3, 4, 5
- (U) [redacted]

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

(U//~~FOUO~~) FBI personnel and facilities [redacted] may not accept service requests to b7E -3, 4, 5, 6 provide DE services in administrative or civil matters. The AD, OTD may grant exceptions after consultation with OGC [redacted] In considering requests for exceptions, the AD, OTD must determine:

- (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 [redacted] b7E -3, 4, 5
- (U) The cost to the FBI in having to provide personnel to testify in a civil matter, as well as being deposed and completing other civil discovery.
- (U) Other relevant factors presented by particular situations.

20-cv-9284(FBI)-41

(U//~~FOUO~~) These limitations do not preclude providing DE support for FBI internal investigation matters or for RCFLs to provide DE support [redacted] b7E -3, 4, 5

(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.

4.3.10. (U) Reexaminations

4.3.10.1. (U) Definition of Examination

(U//~~FOUO~~) An examination is defined as a forensic process whereby a forensic examiner reviews digital evidence [redacted] b7E -3, 4, 5

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

4.3.10.2. (U) Overview of Reexaminations

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

(U//~~FOUO~~) A reexamination occurs when evidence already subjected to a technical examination [redacted] b7E -3, 4, 5

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

- (U//~~FOUO~~) Eliminate duplication of effort.
- (U//~~FOUO~~) Ensure that the integrity of the evidence is maintained.
- (U//~~FOUO~~) [redacted] b7E -3, 4, 5
  - o (U//~~FOUO~~) [redacted]
  - o (U//~~FOUO~~) [redacted]
  - o (U//~~FOUO~~) [redacted]

20-cv-9284(FBI)-42

4.3.10.3. (U) Requesting a Reexamination

(U//~~FOUO~~) Within the FBI, reexaminations may only be requested via an EC that has been approved by the head of the requesting field office. ECs must be addressed to the AD, OTD and routed through the UC, FSU and the appropriate CART FO program manager. [redacted] b7E -3, 4, 5

[redacted]

(U//~~FOUO~~) The request must include a letter from the USAO (or a letter from the district attorney if a state or a local case or a letter from the staff judge advocate [if applicable] in the case of a military investigation), containing:

- (U//~~FOUO~~) The extraordinary circumstances compelling the requested reexamination.
- (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 [redacted] b7E -3, 4, 5

[redacted]

4.3.10.4. Approval of Reexamination Requests

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

After a determination that the requested examination is or is not a reexamination, a recommendation for the AD of approval or denial will be prepared. OTD will consider the following factors:

- (U//~~FOUO~~) Scope of the requested reexamination
- (U//~~FOUO~~) Responsiveness of the prior examination to previous and current service requests or legal authorities
- (U//~~FOUO~~) Types 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 -3, 4, 5
- (U//~~FOUO~~) Nature of prior review or examination (including whether prior examination substantially followed or was analogous to FBI CART SOPs)

20-cv-9284(FBI)-43

- (U//~~FOUO~~) Whether documentation of prior examination or review provides sufficient detail (including whether there are indicia of a completed examination [redacted] b7E -3, 4, 5
[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 reexamination and, after coordination with OGC/[redacted] as needed, approve or deny the request. Notice of approval or denial of the b7E -3, 4, 5, 6
reexamination request will be transmitted via EC (to FBI field offices or FBIHQ divisions) [redacted]. If approved and if required by the circumstances, the approval document may also outline any conditions or limitations placed on the reexamination. The approval documentation must be maintained in the examination file.

(U//~~FOUO~~) Questions regarding whether a service request constitutes a reexamination 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 reexamination. b7E -3, 4, 5

4.3.11. (U) Advanced Technical Analysis

(U//~~FOUO~~) With respect to DE within their domains of expertise, advanced technical analysis of DE may only be performed by [redacted] b7E -3, 4, 5
[redacted]

4.3.11.1. (U) [redacted]

(U//~~FOUO~~) Requests for advanced analysis must be made via a service request. All service requests must be submitted via EC or, where available, an automated request through the approved OTD [redacted] using an open FBI case file or a request for assistance fro b7E -3, 4, 5, 6
an [redacted] to the field office or RCFL.

