

Exhibit 7

Ballard Spahr LLP

1909 K Street, NW
12th Floor
Washington, DC 20006-1157
TEL 202.661.2200
FAX 202.661.2299
www.ballardspahr.com

Charles D. Tobin
Tel: 202.661.2218
Fax: 202.661.2299
tobinc@ballardspahr.com

March 3, 2023

Via FOIA STAR and FedEx

Bobak Talebian
Director, Office of Information Policy
Department of Justice
441 G Street NW
Washington, DC 20530

Re: Freedom of Information Act Appeal – FBI Request No. 1584620-000

Dear Mr. Talebian:

This firm represents 12 news organizations (the “Press Coalition”)¹ with respect to the above-referenced Freedom of Information Act (“FOIA”) request, made to the Federal Bureau of Investigation (“FBI”) on February 24, 2023. The FOIA request seeks copies of all closed-circuit camera footage recorded on January 6, 2021, inside the United States Capitol and on its surrounding outside grounds, on Capitol surveillance cameras (the “CCTV videos”). The FOIA request is attached as Exhibit A.

Pursuant to 5 U.S.C. § 552 and 28 C.F.R. § 16.8, the Press Coalition appeals the FBI’s March 2, 2023 response to that request, in which the FBI stated that it “conducted a search of the places reasonably expected to have records” but was “unable to identify records subject to [FOIA] that are responsive to [the] request.” A copy of the FBI’s response is attached as Exhibit B.

For multiple reasons, it defies belief that the FBI would be unable to locate any CCTV videos from “the most significant assault on the Capitol since the War of 1812.” *Trump v. Thompson*, 20 F.4th 10, 18-19 (D.C. Cir. 2021). **First**, the Department of Justice has made it clear that the FBI is leading the investigation into the Capitol riot in partnership with federal prosecutors in the District. *See 25 Months Since the Jan. 6 Attack on the*

¹ The Press Coalition consists of Advance Publications, Inc., American Broadcasting Companies, Inc. d/b/a ABC News, The Associated Press, Axios Media Inc., Cable News Network, Inc., CBS Broadcasting Inc. o/b/o CBS News, The E.W. Scripps Company, Gannett Co., Inc., Los Angeles Times Communications LLC, The New York Times Company, POLITICO LLC, and Pro Publica, Inc.

Mr. Talebian
FOIA Appeal – FBI Request No. 1584620-000
Page 2

Capitol (Feb. 7, 2023), <https://www.justice.gov/usao-dc/25-months-jan-6-attack-capitol> (“Under the continued leadership of the U.S. Attorney’s Office for the District of Columbia and the FBI’s Washington Field Office, the investigation and prosecution of those responsible for the attack continues to move forward at an unprecedented speed and scale.”).

Second, the Department of Justice has represented in court that “voluminous materials accumulated by the government in the Capitol Breach investigation thus far include . . . *[s]urveillance footage, including but not limited to more than 14,000 hours of camera footage from the U.S. Capitol Police’s extensive system of cameras on U.S. Capitol grounds.*” See Mot. to Authorize the Disclosure of Grand Jury Materials at 2, *In re Capitol Breach Grand Jury Investigations Within the District of Columbia*, No. 21-gj-20 (D.D.C. June 30, 2021), ECF No. 1 (emphasis added). A copy of the Motion containing that representation is attached as Exhibit C.

Third, as part of its continuing efforts to identify rioters, the FBI has published several videos that clearly include footage from January 6, 2021, taken from Capitol surveillance cameras. See Office of Public Affairs, *FBI Washington Field Office Releases Videos of Assaults on Officers at U.S. Capitol, Seeks Public’s Help to Identify Suspects*, FBI (Mar. 18, 2021), <https://www.fbi.gov/contact-us/field-offices/washingtondc/news/press-releases/fbi-washington-field-office-releases-videos-of-assaults-on-officers-at-us-capitol-seeks-publics-help-to-identify-suspects-031821>. The “AFO #91” video, for example, includes stationary surveillance footage from inside the Lower West Terrace. See <https://www.fbi.gov/video-repository/capitol-violence-91-af0-010621.mp4/view> at 0:29 – 0:39. The “AOM #174 and 175” video likewise consists of stationary surveillance footage from above a staircase within the Capitol building. See <https://www.fbi.gov/video-repository/bolo174-175.mp4/view>.

