REVISED

An Investigation of Alleged Misconduct by Then DOJ Trial Attorney [redacted]

(b)(6); (b)(7)(C)

★ ★ ★

September 2023

I. Introduction

This report summarizes the Department of Justice (Department or DOJ) Office of the Inspector General's (OIG) investigation of allegations that [redacted] then a trial attorney [redacted] of the Criminal Division, disclosed Department [redacted] information [redacted] the Criminal Division referred to the OIG allegations that [redacted] had improperly provided Department [redacted] information [redacted]

(b)(6); (b)(7)(C)

The OIG found that (b)(6); (b)(7)(C) 72-page (b)(6); (b)(7)(C) memorandum contained grand jury information subject to Rule 6(e) of the Federal Rules of Criminal Procedure. The grand jury information revealed the existence of an indictment that was under seal as to the lead defendant and multiple codefendants as of the time (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

During the course of our investigation, the OIG interviewed 14 witnesses. (b)(6); (b)(7)(C) resigned during the course of our investigation and declined our subsequent requests for a voluntary interview. The OIG lacks testimonial subpoena authority over former DOJ employees, including those who retire or resign during the course of an OIG investigation, and therefore was unable to compel (b)(6); (b)(7)(C) participation in an interview. When we initially requested a voluntary interview of (b)(6); (b)(7)(C) in (b)(6); (b)(7)(C) we sought to conduct the interview via a virtual video platform due to the COVID-19 pandemic. We informed (b)(6); (b)(7)(C) counsel that because (b)(6); (b)(7)(C) was a former Department employee, we would require him to sign a non-disclosure agreement (NDA) in connection with an interview because the OIG would be sharing documents containing sensitive, non-public information with him electronically during the interview. Through counsel, (b)(6); (b)(7)(C) declined our request for a voluntary interview because of the requirement that he sign an NDA. (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) we requested through (b)(6); (b)(7)(C) counsel a voluntary interview in-person of (b)(6); (b)(7)(C) which we said would obviate the need for an NDA. Through counsel, (b)(6); (b)(7)(C) declined that request as well.

(b)(6); (b)(7)(C) attorney participated in a proffer process with the OIG between (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) As part of that process, (b)(6); (b)(7)(C) attorney proffered (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

We reviewed more than 5,000 documents, and our investigation included a digital forensic review of (b)(6); (b)(7)(C) DOJ-issued iPhone and laptop. As we discuss in detail in the report, in our digital forensic review of (b)(6); (b)(7)(C) DOJ-issued laptop, we found a shortened and heavily-redacted version of (b)(6); (b)(7)(C) memorandum. Our forensic examination further found that (b)(6); (b)(7)(C) copied this version of his memorandum, and other documents, to removable media devices that he attached to his DOJ-issued laptop.

Also among the documents we reviewed, and that we reference in this report, are (b)(6); (b)(7)(C) his (b)(6); (b)(7)(C) memorandum, which was a 72-page (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
(b)(6); (b)(7)(C) an (b)(6); (b)(7)(C) statement his attorney provided to the OIG during the proffer process.

Our investigation also included a separate forensic analysis of DOJ emails in which DOJ personnel sent or received (b)(6); (b)(7)(C) memorandum. We found that (b)(6); (b)(7)(C) sent copies of his memorandum to his personal email address, together with the exhibits to his memorandum. (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)

We also reviewed relevant laws and DOJ policies. We did not issue administrative subpoenas for records related to (b)(6); (b)(7)(C) personal email address or personal cell phone.[2] (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)

[2] The Inspector General Act of 1978 authorizes Inspectors General to "require by subpoena the production of all information, documents, reports, answers, records, accounts, papers, and other data in any medium (including electronically stored information), as well as any tangible thing and documentary evidence necessary in the performance of the functions assigned by [the Act]." 5 U.S.C. §§ 401 et seq., § 6(a)(4).

(b)(6); (b)(7)(C)

we found that both the 72-page memorandum (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) and the shortened and redacted version of the memorandum saved to (b)(6); (b)(7)(C) DOJ-issued laptop contained grand jury information, (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

The OIG did find that (b)(6); (b)(7)(C) violated (a) Department policy and rules of behavior related to the use of non-official email by emailing certain Department records, including records containing grand jury information, to his personal email account, and (b) Department policy related to the removal of federal records when he refused to return to the Department certain DOJ records following his resignation from DOJ. (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

---

3 (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

We have provided a copy of this report to the Criminal Division for its information and to the Department's Professional Misconduct Review Unit for such action as it deems appropriate. Unless otherwise noted, the OIG applies the preponderance of the evidence standard in determining whether Department personnel have committed misconduct. The Merit Systems Protection Board applies this same standard when reviewing a federal agency's decision to take adverse action against an employee based on such misconduct. See 5 U.S.C. § 7701(c)(1)(B); 5 C.F.R. § 1201.56(b)(1)(ii).