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

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

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

(U//FOUO) All requests for [redacted] must be submitted to OTD/FAVIAU via EC or other appropriate documentation identified by FAVIAU. b7E -3, 4, 5, 6

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

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

4.3.11.5. (U//~~FOUO//LES~~) [redacted] b7E -3, 4, 5, 6

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

4.3.12. (U) Assigning Requests to Examiners and Digital Evidence Backlog Definition

(U//~~FOUO~~) In order to more accurately assess a 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 those requests. 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 the investigation [redacted] b7E -3, 4, 5

(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 week of receipt, regardless of other proprietary software/databases used to manage service requests in individual field offices and RCFLs. Offices using the Digital Evidence Management System (DEMS) are exempt from this requirement.

4.4. (U) Testifying Regarding Digital Evidence Processing

4.4.1. (U) Computer Analysis and Response Team Forensic Examiners; Forensic Audio, Video and Image Analysis Unit Examiners; Computer Scientists-Field Office; and Operational Technology Division, Digital Forensics and Analysis Section Technical Experts

(U//~~FOUO~~) CART FEs, FAVIAU examiners, CS-FOs, and OTD/DFAS technical expert personnel, based upon their training and experience, are expected and authorized to provide expert opinion testimony within the scope of their duties, in accordance with DOJ and other applicable ethical requirements and as supported by their examinations and the scientific principles underlying their applicable disciplines.

4.4.2. (U) Digital Extraction Technicians and Computer Analysis and Response Team Technicians

(U//~~FOUO~~) Personnel processing or handling DE as DExTs or CART techs may only provide fact-based testimony consistent with their roles, as they are only trained to the technician level to operate specific categories of tools and conduct specific procedures in accordance with applicable SOPs. These individuals are not expected to possess the requisite breadth and depth of knowledge necessary to provide expert opinion testimony. Instead, DExTs and CART techs may only, if qualified, testify as expert factual witnesses. The scope of their testimony must remain confined to factual assertions concerning the operation of their tools or the application of their procedures (as opposed to, for example, providing opinions on computer forensics or computer operations in general).

4.5. (U) Seeking Legal Advice

(U//~~FOUO~~)

b7E -3, 4, 5

20-cv-9284(FBI)-46

5. (U) Summary of Legal Authorities

- (U) PD 0102D, Operational Technology Division Statement of Authorities and Responsibilities
- (U) 28 CFR § 0.85 (general functions of the FBI): provides that the FBI investigate violations of the law, collect evidence, operate the FBI laboratories, [redacted] (see specifically, 28 CFR § 0.85(a), (d), (g) and (l)). b7E -3, 4, 5

20-cv-9284(FBI)-47

6. (U) Recordkeeping Requirements

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

(U//~~FOUO~~) DE must not be uploaded into the FBI's central recordkeeping system or any other FBI administrative or records management system (e.g., FBINet). The FBI's central recordkeeping system (currently Sentinel) is the FBI's official recordkeeping system for all case file management. Nonrecord materials, per the legal definition of federal records, must not be placed in the recordkeeping system. Nonrecord materials include any copies preserved for convenience or reference. Although the FBI's central recordkeeping system has the ability to accept many documents and file types as either serials or attachments to both 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 DE (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. [redacted] b7E -3, 4, 5 [redacted] may 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 may contraband material be serialized into the FBI's central recordkeeping system.

[redacted]

6.2. (U) Additional Information on Recordkeeping and Forms Use

- (U) FOU Intranet site
- (U) DEL Quality Assurance Intranet site
- (U) DEL Training Intranet site [restricted access]
- (U) DIOG
- (U) [redacted] b7E -3, 4, 5

[redacted]

20-cv-9284(FBI)-48

Appendix A: (U) Final Approvals

POLICY TITLE: *Digital Evidence Policy Guide*	
Date of Last Renewal	N/A
Publish Date	2016-07-31
Effective Date	2016-07-31
Review Date	2019-07-31
APPROVALS	
Sponsoring Executive Approval	**Brian K. Brooks** Deputy Assistant Director Operational Technology Division
General Counsel Approval	**James A. Baker** General Counsel
Final Approval	**Amy S. Hess** Executive Assistant Director Science and Technology Branch

20-cv-9284(FBI)-49

Appendix B: (U) Sources of Additional Information

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

(U//~~FOUO~~) All of the below are to be marked (U//~~FOUO~~), [redacted] b7E -3, 4, 5, 6

[redacted] They are not to be identified to the public.

- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) [redacted] b7E -3, 4, 5, 6
- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) [redacted]

OTD Offices	OTD Phone Numbers, Intranet Sites, and Addresses
OTD Deputy Assistant Director Technical Analysis and Support Branch	[redacted] b7E -1
OTD Section Chief Digital Forensics and Analysis Section	
OTD Assistant Section Chief Digital Forensics and Analysis Section, Digital Evidence Lab Director	
Digital Evidence Help Desk Hours: 7:00 a.m.–5:30 p.m. Eastern standard time Monday–Friday	

20-cv-9284(FBI)-50

OTD Offices	OTD Phone Numbers, Intranet Sites, and Addresses
Unit Chief	
Unit Chief	
Unit Chief	
Unit Chief	
Unit Chief	

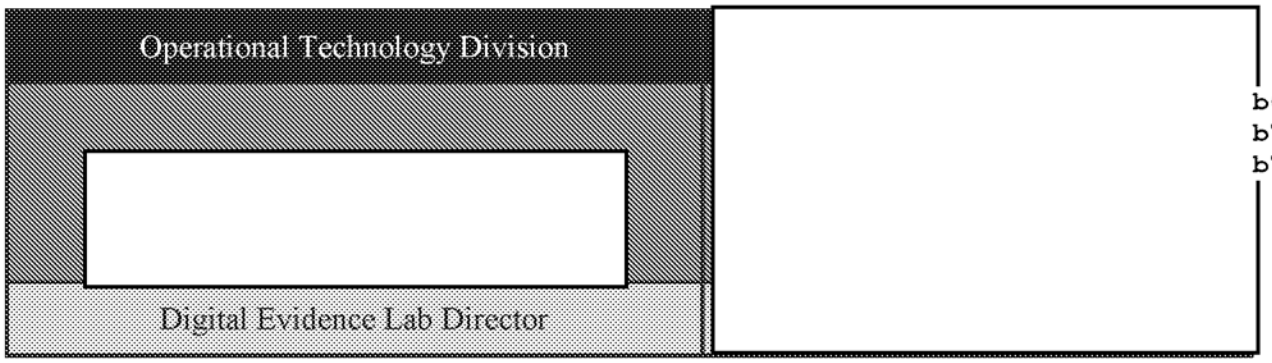
b6 -1
b7C -1
b7E -1, 4, 6

20-cv-9284(FBI)-51

OTD OFFICES	OTD PHONE NUMBERS, INTRANET SITES, AND ADDRESSES
[redacted] Unit Chief	b6 -1 b7C -1 b7E -1, 4, 6
[redacted] Unit Chief	

20-cv-9284(FBI)-52

Appendix C: (U) Contact Information



b6 -1
b7C -1
b7E -1, 4, 6

20-cv-9284(FBI)-53

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 [redacted] b7E -3, 4, 5

(U//~~FOUO~~) On-scene, digital media may either be [redacted] Otherwise, based on legal authority, there may be a decision as to whether to [redacted] 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 [redacted] b7E -3, 4, 5 U//~~FOUO~~.

[redacted] b7E -3, 4, 5

Figure 3. (U//~~FOUO~~) [redacted]

20-cv-9284(FBI)-54

(U) Imaging (Copying) DE

(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, b7E -3, 4, 5

(U//~~FOUO~~) In order to preserve and maintain the original evidence as it was found, b7E -3, 4, 5

(U//~~FOUO~~) To prevent cross contamination, b7E -3, 4, 5

(U//~~FOUO~~) The above processes related to [redacted] are described in the CART 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 site.

(U//~~FOUO~~) **Computer Analysis Response Team technician**: personnel trained and certified by OTD's Digital Sciences Development and Staffing Unit to forensically copy or image DE.

(U//~~FOUO~~) **Computer Analysis Response Team forensic examiner**: FBIHQ or field personnel, typically assigned full time to DE work, who are trained, equipped, and certified by OTD's Digital Sciences Development and Staffing Unit to copy or image DE, search DE, extract data from DE, and are authorized to provide opinions related to DE in court.