In light of the foregoing, we insist that your office direct the FBI to immediately conduct a proper search for the requested CCTV videos. We look forward to your prompt response to this appeal within 20 working days, and in any event no later than the close of business on March 31, 2023. See 5 U.S.C. § 552(a)(6)(A)(ii). Please do not hesitate to contact us in the interim if you would like to discuss the request or this appeal or the logistics of accessing the CCTV video.

Sincerely,



Charles D. Tobin
Maxwell S. Mishkin
Lauren Russell

cc: Honorable Merrick B. Garland, Attorney General of the United States

Exhibit A

Ballard Spahr LLP

1909 K Street, NW
12th Floor
Washington, DC 20006-1157
TEL 202.661.2200
FAX 202.661.2299
www.ballardspahr.com

Charles D. Tobin
Tel: 202.661.2218
Fax: 202.661.2299
tobinc@ballardspahr.com

February 24, 2023

Via FedEx, Email and eFOIA Portal

Arla Witte-Simpson
FOIA Public Liaison
Executive Office for U.S. Attorneys
Department of Justice
175 N Street NE, Suite 5.400
Washington, DC 20530
usaeo.foia.requests@usdoj.gov

Michael G. Seidel, Section Chief
Record/Information Dissemination Section
Records Management Division
Federal Bureau of Investigation
200 Constitution Drive
Winchester, VA 22602
<https://efoia.fbi.gov>

Re: EXPEDITED FOIA Request for January 6, 2021 Capitol Surveillance Video

Dear Ms. Witte-Simpson and Mr. Seidel:

Pursuant to the Freedom of Information Act, 5 U.S.C. § 552 *et seq.*, (“FOIA”) and on behalf of 12 news organizations (the “Press Coalition”),¹ we request copies of all closed-circuit camera footage recorded on January 6, 2021, inside the United States Capitol and on its surrounding outside grounds, on Capitol surveillance cameras (the “CCTV videos”).

No exemption to the FOIA would justify withholding any portion of these records. Indeed, during the February 20, 2023 episode of “Tucker Carlson Tonight,” Fox News host Tucker Carlson announced that he and his colleagues have received “unfettered” access to “44,000 hours” of Capitol surveillance footage and will soon begin reporting on that footage. The Speaker of the House of Representatives, Kevin McCarthy, provided the footage to Mr. Carlson. *See, e.g.,* Annie Grayer et al., *McCarthy gives Tucker Carlson access to January 6 Capitol security footage, sources say*, CNN (Feb. 21, 2023), <https://www.cnn.com/2023/02/20/politics/kevin-mccarthy-tucker-carlson-january-6-footage/index.html>. Therefore, we expect that your offices will provide access to these records promptly, without any claims of exemptions and without redactions.

¹ The Press Coalition consists of Advance Publications, Inc., American Broadcasting Companies, Inc. d/b/a ABC News, The Associated Press, Axios Media Inc., Cable News Network, Inc., CBS Broadcasting Inc. o/b/o CBS News, The E.W. Scripps Company, Gannett Co., Inc., Los Angeles Times Communications LLC, The New York Times Company, POLITICO LLC, and Pro Publica, Inc.

Ms. Witte-Simpson & Mr. Seidel
EXPEDITED FOIA Request
Page 2

Moreover, as the Speaker provided access to these public records in his official capacity, following the conclusion of the House Select Committee to Investigate the January 6th Attack on the United States Capitol's review of these materials, the United States has "officially" disclosed these records. For this additional reason, the Government may not withhold them under the FOIA. *See Wolf v. CIA*, 473 F.3d 370, 378 (D.C. Cir. 2007).

As you may know, the Honorable Beryl A. Howell, Chief Judge of the U.S. District Court for the District of Columbia, has previously granted the Press Coalition's application for access to Capitol CCTV footage, noting that "the areas of the Capitol in [those] videos are generally open to visitors taking public tours," and that any asserted security risk was "undercut by the already extensive release of [CCTV] footage from the Capitol." *United States v. Torrens*, 560 F. Supp. 3d 283, 294 (D.D.C. 2021). Since the Chief Judge issued that decision in September 2021, the Court has, without incident, released hundreds more CCTV videos to the press and public. *Video Evidence Shown in the Capitol Insurrection Criminal Cases*, ProPublica (July 27, 2021), <https://projects.propublica.org/jan-6-video-evidence/> (compiling videos provided to the Press Coalition by orders of the Court).