II. Relevant Statutes and Policies

A. Federal Rule Prohibiting Disclosure of Grand Jury Information

Federal Rule of Criminal Procedure 6(e) prohibits government attorneys, among other individuals, from disclosing a matter occurring before a grand jury.[4] Rule 6(e) does not define the term "matter occurring before the grand jury." Courts have interpreted it to cover only information that would reveal the strategy or direction of the grand jury investigation, the nature of the evidence produced before the grand jury, the views expressed by members of the grand jury, or anything else that actually occurred before the grand jury.

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) A Maryland federal district court has explained that protecting matters occurring before the grand jury prevents disclosures that "reveal the identity of grand jurors or expected witnesses, reveal witness' [sic] expected testimony or questions they would be asked, reveal transcripts or the substance of testimony, reveal the strategy or direction of a grand jury investigation, or report when the grand jury will return an indictment." *In re Search of 14416 Coral Gables Way, N. Potomac, Md.*, 946 F.Supp.2d 414, 427 (D. Md. 2011) (citing *United States v. Rosen*, 471 F.Supp.2d 651, 655 (E.D. Va.2007)). The Maryland court cited to an opinion from the District Court for the Eastern District of Virginia, which is also in the Fourth Circuit. *Id.*

The Court of Appeals for the Fourth Circuit has held that although matters occurring before the grand jury can "be anything that may reveal what has transpired before the grand jury," Rule 6(e)(2) protects "only the essence of what takes place in the grand jury room, in order to preserve the freedom and integrity of the deliberative process." *In re*

[4] Fed. R. Crim. P. 6(e)(2)(B).

Grand Jury Subpoena, 920 F.2d 235, 241-242 (4th Cir. 1990) (citing *In re Grand Jury Matter (Catania)*, 682 F.2d 61, 63 (3d Cir. 1982)). Although the Fourth Circuit does not appear to have directly addressed the question, other courts have held that government memoranda that reflect grand jury information are covered by Rule 6(e) to the extent that their disclosure would reveal grand jury matters.

Rule 6(e) separately expressly prohibits the disclosure of the existence of a sealed indictment.[5] It provides that the "magistrate judge to whom an indictment is returned may direct that the indictment be kept secret until the defendant is in custody or has been released pending trial. The clerk must then seal the indictment, and no person may disclose the indictment's existence except as necessary to issue or execute a warrant or summons."[6]

A knowing violation of Rule 6(e) may be punished by contempt of court.[7] Similarly, a knowing violation of a court's order also may be punished by contempt of court.[8]

(b)(6); (b)(7)(C)

[redacted]

[5] Fed. R. Crim. P. 6(e)(4).

[6] *Id.*

[7] Fed. R. Crim. P. 6(e)(7). *See also* 18 U.S.C. § 401(3).

[8] 18 U.S.C. § 401(3).

[9] (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

[redacted]

(b)(6); (b)(7)(C)

C. Federal Records and Government Information

1. The Definition of Federal Records

The statutory definition of federal records is broad, and includes:

> all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency...as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.[11]

Under DOJ policy, federal records include "[e]mail containing content that is evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Department."[12]

---

[10] (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

[11] 44 U.S.C. § 3301(a)(1)(A).

[12] DOJ Policy Statement 0801.04, Electronic Mail and Electronic Messaging Records Retention, § II.A (September 21, 2016) (hereinafter DOJ Policy Statement 0801.04).

In contrast, federal regulations define personal files or records as "documentary materials belonging to an individual that are not used to conduct agency business."[13] DOJ similarly defines personal emails as "[e]mail messages that are not related to business."[14] Merely labeling a document as "personal" does not affect the status of a document if it is "used in the transaction of public business."[15]

2. Department Policy and Rules of Behavior Regarding Use of Non-Official E-Mail Accounts (b)(6); (b)(7)(C)

The Department policy on the retention of email records requires all Department employees to use only approved email accounts to send and receive DOJ business-related communications.[16] The policy defines a business email as an email that contains information related to the mission of the Department or administrative matters.

Department employees are required to complete annual Computer Security Awareness Training and to acknowledge reading the Department of Justice Cybersecurity and Privacy Rules of Behavior for General Users (Rules of Behavior) concerning the use, security, and acceptable level of risk for Department systems and applications. The Rules of Behavior prohibit Department employees from using personal email accounts for DOJ business except under exigent circumstances and require employees to comply with DOJ Policy Statement 0801.04, the Department's email policy. The Rules of Behavior also prohibit Department employees from using personally-owned information technology such as computers or removable media to store government-related work. Relevant here, on (b)(6); (b)(7)(C) reviewed and acknowledged his compliance with the Rules of Behavior (Version 12).

