

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF TEXAS  
SHERMAN DIVISION

BRIAN HUDDLESTON,

Plaintiff,

v.

CIVIL ACTION No. 4:20CV00447

FEDERAL BUREAU OF  
INVESTIGATION and UNITED  
STATES DEPARTMENT OF JUSTICE,

Defendants.

**SIXTH DECLARATION OF MICHAEL G. SEIDEL**

I, Michael G. Seidel, declare as follows:

1. I am the Section Chief of the Record/Information Dissemination Section (RIDS), Information Management Division (IMD), Federal Bureau of Investigation (FBI), Winchester, Virginia. My previous declarations in this matter describe my employment history, responsibilities at the FBI, as well as the FBI's processing of the Freedom of Information Act (FOIA) requests at issue in this case. This is my sixth declaration overall in this action and it supplements and incorporates by reference the information previously provided by me in my prior declarations dated December 8, 2020 (First Seidel); dated January 6, 2021 (Second Seidel); dated April 20, 2021 (Third Seidel); dated December 15, 2021 (Fourth Seidel); and dated May 5, 2022 (Fifth Seidel). (ECF Nos. 10-1, 12-1, 23-1, 39-1, and 54-1.)

2. The FBI submits this declaration in further support of Defendant's Motion for Summary Judgment; in reply to Plaintiff's opposition to FBI's Motion for Clarification and/or Reconsideration; and in response to Plaintiff's Motion for Clarification of the Memorandum Opinion and Order Entered September 29, 2022. Part I of this declaration provides the Court

with a summary of the administrative history of Plaintiff's request; Part II addresses the FBI's position regarding Seth Rich's personal and work laptops; and Part III, in accordance with *Vaughn v. Rosen*, 424 F.2d 820 (D.C. Cir. 1973), provides the FBI's justification for the FBI's assertion of FOIA Exemptions 3, 6, 7(A), 7(C) and 7(E), 5 U.S.C. § (b)(3), (b)(6), (b)(7)(A), (b)(7)(C), and (b)(7)(E), to withhold in full seven (7) pages of newly discovered responsive records.

### **ADMINISTRATIVE HISTORY OF PLAINTIFF'S REQUEST**

*FOIPA REQUEST NO. 1465531; SUBJECT: SETH RICH (JANUARY 1, 2016, TO PRESENT)*

3. The administrative history related to the initial handling of Plaintiff's FOIA request has been previously discussed in the FBI's Fourth Seidel declaration in this case at paragraphs 7-24. The subsequent administrative history of Plaintiff's FOIA request is outlined below.

4. By letter dated December 9, 2022, the FBI made an additional release of records in response to Plaintiff's FOIA request. The FBI advised it reviewed 7 pages and all pages are being withheld in full pursuant to FOIA Exemptions (b)(3), (b)(6), (b)(7)(A), (b)(7)(C) and (b)(7)(E). Also, the FBI advised Plaintiff he could appeal the FBI's response to the Office of Information Policy (OIP) within ninety (90) days of its letter, contact the FBI's public liaison, or seek dispute resolution services by contacting the Office of Government Information Services (OGIS). **(Ex. A.)**

### **THE PERSONAL LAPTOP**

5. As previously stated, the information the FBI possesses relates to Seth Rich's personal laptop and is a compact disc containing images of the laptop provided to the FBI by a local law enforcement agency. The FBI does not have, nor has it ever had, physical possession of

the actual personal laptop. To simplify this matter for the Court and squash Plaintiff's "hot potato" concerns, the FBI submitted for *in camera* inspection, a see-through redacted version of the FD-302 identified in the FBI's *Vaughn* Index at Bates pages 405-407. The see-through redacted FD-302 clarifies for the Court exactly what was provided to the FBI, by whom, and for what purpose. The FD-302 also further justifies the FBI's assertion of Exemptions 7(D)-3 and 7(E)-6.

6. Plaintiff also argues that the FBI has provided inconsistent statements about whether the FBI extracted and processed data from the compact disc, referencing a motion filed early in the litigation when the FBI was still trying to provide the Court with a page count of documents to process. The FBI can typically identify the types and approximate volume of files on a compact disc without extracting the data. In this case, as soon as the FBI determined that the compact disc was exempt in its entirety pursuant to several FOIA exemptions, the FBI found no need for data extraction; therefore, no data extraction occurred.