The Press Coalition requests expedited processing of this request pursuant to 5 U.S.C. § 552(a)(6)(E)(i). There is an urgent need for these CCTV videos – which are of the highest public interest – to be viewed by the Press Coalition given that the newsworthiness of the records is fleeting, and the public should have an opportunity to read and view reporting about the CCTV videos from different news organizations contemporaneously. The public benefits from different perspectives on these important issues and should not have to rely on a single news outlet for information about the CCTV videos. I certify that this information in support of our request for expediting is true and correct to the best of my knowledge. *See Al-Fayed v. CIA*, 254 F.3d 300, 310-11 (D.C. Cir. 2001); *Bloomberg, L.P. v. FDA*, 500 F. Supp. 2d 371, 378 (S.D.N.Y. 2007).

The Press Coalition qualifies for news media fee status under 5 U.S.C. § 552(a)(4)(A)(ii)(II) and may not be charged for search and review fees. Because this footage will be used by the Press Coalition for the preparation of news reporting that will be broadly disseminated to the general public, it will contribute significantly to public understanding of the operations or activities of the government and is not primarily in the Press Coalition's commercial interest. As such, please grant a fee waiver for any remaining fees incurred, and please notify me before incurring over \$500 in fees.

We look forward to your prompt response regarding expedition of this request within 10 days, and in any event by no later than March 6, 2023. 5 U.S.C. § 552(a)(6)(E)(ii). We hope that your agencies will not force the Press Coalition to file a lawsuit to secure the release of these public records. Please be advised, however, that if you should refuse to

Ms. Witte-Simpson & Mr. Seidel
EXPEDITED FOIA Request
Page 3

produce these videos for any reason, the Press Coalition has authorized us to file a lawsuit immediately in the U.S. District Court for the District of Columbia.

If you would like to discuss this request or the logistics of accessing the CCTV video, please do not hesitate to contact me at tobinc@ballardspahr.com.

Sincerely,

A handwritten signature in blue ink, appearing to read "Charles D. Tobin".

Charles D. Tobin
Maxwell S. Mishkin
Lauren Russell

cc: Honorable Merrick B. Garland, Attorney General of the United States

Exhibit B



U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

March 2, 2023

MAXWELL S. MISHKIN
BALLARD SPAHR LLP
1909 K STREET NORTHWEST
12TH FLOOR
WASHINGTON, DC 20006

Request No.: 1584620-000
Subject: Closed- Circuit Camera Footage inside
Capital
(January 6th, 2021)

Dear Maxwell Mishkin:

This is in response to your Freedom of Information/Privacy Acts (FOIPA) request. Based on the information you provided, we conducted a search of the places reasonably expected to have records. However, we were unable to identify records subject to the FOIPA that are responsive to your request. Therefore, your request is being closed. If you have additional information pertaining to the subject of your request, please submit a new request providing the details, and we will conduct an additional search. For more information about records searches, see the enclosed FBI FOIPA Addendum General Information Section.

Please see the paragraphs below for relevant information that may be specific to your request. Only checked boxes contain corresponding paragraphs relevant to your request. If no boxes are checked, the corresponding information does not apply.

- Please be advised that your request was reopened based on the additional information you provided. A new search was conducted, and we were unable to identify records subject to the FOIPA that are responsive to your request.
- Requests for expedited processing are not applicable when a final response is issued within ten calendar days.
- You also requested information regarding one or more third parties. Please be advised the FBI will neither confirm nor deny the existence of such records pursuant to FOIA exemptions (b)(6) and (b)(7)(C), 5 U.S.C. §§ 552 (b)(6) and (b)(7)(C). The mere acknowledgement of the existence of FBI records on third party individuals could reasonably be expected to constitute an unwarranted invasion of personal privacy. This is our standard response to such requests and should not be taken to mean that records do, or do not, exist.

Please refer to the enclosed FBI FOIPA Addendum for additional standard responses applicable to your request. **“Part 1”** of the Addendum includes standard responses that apply to all requests. **“Part 2”** includes additional standard responses that apply to all requests for records about yourself or any third party individuals. **“Part 3”** includes general information about FBI records that you may find useful. Also enclosed is our Explanation of Exemptions.