(b)(6); (b)(7)(C)

3. Department Policy Regarding Removal of Federal Records

A Department policy on the removal of and access to Department information states that "[a]ll DOJ employees are responsible for maintaining the information they generate, receive, or review while conducting Departmental business in accordance with Departmental and component policies."[18] The policy states that employees may not,

---

[13] 36 C.F.R. § 1220.18.

[14] DOJ Policy Statement 0801.04, § II.C.

[15] 36 C.F.R. § 1222.20(b)(3).

[16] DOJ Policy Statement 0801.04, § V.D.

[17] (b)(6); (b)(7)(C)

[18] DOJ Policy Statement 0801.02, Removal of and Access to Department of Justice Information, § I (December 18, 2014) (hereinafter DOJ Policy Statement 0801.02).

without agency permission, remove records from the Department—either during or after employment.[19] The only items that departing employees may remove without prior approval are personal information or documents that are unrelated to the Department and official business; copies of any unclassified information already officially in the public domain; and copies of the employee's email contacts.[20]

A departing employee must make a written request, receive approval from the appropriate official, and execute a nondisclosure agreement before removing any records or information.[21] Before authorizing any such request, the approving official must ensure that the requested documents do not contain any prohibited categories of information, such as grand jury information.[22]

III. Factual Findings

A. [redacted] Professional Background

[redacted] joined the Department in [redacted] as a trial attorney [redacted] At the time of the events described here, [redacted] was a member of a unit of the [redacted]

[redacted] received a law degree from [redacted] in [redacted] He is licensed to practice law in [redacted] Before joining the Department, [redacted] was [redacted]

---

[19] DOJ Policy Statement 0801.02, §§ I.A., I.B.

[20] DOJ Policy Statement 0801.02, § I.B.

[21] DOJ Policy Statement 0801.02, § I.A.

[22] DOJ Policy Statement 0801.02, §§ I.A, II.A.2.

[23] [redacted]

Withheld pursuant to exemption

(b)(6) ; (b)(7)(C)

of the Freedom of Information and Privacy Act

(b)(6); (b)(7)(C)

D. (b)(6); (b)(7)(C) Submits a 72-Page Memorandum that Contains Grand Jury Information (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) a 72-page memorandum, with 47 exhibits, (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

Withheld pursuant to exemption

(b)(6) ; (b)(7)(C)

of the Freedom of Information and Privacy Act

(b)(6); (b)(7)(C)

Subsequent to providing it to the OIG, (b)(6); (b)(7)(C) informed the OIG that it believed the (b)(6); (b)(7)(C) memorandum contained grand jury information, as did (b)(6); (b)(7)(C) of the 47 exhibits to the memorandum. (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) We discuss in more detail below the memorandum, the two exhibits containing grand jury information, and the third exhibit that was filed under seal. (b)(6); (b)(7)(C) (b)(6); (b)(7)(C)

The (b)(6); (b)(7)(C) further informed us that the memorandum also referred to investigative work that the Department had not made public. More than a dozen other exhibits attached to the memorandum contained law enforcement sensitive information, Department attorney work product, or deliberative process information. We do not describe these exhibits in detail here, but we note that they included internal Department emails discussing work on and strategy in the (b)(6); (b)(7)(C) internal Department emails discussing settlement and a non-prosecution agreement in a different matter, and a draft plea agreement for a cooperating witness in the (b)(6); (b)(7)(C) (b)(6); (b)(7)(C)

We next discuss the grand jury information in (b)(6); (b)(7)(C) memorandum.

1. Grand Jury Information in the Memorandum

Throughout the memorandum, (b)(6); (b)(7)(C) referred to a (b)(6); (b)(7)(C) related to (b)(6); (b)(7)(C) and in which the indictment was under seal as to all defendants on (b)(6); (b)(7)(C) The lead defendant in that case is (b)(6); (b)(7)(C) and in his memorandum (b)(6); (b)(7)(C) referred to the case variously as (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) individuals had been charged under seal in (b)(6); (b)(7)(C)

On (b)(6); (b)(7)(C) the Department filed a motion to seal the (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) signed the motion, in which the Department argued (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) The same day, the court entered an order sealing the indictment and the other documents the Department had requested.