7. Finally, Plaintiff argues that the FBI waived Exemptions 7(D)-3 and 7(E)-6 by failing to brief them. The FBI clearly asserted and explained these exemptions in the *Vaughn* Index, Seidel declarations, and related summary judgment briefing. The FBI addressed Exemption 7(D)-3 in the Fourth Seidel declaration, paragraphs 150-151 and in Part III.(C)(7) as further addressed within the Defendant's Motion for Summary Judgment. (ECF No. 39.) The FBI also justified its use of Exemption 7(E)-6 in the Fourth Seidel declaration paragraph 171 and in Part III.(C)(8) of the Defendant's Motion for Summary Judgment.

8. Plaintiff requested clarification as to whether the Court's September 29th Order is referring to Seth Rich's personal laptop or work laptop; however, the FBI presumed the Order is

referring to the compact disc containing images of Seth Rich's personal laptop, as that is the only "laptop" at issue in this case.

#### THE WORK LAPTOP

9. Plaintiff is correct that the FBI made no mention of the work laptop in its Motion for Summary Judgment. That is because the work laptop is not an agency record subject to the FOIA. During its search for records responsive to this request, the FBI located records acknowledging the FBI's receipt of the work laptop. The FBI processed these records, which document the receipt of the work laptop, releasing all segregable information.<sup>1</sup> These records are identified as follows:

- a) Email dated April 10, 2017, released in part on Bates page FBI(20-cv-447)-625;
- b) FBI form FD-1087 dated May 19, 2017, and 1B Evidence form released in part on Bates pages FBI(20-cv-447)-690 through 691; and
- c) Email dated June 26, 2018, consulted to the FBI by OIP released in part on Bates Page FBI(20-cv-447)-985.

10. The FBI collected the physical work laptop from a non-government third-party as acknowledged in the *Vaughn* Index at Bates page 690, and the work laptop is in an FBI Evidence Control Room according to information provided in the FBI 1B Evidence form, referenced in the *Vaughn* Index at Bates page 691. The work laptop is not an actual record; but rather physical object/evidence that is not subject to the FOIA; and therefore, the FBI did not address this item in its prior filings.

11. While conducting additional research to confirm the whereabouts of the work laptop, the FBI located a DVD and a tape drive which are also currently stored in the same Evidence Control Room and are marked as derivative evidence. Derivative evidence is defined

---

<sup>1</sup> The FBI's justifications for withholding these records were provided in the Fourth Seidel declaration.

as “evidence generated from the original or source evidence in Laboratory Division, a partner laboratory, or CART unit.” See the FBI’s Field Evidence Management Policy Guide 1132PG, July 23, 2021.

*The Work Laptop, Tape Drive, and DVD are not Agency Records Under the FOIA*

12. The term “agency record” under the FOIA extends only to those documents that an agency both (1) creates or obtains, and (2) controls at the time the FOIA request was made. The work laptop, tape drive, and DVD are not agency records under the FOIA because control by an agency requires more than mere possession. The FBI relied on *DOJ v. Tax Analysts*, 492 U.S. 136, 144-45 (1989) and *Burka v. United States Department of Health Human Serv.*, 318 U.S. App. D.C. 274, 87 F.3d 508, 515 (D.C. Cir. 1996) to reach this determination. Under the first part of *Tax Analysts*, the determination of whether something is an “agency record” (and therefore subject to the FOIA) depends on whether the “record” was (1) either created or obtained by an agency, and (2) under agency control at the time of the FOIA request. The second part of *Tax Analysts* under *Burka* established four factors relevant to a determination of whether the FBI exercises sufficient control over a record to render it an agency record including: (1) the intent of the document creator to retain or relinquish control; (2) the ability of the agency to use and dispose of the record as it sees fit; (3) the extent to which agency personnel have read or relied upon the document; and (4) the degree to which the document was integrated into the agency record system or files.