For questions regarding our determinations, visit the www.fbi.gov/foia website under “Contact Us.” The FOIPA Request Number listed above has been assigned to your request. Please use this number in all correspondence concerning your request.

If you are not satisfied with the Federal Bureau of Investigation’s determination in response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, D.C. 20530, or you may submit an appeal through OIP’s FOIA STAR portal by creating an account following the instructions on OIP’s website: <https://www.justice.gov/oip/submit-and-track-request-or-appeal>. Your appeal must be postmarked or electronically transmitted within ninety (90) days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked “Freedom of Information Act Appeal.” Please cite the FOIPA Request Number assigned to your request so it may be easily identified.

You may seek dispute resolution services by emailing the FBI's FOIA Public Liaison at foipaquestions@fbi.gov. The subject heading should clearly state "Dispute Resolution Services." Please also cite the FOIPA Request Number assigned to your request so it may be easily identified. You may also contact the Office of Government Information Services (OGIS). The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Sincerely,

A handwritten signature in black ink, appearing to read "M. G. Seidel".

Michael G. Seidel
Section Chief
Record/Information
Dissemination Section
Information Management Division

FBI FOIPA Addendum

As referenced in our letter responding to your Freedom of Information/Privacy Acts (FOIPA) request, the FBI FOIPA Addendum provides information applicable to your request. Part 1 of the Addendum includes standard responses that apply to all requests. Part 2 includes standard responses that apply to requests for records about individuals to the extent your request seeks the listed information. Part 3 includes general information about FBI records, searches, and programs.

Part 1: The standard responses below apply to all requests:

- (i) **5 U.S.C. § 552(c).** Congress excluded three categories of law enforcement and national security records from the requirements of the FOIPA [5 U.S.C. § 552(c)]. FBI responses are limited to those records subject to the requirements of the FOIPA. Additional information about the FBI and the FOIPA can be found on the www.fbi.gov/foia website.
- (ii) **Intelligence Records.** To the extent your request seeks records of intelligence sources, methods, or activities, the FBI can neither confirm nor deny the existence of records pursuant to FOIA exemptions (b)(1), (b)(3), and as applicable to requests for records about individuals, PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(1), (b)(3), and (j)(2)]. The mere acknowledgment of the existence or nonexistence of such records is itself a classified fact protected by FOIA exemption (b)(1) and/or would reveal intelligence sources, methods, or activities protected by exemption (b)(3) [50 USC § 3024(i)(1)]. This is a standard response and should not be read to indicate that any such records do or do not exist.

Part 2: The standard responses below apply to all requests for records on individuals:

- (i) **Requests for Records about any Individual—Watch Lists.** The FBI can neither confirm nor deny the existence of any individual's name on a watch list pursuant to FOIA exemption (b)(7)(E) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (j)(2)]. This is a standard response and should not be read to indicate that watch list records do or do not exist.
- (ii) **Requests for Records about any Individual—Witness Security Program Records.** The FBI can neither confirm nor deny the existence of records which could identify any participant in the Witness Security Program pursuant to FOIA exemption (b)(3) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(3), 18 U.S.C. 3521, and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.
- (iii) **Requests for Confidential Informant Records.** The FBI can neither confirm nor deny the existence of confidential informant records pursuant to FOIA exemptions (b)(7)(D), (b)(7)(E), and (b)(7)(F) [5 U.S.C. §§ 552 (b)(7)(D), (b)(7)(E), and (b)(7)(F)] and Privacy Act exemption (j)(2) [5 U.S.C. § 552a (j)(2)]. The mere acknowledgment of the existence or nonexistence of such records would reveal confidential informant identities and information, expose law enforcement techniques, and endanger the life or physical safety of individuals. This is a standard response and should not be read to indicate that such records do or do not exist.

Part 3: General Information:

- (i) **Record Searches and Standard Search Policy.** The Record/Information Dissemination Section (RIDS) searches for reasonably described records by searching systems, such as the Central Records System (CRS), or locations where responsive records would reasonably be found. The CRS is an extensive system of records consisting of applicant, investigative, intelligence, personnel, administrative, and general files compiled by the FBI per its law enforcement, intelligence, and administrative functions. The CRS spans the entire FBI organization, comprising records of FBI Headquarters, FBI Field Offices, and FBI Legal Attaché Offices (Legats) worldwide; Electronic Surveillance (ELSUR) records are included in the CRS. The standard search policy is a search for main entity records in the CRS. Unless specifically requested, a standard search does not include a search for reference entity records, administrative records of previous FOIPA requests, or civil litigation files.
 - a. *Main Entity Records* – created for individuals or non-individuals who are the subjects or the focus of an investigation
 - b. *Reference Entity Records*- created for individuals or non-individuals who are associated with a case but are not known subjects or the focus of an investigation
- (ii) **FBI Records.** Founded in 1908, the FBI carries out a dual law enforcement and national security mission. As part of this dual mission, the FBI creates and maintains records on various subjects; however, the FBI does not maintain records on every person, subject, or entity.
- (iii) **Foreseeable Harm Standard.** As amended in 2016, the Freedom of Information Act provides that a federal agency may withhold responsive records only if: (1) the agency reasonably foresees that disclosure would harm an interest protected by one of the nine exemptions that FOIA enumerates, or (2) disclosure is prohibited by law (5 United States Code, Section 552(a)(8)(A)(i)). The FBI considers this foreseeable harm standard in the processing of its requests.
- (iv) **Requests for Criminal History Records or Rap Sheets.** The Criminal Justice Information Services (CJIS) Division provides Identity History Summary Checks – often referred to as a criminal history record or rap sheet. These criminal history records are not the same as material in an investigative “FBI file.” An Identity History Summary Check is a listing of information taken from fingerprint cards and documents submitted to the FBI in connection with arrests, federal employment, naturalization, or military service. For a fee, individuals can request a copy of their Identity History Summary Check. Forms and directions can be accessed at www.fbi.gov/about-us/cjis/identity-history-summary-checks. Additionally, requests can be submitted electronically at www.edo.cjis.gov. For additional information, please contact CJIS directly at (304) 625-5590.

EXPLANATION OF EXEMPTIONS**SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552**

- (b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

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

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

Exhibit C

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

IN RE:)
CAPITOL BREACH)
GRAND JURY INVESTIGATIONS WITHIN)
THE DISTRICT OF COLUMBIA)
_____)

Misc. No. Case: 1:21-gj-00020
Assigned To : Howell, Beryl A.
Assign. Date : 6/29/2021
Description: Misc.

Under Seal

MOTION TO AUTHORIZE THE DISCLOSURE OF GRAND JURY MATERIALS

The United States of America respectfully requests this Court to enter the attached proposed order authorizing the disclosure of grand jury matters to an independent contractor, Deloitte Financial Advisory Services, LLP (“Deloitte”), pursuant to Federal Rule of Criminal Procedure 6(e)(3)(A)(ii). In support of its motion, the government states as follows:

BACKGROUND

On January 6, 2021, as a Joint Session of the United States House of Representatives and the United States Senate convened to certify the vote of the Electoral College of the 2020 U.S. Presidential Election, members of a large crowd that had gathered outside forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of law enforcement, as others in the crowd encouraged and assisted those acts. Thousands of individuals entered the U.S. Capitol without authority to be there. As a result, the Joint Session and the entire official proceeding of the Congress was halted until the Capitol Police, the Metropolitan Police Department, and other law enforcement agencies from the city and surrounding region were able to clear the Capitol of hundreds of unlawful occupants and ensure the safety of elected officials. This event in its entirety is hereinafter referred to as the “Capitol Breach.”

The investigation and prosecution of the Capitol Breach will be one of the largest in American history, both in terms of the number of defendants prosecuted and the nature and volume of the evidence. To date, over 500 individuals located throughout the nation have been charged

with a multitude of criminal offenses arising out of the Capitol Breach, including conspiracy, tampering with documents or proceedings, destruction and theft of government property, obstruction of law enforcement during civil disorder, assaults on law enforcement, obstruction of an official proceeding, engaging in disruptive or violent conduct in the Capitol or on Capitol grounds, and trespass.