(U//~~FOUO~~) **CART on-the-job trainee**: personnel identified by field office management to participate in training, with a commitment toward becoming certified CART FEs.

(U//~~FOUO~~) **CART forensic examiner trainee**: personnel assigned to work toward CART FE certification 100 percent 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 percent of their time to CART FE work.

(U//~~FOUO~~) **Content review report**: factual report of SFE 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**: 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 -3, 4, 5

20-cv-9284(FBI)-55

(U//~~FOUO/LES~~) **DFAS technical experts**: DFAS [redacted] b7E -3, 4, 5

[redacted]

(U//~~FOUO~~) **Digital evidence**: data stored digitally on integrated circuits, microcontrollers, 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**: personnel trained to copy or image DE and perform simple SFE processes on copies of DE.

(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).

(U//~~FOUO/LES~~) **Digital evidence processing**: Processing of DE applies to personnel who are trained and tested to process DE, which includes procedures related to on-scene previewing, imaging, memory capture, performing content reviews, DE searches, extraction, preparing reports, and advanced technical analyses [redacted] b7E -3, 4, 5

[redacted]

(U//~~FOUO~~) **Examination**: forensic process whereby a forensic examiner reviews digital evidence for [redacted] b7E -3, 4, 5

[redacted] 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 [redacted]

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

(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 or her 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 other 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] and b7E -3, 4, 5
provided for investigative purposes.

20-cv-9284(FBI)-56

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

(U//~~FOUO~~) **Field Audio Video Personnel forensic analyst**: personnel trained to perform basic forensic functions related to audio and video DE.

(U) [redacted] b7E -3, 4, 5

(U//~~FOUO~~) **Master copy**: the required copy of DE that is stored on media to be retained and logged on FD-1004, "Federal Bureau of Investigation Evidence Chain of Custody" form. This is a [redacted] 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 reviewed before making any copies. If there is a question as to whether a copy of the legal authority documents can be retained and/or forwarded, contact OGC or the local CDC.

(U) **Metadata**: A set of data that describes and gives information about other data.

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

(U) **Random-Access Memory**: a computer system's memory that contains contents of recent applications and data so that they can be accessed quickly when needed by the computer's processor.

(U//~~FOUO~~) **Reexamination**: A reexamination of DE occurs when data/evidence, already [redacted] b7E -3, 4, 5

(U//~~FOUO~~) **Regional Computer Forensics Laboratory associate examiner**: former certified CART FE from an agency participating in the RCFL program who has completed his or her commitment to the RCFL, returns to his or her home agency, and continues a relationship with the RCFL to maintain certification and training.

(U//~~FOUO~~) **Report of examination**: The official report of examination used by CART FEs, Forensic Audio Video Image examiners, and other DE technical experts to report the results of [redacted] b7E -3, 4, 5

(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 for review by personnel working for or with the FBI in its investigations [redacted] b7E -3, 4, 5

Acronyms

AD	assistant director

20-cv-9284(FBI)-57

ADC	associate division counsel	
ADIC	assistant director in charge	
[redacted]		b7E -3, 4, 5
AG	Attorney General	
AGC	assistant general counsel	
ASAC	assistant special agent in charge	
ASAC	assistant special agent in charge	
ASCLD	American Society of Crime Laboratory Directors	
AUSA	assistant United States attorney	
[redacted]		b7E -3, 4, 5
CART	Computer Analysis Response Team	
CD	compact disc	
CDC	chief division counsel	
[redacted]		b7E -3, 4, 5, 6
CFR	Code of Federal Regulations	
CID	Criminal Investigative Division	
CIOS	Counterterrorism Internet Operations Section	
[redacted]		b7E -3, 4, 5
CS-FO	computer scientist-field operations	
CSO	chief security officer	
CSO	chief security officer	
[redacted]		b7E -3, 4, 5, 6
CTD	Counterterrorism Division	