13. There is no question the work laptop was obtained by the FBI and was under agency control at the time of the request; however, per the four factor *Burka* analysis, the FBI determined the tape drive, DVD, and physical work laptop, are not “record[s] under agency control” based on the below analysis:

a. Factor 1: The intent of the document creator to retain or relinquish control: Before embarking on the analysis, it should be noted that the analysis assumes the item being evaluated is a “document” or a “record.” The work laptop is not, itself, neither a document nor a record under the normal meaning of those terms. The laptop is a physical evidentiary item. As referenced on Bates page FBI(20-cv-447)-690, the owner of the work laptop is a non-governmental third-party not subject to the FOIA. Upon receipt of the work laptop, the FBI stored the physical item in an Evidence Control Room. The work laptop is not FBI property, nor is any of the data contained on the device generated by the FBI. The same applies to the derivative evidence, specifically the tape drive and DVD containing duplicated images of the original work laptop’s content. These duplicated images are also stored in an Evidence Control Room. The FBI’s Digital Evidence Policy Guide<sup>2</sup> defines digital evidence as “digital evidence seized at a search scene or otherwise lawfully obtained and stored in an Evidence Control Facility.” (Ex. B.) Likewise, master copies are copies of digital evidence that are stored on media to be retained and logged on an FD-1004, FBI Evidence Chain of Custody form. Per the FBI’s Records Management Policy Guide,<sup>3</sup> the physical items, such as the work laptop, DVD, and tape drive, are not considered a record and are treated as evidentiary property managed under a different set of rules and regulations than actual agency records, which must follow specific record retention plans approved by National Archive and Record Administration (NARA) as described in the Policy Guide. (Ex. C.) Except for contraband, items subject to statutory forfeiture or instrumentalities of a crime, original digital evidence as well as the derivative

---

<sup>2</sup> Digital Evidence Policy Guide 0830PG, July 31, 2016.

<sup>3</sup> Records Management Policy Guide 0769PG, June 4, 2015.

evidence should be returned to its rightful owners when all criminal proceedings have terminated.

b. Factor 2: The ability of the agency to use and dispose of the record as it sees fit:

The laptop and derivative evidence at issue here are in an FBI Evidence Control Room as documented in the FBI's 1B Evidence Form Bates page FBI(20-cv-447)-691 and the FBI will provide the FD-1004 (FBI Evidence Chain of Custody),<sup>4</sup> in its December 9, 2022 supplemental release (Bates pages FBI(20-cv-447)-1802 and FBI(20-cv-447)-1803). Based on the nature of the information within the above cited records, the FBI determined it does not have the right to use and dispose of the evidentiary items (i.e., work laptop, DVD, and tape drive) as it sees fit. Instead, per the Digital Evidence Policy Guide referenced above, this evidence will be returned to its rightful owners when all criminal proceedings have terminated.

c. Factor 3: The extent to which agency personnel have read or relied upon the

document: The FBI found no indication that the FBI relied on the content of the work laptop, DVD, or tape drive.

d. Factor 4: The degree to which the document was integrated into an agency record

system or file: While the FBI documented the receipt of the evidentiary items described in the two documents referenced above, the FBI found no indication that either the work laptop or the derivative evidence was incorporated into its records systems or files. Instead, the FBI stored the evidentiary items in an Evidence Control Room as a physical item of evidence, in substantially the same manner as it would handle a bloody glove or a firearm. In sum, the FBI clearly distinguished these physical items as non-record evidence subject to the disposition of evidence,

---

<sup>4</sup> FD-1004 (FBI Evidence Chain of Custody): This form tracks evidence within an investigation and contains essential information about the handling, storage, and retrieval of evidence.

as distinguished from the related investigative case file documents subject to the FOIA handled under the established record retention plan approved by NARA.

14. The FBI determined the physical work laptop, DVD, and tape drive are not actual agency records; but rather are physical evidentiary objects, not subject to the FOIA. Accordingly, because the physical work laptop, DVD, and tape drive are not agency records under the FOIA, the FBI did not address these items in its prior filings.