(b)(6); (b)(7)(C) indictment was unsealed as to (b)(6); (b)(7)(C), but it was not unsealed as to all remaining defendants, including (b)(6); (b)(7)(C) until (b)(6); (b)(7)(C) At that time, a superseding indictment that had been filed under seal (b)(6); (b)(7)(C) was fully unsealed. Thus, (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) the version of the memorandum (b)(6); (b)(7)(C) contained grand jury information that had been sealed by the court.

(b)(6); (b)(7)(C)

2. Grand Jury Information in Two Exhibits to the Memorandum

One exhibit, a document titled (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) the indictment in (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) Although it did not mention (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) or any other defendant by name, it identified the relevant (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e)

(b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e)

(b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) As discussed above, the superseding indictment against (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) was not fully unsealed until (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e). The exhibit also described the fact that the Department was preparing a (b)(5); (b)(6); (b)(7)(C)

(b)(5); (b)(6); (b)(7)(C)

A second exhibit to the (b)(6); (b)(7)(C) memorandum discussed (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e)

(b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) (b)(5); (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e)

(b)(5); (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e)

(b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) (b)(5); (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e)

(b)(5); (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e)

(b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) As discussed above, the superseding indictment against (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) including one named in this email, was not fully unsealed until (b)(5); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e)

In the second exhibit, (b)(6); (b)(7)(C) also (b)(5); (b)(6); (b)(7)(C)

(b)(5); (b)(6); (b)(7)(C)

3. Court-Sealed Information in One Exhibit to the Memorandum

On (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) (b)(6); (b)(7)(C) filed a motion in the (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) (b)(6); (b)(7)(C) the Department's response to (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e)

(b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e)

(b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) He also filed on the public docket a redacted version of the Department's response. The court sealed the unredacted version of the Department's response, as requested by (b)(6); (b)(7)(C) One of the