20-cv-9284(FBI)-58

DAG	Deputy Attorney General
DARC	Digital Analysis and Research Center
DE	digital evidence
DEFOU	Digital Evidence Field Operations Unit
DEL	Digital Evidence Laboratory
DEMS	Digital Evidence Management System
DExT	digital extraction technician
DFAS	Digital Forensics and Analysis Section
DIOG	*Domestic Investigations and Operations Guide*
DOJ	Department of Justice
DTA	domestic technical assistance
DVD	digital video disc
DVR	digital video recorder
EC	electronic communication
ECF	evidence control facility
ECT	evidence control technician
ELSUR	electronic surveillance
FA	forensic analyst
FAU	Forensic Analysis Unit
FAVIAU	Forensic Audio, Video, and Image Analysis Unit
FAVP	Field Audio Video Program
FBI	Federal Bureau of Investigation
FBINet	FBI Intranet

b7E -3, 4, 5

20-cv-9284(FBI)-59

FE	forensic examiner
FET	forensic examiner trainee
[redacted]	[redacted]
FSU	Forensic Support Unit
[redacted]	[redacted]
GB	gigabyte
GC	general counsel
IAU	Investigative Analysis Unit (OTD)
IC	Intelligence Community
IED	improvised explosive device
IINI	Innocent Images National Initiative
ISO	International Standards Organization
IT	information technology
ITS	information technology specialist
JTF	joint task force
LA	legal advisor
LD	laboratory director
LEA	law enforcement agency
Legat	legal attaché
LES	Law Enforcement Sensitive
[redacted]	[redacted]
MOU	memorandum of understanding
NDA	nondisclosure agreement

b3 -1
b7E -2, 3, 4, 5

b7E -3, 4, 5

20-cv-9284(FBI)-60

[redacted]		b7E -3, 4, 5, 6
OGC	Office of the General Counsel	
OJT	on-the-job training	
[redacted]		
OTD	Operational Technology Division	
[redacted]		b7E -3, 4, 5, 6
PD	policy directive	
PG	policy guide	
PII	personally identifiable information	
PKI	Public Key Infrastructure	
[redacted]		b3 -1 b7E -2, 3, 4, 5
QA	quality assurance	
QAM	*Quality Assurance Manual*	
RA	resident agency	
RAM	random-access memory	
RCFL	Regional Computer Forensics Laboratory	
SA	special agent	
SAC	special agent in charge	
[redacted]		
SD	Secure Digital [card]	
SFE	search, find, extract	b3 -1 b7E -2, 3, 4, 5
SIM	sensitive investigative matter	
[redacted]		

20-cv-9284(FBI)-61

SSA	supervisory special agent
STB	Science and Technology Branch
STLS	Science and Technology Law Section
tech	technician
TOS	Tactical Operations Section
TURK	Time Utilization and Recordkeeping
U.S.C.	United States Code
U.S.C.	United States Code
UC	unit chief
UCFN	universal case file number
USAO	United States Attorney's Office
USB	Universal Serial Bus
VCAC	violent crimes against children

20-cv-9284(FBI)-62

Appendix E: (U//~~FOUO~~) Examination of FBI Evidence [redacted] b7E -3, 4, 5

[redacted]

(U//~~FOUO~~) As discussed in subsection 4.3.9.1., 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 an authorized forensic program of the FBI 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, a DOJ entity, or another prosecutorial or investigative agency to have FBI evidence processed, examined, or analyzed by [redacted] b7E -3, 4, 5

[redacted]

(U//~~FOUO~~) This procedure is separate and distinct from reexamination (as defined in subsection 4.2.11.2. above). A reexamination 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 must follow the guidance in subsection 4.3.9.2. regarding the transfer of evidence. b7E -3, 4, 5, 6

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

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

(U//~~FOUO~~) [redacted] b7E -3, 4, 5

(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 UC, FSU and the appropriate CART Field Operations program manager. [redacted]

[redacted]

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

20-cv-9284(FBI)-63

1. (U) The FBI case ID or UCFN.
2. (U) The FBI field office, telephone number, and fax number.
3. (U) The FBI case agent's name.
4. (U) The applicable case prosecutor's name, if known.
5. (U) A description of the original evidence to be released.
6. (U) The full name, address, and telephone number of [redacted] b7E -3, 4, 5
7. (U) A certification that a supervisory prosecutor and a CDC have concurred in the request, and that the supervisory prosecutor has read and understands the FBI's policy that if [redacted]
8. (U) The full name and position title of the case agent's SSA.
9. (U) An acknowledgement from the case agent that he or she understands that it is the case agent's responsibility to make all required notifications to the prosecutor concerning [redacted] b7E -3, 4, 5