*Newly Located Records*

15. During its search for the work laptop, RIDS contacted an FBI Special Agent (SA) assigned to an FBI computer intrusion investigation. As a result, RIDS also located, a letter from a third-party that accompanied the work laptop, two FD-1004's "FBI Evidence Chain of Custody" Forms and a three (3) page forensic report detailing the actions performed by an outside entity to image the work laptop. These newly located records were not indexed to the subject, Seth Rich within the Central Records System (CRS), nor is Seth Rich's name mentioned in the FD-1004's or forensic report. These records were attached to the physical evidence (i.e., work laptop, DVD, and tape drive) and were not electronically uploaded to the electronic case file in Sentinel. As such, a search of Seth Rich's name would not have located these records, even with a text search of Sentinel. It was only through discussions with the SA assisting RIDS to locate the work laptop, that RIDS was able to determine that the report, letter from a third-party and Chain of Custody forms existed and were related to Seth Rich's work laptop. The SA advised RIDS that disclosure of these records would cause harm to an FBI investigation and Department of Justice prosecution of several employees of the Russian Federation (more details discussed below). Upon review of the letter from a third-party, three (3) page forensic report and two (2) Chain of Custody forms, RIDS determined these documents were responsive records subject to the FOIA,



even though the physical work laptop, DVD, and tape drive are not agency records subject to the FOIA. Therefore, immediately upon discovering these new responsive records, the FBI commenced processing the records and determined they would be withheld in full pursuant to FOIA Exemptions 3, 6, 7(A), 7(C) and 7(E). The FBI's justification for withholding these pending records is discussed below.

#### **JUSTIFICATION FOR NONDISCLOSURE UNDER THE FOIA**

16. The FBI processed all records responsive to Plaintiff's request to achieve maximum disclosure consistent with the access provisions of the FOIA. Every effort was made to provide Plaintiff with all information in the public domain and with all reasonably segregable, non-exempt information. The FBI did not withhold any reasonably segregable, nonexempt portions from Plaintiff. Further description of the information withheld, beyond what is provided in this declaration, could identify the actual exempt information.

17. Bates Numbering: The FBI numbered all pages of its supplemental production consecutively as FBI(20-cv-447)-1802 through FBI(20-cv-447)-1808.<sup>5</sup>

18. Justification Codes: On the Bates-numbered pages withheld in full, the FBI further categorized its application of exemptions to better explain the nature of the information withheld pursuant to the provisions of the FOIA. Specifically, the FBI applied numerical codes that coincide with specific categories of exempt information. This declaration and index demonstrate that all information withheld by the FBI is exempt from disclosure pursuant to the cited FOIA exemptions or is so intertwined with non-exempt information that segregation is not possible without revealing the underlying exempt information.

---

<sup>5</sup> If requested, the FBI can provide copies of all records processed to the Court for *in camera* inspection.

19. Each instance of information withheld pursuant to a FOIA exemption is accompanied by a coded designation that corresponds to one of the categories listed below. For example, if “(b)(7)(C)-1” appears on a page, the “(b)(7)(C)” designation refers to FOIA Exemption 7(C) protecting against unwarranted invasions of personal privacy. The numerical designation “1” following “(b)(7)(C)” narrows the main category into a more specific subcategory, such as “Names and Other Identifying Information of FBI Special Agents and Professional Staff.”

<b>SUMMARY OF EXEMPTION JUSTIFICATION CATEGORIES</b>	
<b>CODED CATEGORIES</b>	<b>INFORMATION WITHELD</b>
<b>Exemption 3</b>	<b>Information Protected By Statute</b>
(b)(3)-1	National Security Act of 1947 [50 U.S.C. 3024(i)(1)]
<b>Exemption 7(A)</b>	<b>Pending Law Enforcement Proceedings</b>
(b)(7)(A)-1	Information the Disclosure of which Could Reasonably be Expected to Interfere with Pending Enforcement Proceedings
<b>Exemptions (6) &amp; 7(C)</b>	<b>Unwarranted/Clearly Unwarranted Invasion Of Personal Privacy</b>
(b)(6)-1 and (b)(7)(C)-1	Names and Other Identifying Information of FBI Special Agents and Professional Staff
(b)(6)-4 and (b)(7)(C)-4	Names and Other Identifying Information of Third Parties who Provided Information
(b)(6)-5 and (b)(7)(C)-5	Names and Other Identifying Information of Non-FBI Federal Government Personnel
<b>Exemption 7(E)</b>	<b>Law Enforcement Techniques And Procedures</b>
(b)(7)(E)-2	Sensitive Investigative File Numbers and Sub-File Names
(b)(7)(E)-3	Database Information
(b)(7)(E)-6	Collection and Analysis of Information
(b)(7)(E)-9	Identities of an FBI Unit, Squad and Division
(b)(7)(E)-10	Highly Sensitive Investigative Law Enforcement Technique and Procedure