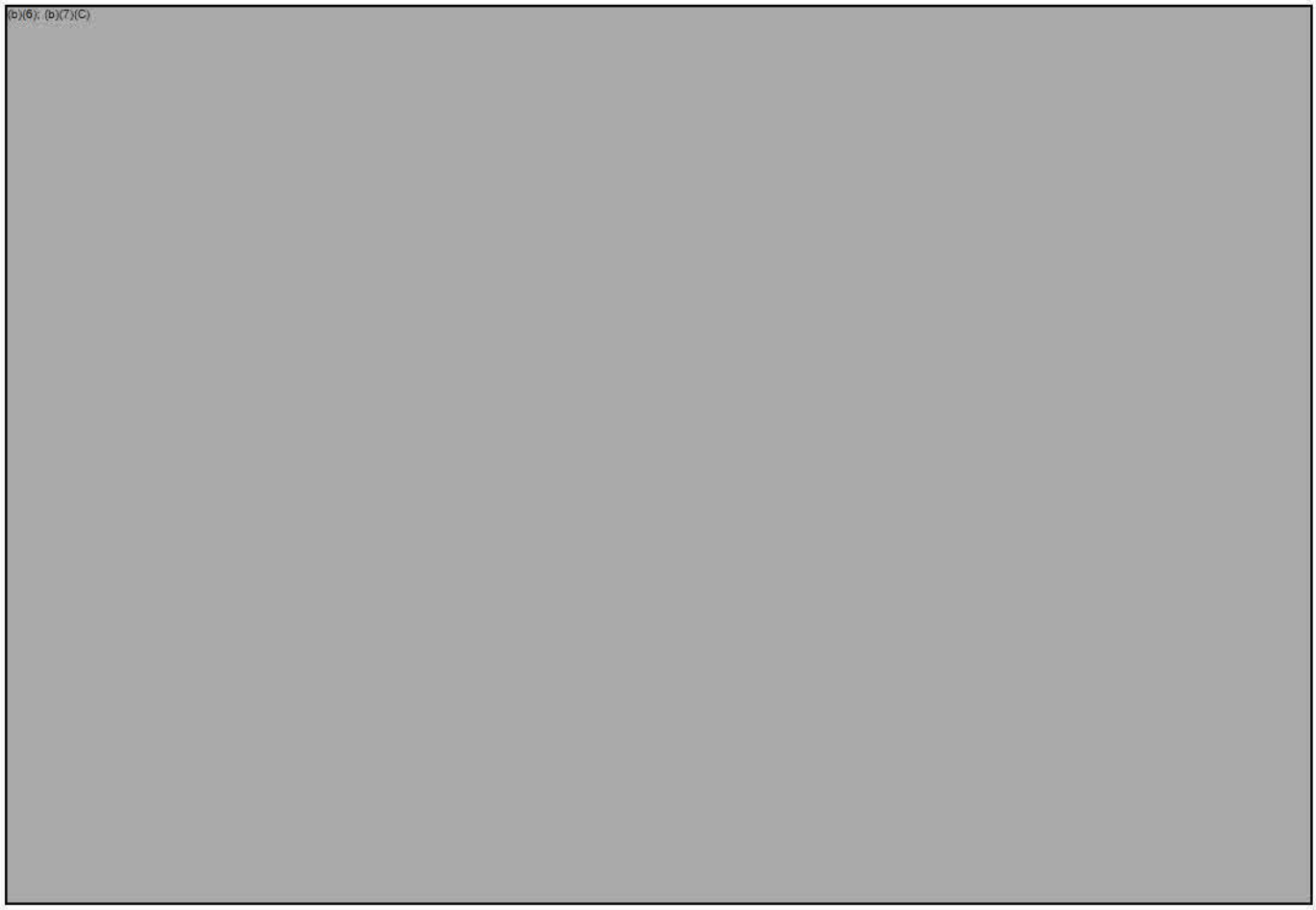
---

28 (b)(5); (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

exhibits that (b)(6); (b)(7)(C) attached to his (b)(6); (b)(7)(C) memorandum was an unredacted version of the Department's filing.[29]

(b)(6); (b)(7)(C)



E. (b)(6); (b)(7)(C) Sends to his Personal Email Account the Final Version and Drafts of his 72-Page Memorandum, as well as Zip Files Containing the Exhibits to the Memorandum—(b)(6); (b)(7)(C)

Our investigation showed that from (b)(6); (b)(7)(C) sent from his DOJ email account to his personal email account three drafts of the (b)(6); (b)(7)(C) memorandum and two zip files containing his potential exhibits. On (b)(6); (b)(7)(C) also from his DOJ email account, (b)(6); (b)(7)(C) sent to his personal email account the final version of his memorandum and a zip file containing the final exhibits. (b)(6); (b)(7)(C) password-protected each of the three

29 (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)

zip files of exhibits; he did not password-protect the draft or final versions of the memorandum.[30]

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

[redacted]

30 (b)(6); (b)(7)(C) attorney proffered that (b)(6); (b)(7)(C) sent these documents to his personal email account to work on the memorandum on his own time, share materials with his attorney in a privileged manner, and print documents on his own time and at his own expense. However, because (b)(6); (b)(7)(C) had a DOJ-issued laptop that he could take home, he could have worked on the (b)(6); (b)(7)(C) memorandum on his own time without removing the memorandum or its exhibits from the DOJ network. Additionally, because (b)(6); (b)(7)(C) was preparing the memorandum (b)(6); (b)(7)(C) it would have been appropriate for (b)(6); (b)(7)(C) to print the memorandum and exhibits from a DOJ-networked printer, at the Department's expense. Finally, because the memorandum and two of its exhibits contained grand jury information, Rule 6(e) prohibited (b)(6); (b)(7)(C) from sharing with his attorney the two exhibits and the portions of the memorandum that contained the grand jury information.

Withheld pursuant to exemption

(b)(6) ; (b)(7)(C)

of the Freedom of Information and Privacy Act

Withheld pursuant to exemption

(b)(6) ; (b)(7)(C)

of the Freedom of Information and Privacy Act

(b)(6); (b)(7)(C)

I. (b)(6); (b)(7)(C) Copies a DOJ Document Containing Grand Jury Information to a Removable Media Device and Accesses a Shortened and Redacted Version of His 72-Page Memorandum–(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) had a single government-issued laptop computer that he used both in and outside of his DOJ office. The OIG's forensic analysis of (b)(6); (b)(7)(C) DOJ laptop showed that on (b)(6); (b)(7)(C) laptop was used to log into the DOJ networked system using (b)(6); (b)(7)(C) Department user credentials and that documents related to the (b)(6); (b)(7)(C) and drafts and the final version of the (b)(6); (b)(7)(C) memorandum were accessed. The forensic analysis further showed that on at least (b)(6); (b)(7)(C) the laptop was used to copy documents to a removable media device.

The OIG concluded that (b)(6); (b)(7)(C) was the individual who accessed and copied these records to removable media devices based on the fact that the individual who accessed these documents used (b)(6); (b)(7)(C) laptop, credentials, and password to do so; and we found no information to suggest that someone else had access to and used (b)(6); (b)(7)(C) laptop, credentials, and password.

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C), as noted earlier, DOJ records reflect that in (b)(6); (b)(7)(C) sent from his DOJ email account to his personal email account drafts of the (b)(6); (b)(7)(C) memorandum and zip files containing its potential exhibits. As noted above, we did not seek (b)(6); (b)(7)(C) personal email records, (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) As noted above, (b)(6); (b)(7)(C) attorney proffered to the OIG that (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

The following summarizes the findings of the OIG's forensic analysis for (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) We discuss (b)(6); (b)(7)(C) use of a removable media device on (b)(6); (b)(7)(C) in Section III.L below.