As a result of the government's investigation, the government has collected enormous amounts of data. An illustrative list of voluminous materials accumulated by the government in the Capitol Breach investigation thus far include:

- Surveillance footage, including but not limited to more than 14,000 hours of camera footage from the U.S. Capitol Police's extensive system of cameras on U.S. Capitol grounds;
- More than 2,000 hours of body worn camera footage from multiple law enforcement agencies;
- Over 300,000 tips, including approximately 237,000 digital media tips;
- Over 2,000 digital devices;
- Information from the searches of hundreds of accounts maintained with electronic communications service providers and/or remote computing services providers;
- Over 240,000 Federal Bureau of Investigation ("FBI") investigative memoranda and attachments;
- Location history data for thousands of devices present inside the Capitol (obtained from a variety of sources including Google and multiple data aggregation companies);
- Cell tower data for thousands of devices that were inside the Capitol building during the Capitol Breach (obtained from the three major telephone companies);
- A collection of over one million Parler posts, replies, and related data, collected by the FBI from publicly accessible locations on the Internet;
- A collection over one million Parler videos and images (approximately 40 terabytes of data) scraped by an Internet user who voluntarily provided the

material to the FBI; and

- Subscriber information and two weeks of toll records for hundreds of phone numbers that were associated with a Google account identified from the first Google geofence search warrant.

As is most relevant here, the voluminous data accumulated by the United States in connection with the investigation of the Capitol Breach also includes materials that are or may be protected by Federal Rule of Criminal Procedure 6(e) (“Rule 6(e)”). Over 200 individuals have already been indicted by grand juries currently and previously empaneled in this District. Among the documents that must be processed, hosted, reviewed and produced when discoverable are transcripts and exhibits from those grand jury presentations. In addition, over 6,000 grand jury subpoenas have been issued in connection with the Capitol Breach, and thousands of documents have been returned in response, e.g., financial records, telephone records, electronic communications service provider records, and travel records.¹ As the Capitol Breach investigation is still on-going, the number of cases presented to the grand jury and the number of subpoenas for documents will only continue to grow.

¹ As a general matter, Rule 6(e) does not apply to individual subpoenaed documents that are sought only for the information they contain, rather than to reveal the direction or strategy of the grand jury investigation. *See United States v. Dynavac*, 6 F.3d at 1411-12 (citing *DiLeo v. Commissioner of Internal Revenue*, 959 F.2d 16, 19 (2d Cir. 1992)) (if a document is sought for its own sake rather than to learn what took place before the grand jury, and if its disclosure will not compromise the integrity of the grand jury process, Rule 6(e) does not prohibit its release); *In re Grand Jury Investigation*, 630 F.2d at 1000-01; *Securities and Exchange Comm'n v. Dresser Indus.*, 628 F.2d 1368, 1382-83 (D.C. Cir. 1980); *United States v. Stanford*, 589 F.2d 285, 291 (7th Cir. 1978); *United States v. Interstate Dress Carriers*, 280 F.2d 52, 54 (2d Cir. 1960); *Ferreira v. United States*, 350 F.Supp.2d 550, 559-60 (S.D.N.Y. 2004). *But see In re Grand Jury Proceedings*, 851 F.2d 860, 866 (6th Cir. 1988); *In re Grand Jury Disclosure*, 550 F. Supp. 1171, 1177 (E.D. Va. 1982) (party must show particularized need and compelling necessity in order to justify disclosure of documents subpoenaed by the grand jury).

The government recognizes, however, that the Court may view the disclosure of all documents subpoenaed in connection with the Capitol Breach, together with the subpoenas used to obtain those documents, as covered by Rule 6(e) secrecy requirements, because such a disclosure is more likely to reveal the scope or direction of the investigations arising out of the Capitol Breach. *See Fund for Constitutional Gov't v. National Archives & Records Serv.*, 656 F.2d 856, 868-70 (D.C. Cir. 1981) (Freedom of Information Act request for all documents obtained by the grand jury was properly denied by the district court because disclosure would reveal matters occurring before the grand jury).

A large volume of the information that has been collected (including the materials that are or may be protected by Rule 6(e)), consists of Electronically Stored Information (“ESI”). ESI frequently contains significant metadata that may be difficult to extract and produce if documents are not processed using specialized techniques. Metadata is information about an electronic document and can describe how, when and by whom ESI was created, accessed, modified, formatted, or collected. In the case of a document created with a word processing program, for example, metadata may include the author, date created, and date last accessed. In the case of video footage, metadata may identify the camera that was used to capture the image, or the date and time that it was captured. Metadata may also explain a document’s structural relationship to another document, e.g., by identifying a document as an attachment to an investigative memoranda.