20. I hereby incorporate by reference the information contained in my Fourth Seidel Declaration concerning FOIA Exemptions (b)(6), (b)(7)(C) and (b)(7)(E),<sup>6</sup> to include specifically, FOIA Exemption Coded Categories (b)(6)-1, 4, 5; (b)(7)(C)-1, 4, 5; and (b)(7)(E)-2, 3, 6, 9 discussed in ¶¶ 126-129, 132-135, 159-167, 171, 176-177. Each of these FOIA Exemption Coded Categories have also been asserted to withhold information in the newly produced records.

21. In addition, to the above mentioned FOIA Exemptions and Coded Categories, the FBI hereby asserts FOIA Exemption 7(E) to protect Highly Sensitive Investigative Law Enforcement Technique and Procedure.

#### **EXEMPTION 7 THRESHHOLD**

22. Before an agency can invoke any of the harms enumerated in Exemption (b)(7), it must demonstrate the records or information at issue were compiled for law enforcement purposes. Pursuant to 28 U.S.C. §§ 533 and 534, Executive Order 12333 as implemented by the Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM), and 28 C.F.R. § 0.85, the FBI is the primary investigative agency of the federal government with authority and responsibility to investigate all violations of federal law not exclusively assigned to another agency, to conduct investigations and activities to protect the United States and its people from terrorism and threats to the national security, and to further the foreign intelligence objectives of the United States. Under this investigative authority, the responsive records herein were created and compiled in furtherance of the FBI's role in the Special Counsel's Office (SCO) investigation and related investigations. These records were created and compiled to document

---

<sup>6</sup> See Fourth Seidel Declaration ¶¶ 123-140, 156-177.

the FBI's investigation of potential crimes and threats to the national security, thus, the FBI determined they were created and compiled for a law enforcement purposes.<sup>7</sup>

**EXEMPTION (b)(3)  
INFORMATION PROTECTED BY STATUTE**

23. As discussed in my Fourth Seidel Declaration at ¶ 94, Exemption (b)(3) exempts from disclosure information which is “specifically exempted from disclosure by statute ... if that statute (A)(i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue; or (A)(ii) establishes particular criteria from withholding or refers to particular types of matters to be withheld.”

(b)(3)-1: NATIONAL SECURITY ACT OF 1947, 50 U.S.C. § 3024(i)(1)

24. I hereby reassert the information contained in my Fourth Declaration ¶¶ 95-98 concerning FOIA Exemption Category (b)(3)-1 to protect from disclosure information pursuant to Section 102A(i)(1) of the National Security Act of 1947 (NSA), as amended by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). This Exemption Coded Category is also applicable to the newly produced records. Specifically in these records, the FBI is asserting Exemption 3, at times in conjunction with Exemption 7(E) to withhold unclassified intelligence sources and methods that were employed as law enforcement techniques, procedures, or guidelines, and thus would qualify as both an intelligence source and method under Exemption 3 and a law enforcement technique under Exemption 7(E). Notably, 50 U.S.C. § 3024(i)(1) protects sources and methods regardless of whether they are classified. *See* Sims, 471 U.S. at 176.

---

<sup>7</sup> Both DOJ and the FBI are responsible for maintaining portions of the SCO record collection, with FBI retaining the investigative records.

**EXEMPTION 7(A)  
PENDING LAW ENFORCEMENT PROCEEDINGS**

25. FOIA Exemption 7(A) exempts from disclosure records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information...could reasonably be expected to interfere with enforcement proceedings. 5 U.S.C. § 552 (b)(7)(A).