1. (b)(6); (b)(7)(C)

The OIG determined that on (b)(6); (b)(7)(C) logged onto the DOJ networked system from his DOJ laptop at 2:00 p.m. and connected a removable media device approximately 15 seconds later. While the device was connected, (b)(6); (b)(7)(C) copied to it, at a minimum, a redacted copy of the (b)(6); (b)(7)(C) which was one of the exhibits to the (b)(6); (b)(7)(C) memorandum that contained grand jury information.[33] Notwithstanding the redactions, this version of the document included grand jury information. Although it did not mention (b)(6); (b)(7)(C) or any other defendant by name, the redacted version of the (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

(b)(5); (b)(7)(C) removed the media device from his laptop at 2:03 p.m. and logged off approximately 12 seconds later. (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

2. (b)(6); (b)(7)(C)

The OIG determined that on the same day as (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) logged onto the DOJ networked system. Between 11:07 and 11:58 a.m., he browsed several files related to the (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

[33] Our forensic analysis identified several digital artifacts relating to (b)(6); (b)(7)(C) accessing files on and copying files to removable media devices. Certain artifacts are created when a user opens a file on the local drive, removable media device, or mapped network drive. Additional artifacts are created when a user moves, copies, or renames a file. For (b)(6); (b)(7)(C) our analysis indicates that (b)(6); (b)(7)(C) accessed a particular document on an external removable media device that was connected to (b)(6); (b)(7)(C) DOJ laptop. A document with the identical filename (b)(6); (b)(7)(C) was found on (b)(6); (b)(7)(C) desktop.

(b)(6); (b)(7)(C) accessed files on the DOJ network, including files related to (b)(6); (b)(7)(C) As we describe below, we determined that on (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) copied these documents to a removable media device that was connected to his DOJ laptop.

One of the documents that (b)(6); (b)(7)(C) accessed was an abbreviated 36-page version of his (b)(6); (b)(7)(C) memorandum, which was significantly redacted on multiple pages.[34] The redactions include redactions of page numbers and exhibit numbers, most of the title of the memorandum, and some section headings. (b)(6); (b)(7)(C)

The document refers in three places to (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e)

[34] Our forensic analysis does not show when this version of the (b)(6); (b)(7)(C) memorandum was created.

In the shortened and redacted version of [redacted] memorandum [redacted] section begins on page 7 and ends on page 12.[35] The reference to [redacted] in that section appears on page 11, in a discussion of the draft response to [redacted]

At the top of page 10, [redacted] The reference to [redacted] proceeding appears as part of that discussion. [redacted]

The second and third references to [redacted] proceeding occur in a section on [redacted] In the second reference, [redacted] noted that the [redacted] As discussed above, the references [redacted] were grand jury information under Rule 6(e) until the indictment was fully unsealed in [redacted] None of the other references to grand jury information in the 72-page [redacted] memorandum were included in the shortened and redacted version.

[redacted]

[35] As noted above, page numbers have been redacted from the shortened and redacted version of the memorandum. The numbers we describe here as page numbers refer to the position of each page within the document.

Withheld pursuant to exemption

(b)(6) ; (b)(7)(C)

of the Freedom of Information and Privacy Act

Withheld pursuant to exemption

(b)(6) ; (b)(7)(C)

of the Freedom of Information and Privacy Act

Withheld pursuant to exemption

(b)(6) ; (b)(7)(C)

of the Freedom of Information and Privacy Act

(b)(6); (b)(7)(C)

L. (b)(6); (b)(7)(C) Copies Additional DOJ Documents to a Removable Media Device—(b)(6); (b)(7)(C)

The OIG determined that on (b)(6); (b)(7)(C) logged onto the DOJ networked system at 7:22 a.m. At 7:34 a.m., he connected a removable media device to the system. (b)(6); (b)(7)(C) then accessed many folders and files on the DOJ network, and copied at least some of them to the removable media device. Many of the documents that were accessed and copied had been saved to the DOJ networked system in folders named "Personal."