(U//~~FOUO~~) [redacted] must include a letter from the USAO, or district attorney if a state or local case, [redacted]

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

(U//~~FOUO~~) Approving [redacted] b7E -3, 4, 5

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

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

(U//~~FOUO~~) [redacted] b7E -3, 4, 5

[redacted] the American Society of Crime Laboratory Directors-Laboratory Accreditation Board (ASCLD-LAB) or the International Standards Organization (ISO), in the recognized forensic discipline or subdiscipline relevant to the examination considered for [redacted]

20-cv-9284(FBI)-64

b7E -3, 4, 5

(U//~~FOUO~~)

- (U//~~FOUO~~) b7E -3, 4, 5
- (U//~~FOUO~~)

(U//~~FOUO~~) b7E -3, 4, 5

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

- (U//~~FOUO~~) Breadth of experience: the number and complexity of forensic examinations/analyses conducted b7E -3, 4, 5
- (U//~~FOUO~~) Testimonial experience: the experience
- (U//~~FOUO~~) Report quality: the quantity and quality of written reports produced by b7E -3, 4, 5
- (U//~~FOUO~~) Equipment acceptance
- (U//~~FOUO~~) Testing and evaluation documentation: whether there exists sufficient test and validation documentation on the equipment, tools, or materials b7E -3, 4, 5
- (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 -3, 4, 5
  - (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] b7E -3, 4, 5 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 (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 (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 -3, 4, 5 [redacted]
- (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 policies, as well as the facility and information technology (IT) system in which the evidence will be stored and reviewed that is compliant with FBI security policies and [redacted] b7E -3, 4, 5
- (U//~~FOUO~~) Occupational safeguard services: whether appropriate [redacted]

20-cv-9284(FBI)-66

- (U//~~FOUO~~) Depth/adequacy of examination: whether all necessary examinations, routines, and procedures will be conducted by [redacted] b7E -3, 4, 5 (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] b7E -3, 4, 5

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

(U//~~FOUO~~) Prior to initiating a request for [redacted] b7E -3, 4, 5

- (U//~~FOUO~~) Conduct the examination(s) and testify, as required, at all proceedings associated with the case.
- (U//~~FOUO~~) Conduct all necessary examinations, taking into consideration 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 an 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 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 -3, 4, 5

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

(U//~~FOUO~~) Disqualified [redacted] b7E -3, 4, 5

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

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

20-cv-9284(FBI)-67

- (U//~~FOUO~~)

- (U//~~FOUO~~) The FBI has information that it believes b7E -3, 4, 5

- (U//~~FOUO~~)

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

(U//~~FOUO~~) may not be used, in whole or in part, to seek or obtain second opinions or reexaminations regarding a forensic examination/analysis or variations of an examination/analysis already commenced or completed by an FBI STB laboratory without obtaining reexamination authority as described in subsection 4.3.10. of this PG. If authority is sought for a second opinion or reexamination, 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 reexamination. b7E -3, 4, 5

(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). b7E -3, 4, 5

(U//~~FOUO~~) Investigations Prohibited b3 -1

(U//~~FOUO~~) b7E -2, 3, 4, 5

- (U//~~FOUO~~)

- (U//~~FOUO~~) b3 -1 b7E -2, 3, 4, 5

- (U//~~FOUO~~)

- (U//~~FOUO~~)

20-cv-9284(FBI)-68

- (U//~~FOUO~~) Any national security investigation.

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

(U//~~FOUO~~) The SC, DFAS must prepare an EC containing the approval or denial of [redacted] b7E -3, 4, 5 request and the case agent must ensure that the EC is serialized to the relevant investigative case file. This EC must include the date the request was either approved or denied.

(U//~~FOUO~~) In the case of an approved [redacted] a certification by the SC, DFAS that he or she has determined that the proposed [redacted]

20-cv-9284(FBI)-69