26. Application of this exemption requires: the existence of law enforcement records; a pending or prospective law enforcement proceeding; and a determination that release of the information could reasonably be expected to interfere with the enforcement proceeding. Often, the FBI asserts Exemption 7(A) categorically to withhold a variety of different documents in an investigative file, which the FBI then groups into functional categories and describes in greater detail. In this case, however, the FBI asserted Exemption 7(A) in a limited fashion to protect information about pending law enforcement investigation. The release of this information would reveal details concerning the pending enforcement procedures, to include the existence and location of the investigation. The FBI determined release of any of this material would provide criminals and agents of foreign powers with information about the United States government's investigation and enforcement strategies in these ongoing matters, which could allow criminals and our national adversaries to predict and potentially thwart these strategies, and/or allowing them to discover and tamper with witnesses and destroy evidence. As such, revealing this previously undisclosed and unacknowledged information could reasonably be expected to interfere with pending enforcement proceedings. Thus, the FBI has applied Exemption 7(A) to protect this information.

## BACKGROUND ABOUT THE PENDING ENFORCEMENT PROCEEDING

27. In or around 2016, the Russian Federation (Russia) operated a military intelligence agency now called the Main Directorate of the General Staff of the Armed Forces of the Russian Federation, then known as the Main Intelligence Directorate, and still commonly known by its abbreviation GRU, the Russian abbreviation of “Glavnoye Razvedyvatelnoye Upravlenie,” that in short, is the foreign military intelligence agency of the General Staff of the Russian Armed Forces. The GRU had multiple units, including Units 26165 and 74455, engaged in cyber operations that involved the staged releases of documents stolen through computer intrusions. These units conducted largescale cyber operations to interfere with the 2016 U.S. presidential election.

28. On July 13, 2018, a Grand Jury for the District of Columbia in *United States of America v. Viktor Borisovich Netyksho, et al.*, Criminal No. 1:18-cr-00215, returned an indictment against 1) Viktor Borisovich Netyksho, 2) Boris Alekseyevich Antonov, 3) Dmitriy Sergeyevich Badin, 4) Ivan Sergeyevich Yermakov, 5) Aleksey Viktorovich Lukashev, 6) Sergey Aleksandrovich Morgachev, 7) Nikolay Yuryevich Kozachek, 8) Pavel Vyacheslavovich Yershov, 9) Artem Andreyevich Malyshev, 10) Aleksandr Vladimirovich Osadhuk, 11) Aleksey Aleksandrovich Potemkin, and 12) Anatoliy Sergeyevich Kovalev, charging them with one or more of the following:

- a. 18 U.S.C. §§ 371 and 3559(g)(1) Conspiracy to Commit an Offense or defraud the United States;
- b. 18 U.S.C. §§ 1028A(a)(1) and (2) Aggravated Identity Theft; and
- c. 18 U.S.C. § 1956(h) Conspiracy to Launder Money.

### REASONABLE EXPECTATION OF INTERFERENCE

29. Release of any of the information concerning this investigation, to include the letter from a third-party, two (2) FD-1004 FBI Evidence Chain of Custody Forms and the Report, would be premature because the defendants are fugitives; therefore, the release of such information would trigger a multitude of harms:

a. Suspects and persons of interest would know investigative details that would either alert them to efforts directed towards them and/or would allow them to analyze pertinent information about the investigation. As a result, these individuals would acquire the unique advantage of knowing certain details about or related to them which could be used to their advantage to escape prosecution and thwart current investigative efforts by altering or counteracting evidence, changing behavior, intimidating or physically harming witnesses or law enforcement officials, and/or flight.

b. Once information is released into the public domain, its use and dissemination by third parties are unrestricted. As such, release of these investigative details would allow third parties who are not directly related to this matter to interfere with investigative efforts or any future prosecution(s) through harassment, intimidation, and creation of false evidence by dispensing extraneous facts discussed in the investigation. Given that individuals involved in cyber operations rarely work alone, the threat posed by such harassment and intimidation is real.

c. The release of the withheld investigative details could lead to the identification of sources of information, witnesses, potential witnesses, law enforcement personnel, and individuals otherwise associated with the investigation who could be targeted for intimidation and/or physical harm.