Among the documents that (b)(6); (b)(7)(C) copied were interim drafts and the final, 72-page version of his (b)(6); (b)(7)(C) memorandum, the final exhibits to his memorandum, (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) and the documents, described above, that he had accessed on (b)(6); (b)(7)(C) removed the media device at approximately 8:10 a.m. (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

Withheld pursuant to exemption

(b)(6) ; (b)(7)(C)

of the Freedom of Information and Privacy Act

Withheld pursuant to exemption

(b)(6) ; (b)(7)(C)

of the Freedom of Information and Privacy Act

(b)(6); (b)(7)(C)

O. Superseding (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) Indictment is Fully Unsealed– (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e)

In (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) the superseding indictment against (b)(6); (b)(7)(C); (b)(3):Fed. R. and all remaining co-defendants was fully unsealed. (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) (b)(6); (b)(7)(C)

P. (b)(6); (b)(7)(C) Resigns from the Department, and Refuses to Return Documents to the Department– (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) resigned from the Department.

On (b)(6); (b)(7)(C) the Department provided (b)(6); (b)(7)(C) with paperwork the Criminal Division typically provides to departing employees. It included an "Exit Clearance Form," and a copy of the Department policy on the removal of and access to Department of Justice information described in Section II.B.3 above (DOJ Policy Statement 801.02). The Exit Clearance Form included the following language, followed by a signature block for (b)(6); (b)(7)(C) to sign.

> I certify that I have reviewed and understand the Memorandum regarding removal of documents and that I am removing from the Department of Justice no documents expressly prohibited from removal in paragraph 1.a of DOJ Policy Statement 0801.02 and that I have obtained the required written approval specified in paragraph 2 of that Policy Statement for the removal of any other non-public documentation.

On (b)(6); (b)(7)(C) sent an email to (b)(6); (b)(7)(C) concerning the "post-employment document retention restrictions" that (b)(6); (b)(7)(C) had received as part of his exit package. (b)(6); (b)(7)(C) wrote, (b)(6); (b)(7)(C) (b)(6); (b)(7)(C), including matters pending before the Office of the Inspector General. As a result, it's my intention to maintain copies of documents that I believe may be relevant to those proceedings." (b)(6); (b)(7)(C) wrote that he intended to proceed in that manner unless he heard otherwise from the OIG or received guidance from a Department official outside the (b)(6); (b)(7)(C)

---

39 (b)(6); (b)(7)(C) (b)(6); (b)(7)(C)

On [redacted] sent [redacted] a memorandum for departing Criminal Division employees titled "Removal of Records" that walked through the steps a departing employee needed to take to request permission to remove copies of documents that the employee originated, reviewed, or signed. She told [redacted] that he should submit any request in connection with this policy to an acting Deputy Assistant Attorney General (DAAG) in the Criminal Division.

On [redacted] sent an email to the DAAG in which he repeated the substance of his email to [redacted] On [redacted] the DAAG responded to [redacted] email. The DAAG attached to his email a copy of the "Removal of Records" memorandum and explained its requirements. The DAAG asked [redacted] to confirm no later than [redacted] whether [redacted] had—as [redacted] email indicated—removed or retained any materials upon his departure from the Criminal Division.

The DAAG instructed [redacted] that if he had removed or retained any materials, that [redacted] provide him with a copy of the materials and a log describing them so that the Department could determine whether any materials [redacted] retained fall within the policy. The DAAG further instructed that to the extent [redacted] had retained documents that fall within the policy, those materials would need to be returned to the Department immediately and any copies destroyed. The DAAG informed [redacted] that once the Department had determined whether [redacted] had removed or retained any documentary materials, and once [redacted] had returned all such materials and confirmed that he had destroyed copies and had not disseminated them to third parties, the Department could then consider [redacted] request to retain copies of documentary materials pursuant to the policy. [redacted] did not respond to the DAAG's email, and he did not return any documents to the [redacted]

[redacted]

Withheld pursuant to exemption

(b)(6) ; (b)(7)(C)

of the Freedom of Information and Privacy Act

(b)(6); (b)(7)(C)

IV. OIG Analysis

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) Thereafter, we analyze his actions in connection with emailing government records, including documents containing grand jury information, to his personal email account and retaining government records when he resigned from the Department.

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) ," did not
(b)(6); (b)(7)(C) (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) (b)(6); (b)(7)(C) (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
(b)(6); (b)(7)(C) (b)(6); (b)(7)(C); (b)(3):Fed. R. (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
(b)(6); (b)(7)(C) (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e) (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C) (b)(6); (b)(7)(C); (b)(3):Fed. R. Crim. P. (6)(e)
(b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)

Withheld pursuant to exemption

(b)(6) ; (b)(7)(C)

of the Freedom of Information and Privacy Act

Withheld pursuant to exemption

(b)(6) ; (b)(7)(C)

of the Freedom of Information and Privacy Act

(b)(6); (b)(7)(C)

C. (b)(6); (b)(7)(C) Sent Government Records, Including Documents Containing Grand Jury Information, to His Personal Email Account in Violation of Department Policy and Rules of Behavior