30. In this case, the FBI continues to work with the Department of Justice and federal, state, and local law enforcement partners to apprehend these fugitives. The information contained within the letter from a third party, report and the two (2) FD-1004 FBI Evidence Chain of Custody forms is tied to that investigation and until these fugitives are apprehended and the prosecutions concluded, any release of this information will interfere with enforcement proceedings.

**EXEMPTION (b)(7)(E)**  
**INVESTIGATIVE TECHNIQUES AND PROCEDURES**

31. FOIA Exemption (b)(7)(E) provides protection for:

law enforcement records [which]...would disclose techniques and procedures for law enforcement investigations or prosecutions or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

U.S.C. § 552(b)(7)(E).

32. Exemption (b)(7)(E) has been asserted to protect information from these records, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

33. Within the responsive documents, the FBI applied Exemption (b)(7)(E) to non-public investigative techniques and procedures utilized by the FBI to pursue its law enforcement mission, and to non-public details about techniques and procedures that are otherwise known to the public. Specifically, the FBI asserted Exemption 7(E) to protect the following categories of information.



(b)(7)(E)-10: HIGHLY SENSITIVE INVESTIGATIVE LAW ENFORCEMENT TECHNIQUE AND PROCEDURE

34. In Exemption Category (b)(7)(E)-10, the FBI protected information pertaining to sensitive law enforcement techniques and procedures the FBI uses for both criminal and national security investigations. Revealing the specific details of how these techniques and procedures are employed, in what situations they are most effective, the types of targets against which these techniques are employed, and the nature of the information gleaned via the use of these techniques and procedures, would be extremely detrimental to the FBI's ability to effectively utilize these techniques and procedures. Release of this information would allow criminals and those who threaten the national security of the United States the ability to develop countermeasures to circumvent the FBI's use of these techniques and procedures, greatly reducing their effectiveness. The use of these techniques and procedures within the investigative records at issue is not known, and further description of these techniques and procedures in this context could result in circumvention of these techniques and procedures by investigative subjects. As further disclosure would undoubtedly compromise crucial law enforcement techniques and procedures, and severely hamper the FBI's law enforcement efforts to detect and apprehend individuals who seek to violate the United States' criminal and national security laws, the FBI withheld this information pursuant to Exemption 7(E). If the Court requires further justification for the withholding of this information, the FBI can provide additional information, *in camera, ex parte*.

**SEGREGABILITY**

35. As discussed in ¶ 4 supra, the FBI identified a total of (seven) 7 additional responsive pages. Following its segregability review, RIDS determined all information on each page was covered by one or more of the cited FOIA exemptions; therefore, there was no

information that could be reasonably segregated for release without triggering foreseeable harm to one or more of the cited FOIA exemptions.

### **CONCLUSION**

36. The FBI processed and released all reasonably segregable non-exempt information from records responsive to Plaintiff's FOIA request that are subject to FOIA. The FBI processed the records under the access provisions of the FOIA to achieve maximum disclosure. Information was properly withheld in its entirety pursuant to FOIA Exemptions 3, 6, 7(A), 7(C), and 7(E). The FBI carefully examined the documents and determined the information withheld from Plaintiff in this case, if disclosed could reasonably be expected to interfere with pending or prospective enforcement proceedings, would reveal statutorily protected information, would cause a clearly unwarranted invasion of personal privacy or could reasonably be expected to constitute an unwarranted invasion of personal privacy, and/or would disclose techniques and procedures for law enforcement investigations. Further, the FBI determined the work laptop, DVD, and tape drive are not records subject to the FOIA. After extensive review of the documents at issue, the FBI determined that there is no further non-exempt information that can be reasonably segregated and released without revealing exempt information.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct, and that Exhibit A-C attached hereto are true and correct copies.

Executed this 9<sup>th</sup> day of December 2022.

A handwritten signature in blue ink, appearing to read "Michael G. Seidel", written over a horizontal line.

MICHAEL G. SEIDEL  
Section Chief  
Record/Information Dissemination Section  
Information Management Division  
Federal Bureau of Investigation  
Winchester, Virginia