We found that the interim drafts and final versions of (b)(6); (b)(7)(C) 72-page (b)(6); (b)(7)(C) memorandum and the zip files of exhibits to the memorandum that (b)(6); (b)(7)(C) emailed to his personal email account were government records.[45] By definition, federal records include "all recorded information, regardless of form or characteristics, made or received by a Federal agency…in connection with the transaction of public business."[46] Under Department policy, federal records include "[e]mail containing content that is evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Department."[47]

The information that (b)(6); (b)(7)(C) included in the (b)(6); (b)(7)(C) memorandum and its exhibits is information that he obtained in the course of his official duties—much of it in connection with his work (b)(6); (b)(7)(C) had access to this information solely because of his work as a federal prosecutor. In addition, many of the exhibits to the memorandum constitute or reflect non-public non-prosecution agreements, settlement discussions, communications with defense counsel, draft court filings, and internal Department discussions of investigative matters. Additionally, the memorandum and two of its exhibits contained grand jury information. All of this information is directly tied to the Department's investigative and prosecutorial activities.

We found that (b)(6); (b)(7)(C) violated Department policy and Rules of Behavior regarding the use of non-official email accounts when he emailed to his personal email account drafts and the final version of his (b)(6); (b)(7)(C) memorandum and its exhibits, including the two

---

45 (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)

46 44 U.S.C. § 3301(a)(1)(A).

47 DOJ Policy Statement 0801.04, Electronic Mail and Electronic Messaging Records Retention, § II.A.

exhibits containing grand jury information.[48] The grand jury information that [redacted] included in the [redacted] memorandum and two of its exhibits is information that he obtained in the course of his official duties in connection with his work [redacted] had access to the grand jury information solely because of his work as a federal prosecutor; the information is business-related because it is tied directly to the Department's investigative and prosecutorial activities.

The Department policy on the retention of email records requires all Department employees to use only approved email accounts to send and receive DOJ business-related communications. The Rules of Behavior prohibit Department employees from using personal email accounts for DOJ business except under exigent circumstances. In our investigation, we did not find that exigent circumstances existed that may have justified his sending these documents, including documents containing grand jury information, to his personal email account.

[redacted]

D. [redacted] Retained Government Records Without Authorization, in Violation of Department Policy

We found that [redacted] violated Department policy regarding the removal of government records when he failed to return the documents he had copied to removable media devices in [redacted] and the draft and final versions of his [redacted] memorandum and its exhibits that he had emailed to his personal email account on [redacted] [redacted][49] Under Department of Justice Policy Statement 0801.02, Removal of and Access to Department of Justice Information, the Department "owns the records and

---

[48] [redacted]

[49] Although [redacted] copied documents to the removable media devices from folders he had labeled as "Personal," given the contents of the documents, any assertion that the documents were personal documents rather than government records would not be reasonable.

information...captured, created, or received during the conduct of official business."[50] A Department employee who wants to retain Department records or information after his employment ends must make a written request, receive approval from the appropriate official, and execute a nondisclosure agreement.[51]

(b)(6); (b)(7)(C) informed Criminal Division leadership that it was "[his] intention to maintain copies of documents" that he believed could be relevant to (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) In response, Criminal Division leadership informed (b)(6); (b)(7)(C) of the steps he was required to follow to obtain authorization to retain the documents. (b)(6); (b)(7)(C) did not seek to obtain authorization, nor did he return any documents to the Department. Based upon the foregoing, we concluded that (b)(6); (b)(7)(C) violated Department policy.

V. Conclusion

(b)(6); (b)(7)(C)
(b)(6); (b)(7)(C) we concluded that both the original and shortened and redacted versions of, and two exhibits to, (b)(6); (b)(7)(C) memorandum contained grand jury information, (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)

We concluded that (b)(6); (b)(7)(C) did commit administrative misconduct when he (1) emailed government records, including documents containing grand jury information, to his personal email account in violation of Department policy and Rules of Behavior related to the use of non-official email, and (2) refused to return to the Department certain DOJ records following his resignation from DOJ in violation of Department policy pertaining to the handling and retention of government records and information. (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)

---

[50] DOJ Policy Statement 0801.02, § I. The only items that departing employees may remove without Department permission are "[p]ersonal materials or information, in any format, that is not related to the business of the Department," copies of any unclassified information that has officially been made public; and a copy of the employee's email contacts. *Id.* With the exception of the publicly-filed court pleadings and published court orders, the documents (b)(6); (b)(7)(C) emailed himself and copied to a removable media device were not within any of these categories.

[51] DOJ Policy Statement 0801.02, § II.A.