Following the Capitol Breach, the United States Attorney’s Office for the District of Columbia (“USAO-DC”) recognized that due to the nature and volume of materials being collected, the government would need to employ software tools for both discovery review and trial preparation. The government also recognized that managing the materials would require the use of an outside contractor who could provide litigation technology support services, to include highly technical and specialized data and document processing and review capabilities.² Accordingly, the government contracted Deloitte to assist in the collection, processing, hosting, review and production of materials related to the Capitol Breach.

Deloitte is a litigation support vendor with extensive experience providing complex

² Processing, hosting, and production of the voluminous and varied materials described above, to include the preservation of significant metadata, involves highly technical considerations of the document’s source, nature, and format. For example, the optimal type of database for hosting and reviewing video footage may differ from the optimal type of database for hosting investigative memoranda. Similarly, a paper document, a word processing document, a spreadsheet with a formula, video footage from a camera, or video footage associated with a proprietary player may each require different types of processing to ensure they are captured by database keyword searches and produced with significant metadata having been preserved.

litigation technology services to various government agencies, including the Departments of Defense, Navy, Air Force, Interior, and State, in addition to the Department of Justice. The government's contract with Deloitte contains all applicable personnel and information security requirements required by the Federal Acquisition Regulations. All Deloitte employees supporting the contract are bound by a strict confidentiality agreement designed to maintain stringent privacy protocols on all materials processed at the Deloitte facility and are subjected to rigorous security background investigations. All data managed by Deloitte maintained under the contract resides in the Deloitte hosting environment, which meets the security requirements under the Federal Risk Authorization Management Program (FedRAMP) Moderate, Federal Information Security Management Act (FISMA), NIST 800-53 Rv. 4, and DoD Mission Assurance Category (MAC) II sensitive security baselines. Deloitte employees are not allowed to take case-related materials outside of their secure facility, which is managed through a digital access control system with area control and access management. Transmission of material between Deloitte and the government is subject to stringent information security protocols that entail the use of data encryption, a dual-container configuration, and other measures specially designed to ensure the security of sensitive information.

USAO-DC supervises and directs the work being performed by Deloitte under the contract. Deloitte's employees will be required to adhere to all grand jury secrecy requirements and other applicable laws, regulations, and Department of Justice policies and procedures, including maintaining properly locked and secure storage of grand jury materials, limiting access to grand jury materials, and preventing any improper disclosure of grand jury materials. If the Court grants this motion, USAO-DC will provide Deloitte a written advisement as to its obligations with respect to grand jury secrecy and will certify to this Court that it has done so, consistent with Rule 6(e)(3)(B).

In sum, Deloitte furnishes secure, complex, and highly technical services with respect to document processing and review. Deloitte's access to voluminous grand jury materials is needed to assist federal prosecutors in the performance of their duties, including document review, discovery production, and trial preparation, and Deloitte's employees will be required to adhere to all grand jury secrecy requirements.

AUTHORITY

Rule 6(e)(3)(A)(ii) of the Federal Rules of Criminal Procedure permits the disclosure of grand jury information to government personnel required to assist the prosecutors' law enforcement mission and provides, in pertinent part, as follows:

(A) Disclosure of a grand-jury matter – other than the grand jury's deliberations or any grand juror's vote – may be made to:

- ...
- (ii) any government personnel – including those of a state, state subdivision, Indian tribe, or foreign government – that an attorney for the government considers necessary to assist in performing that attorney's duty to enforce federal criminal law. . . .

While Rule 6(e)(3)(A)(ii) does not require a court-issued disclosure order, the government nonetheless seeks such an order here out of an abundance of caution, as case law is not extensive on the issue of what types of independent contractors may constitute "government personnel" within the meaning of Rule 6(e)(3)(A)(ii).

Courts have recognized that contract employees may be considered "government personnel" for purposes of Rule 6(e)(3)(A)(ii) when those employees perform necessary prosecutorial functions under government control. In *United States v. Pimental*, 380 F.3d 575 (1st Cir. 2004), for example, the court held that it was proper for a United States Attorney's Office to obtain court approval, under Rule 6(e)(3)(A)(ii), for disclosure of grand jury materials to an investigator employed by a private insurance fraud bureau, even though the investigator was a "private actor [employed by the private bureau], which investigates potential cases of insurance

fraud, is authorized and structured by Massachusetts statute, but partially run and entirely funded by insurers.” *Id.* at 578-79. The court found that such private insurance investigators fell within the “government personnel” provision, and therefore that disclosure was allowed under Rule 6(e)(3)(A)(ii). *Id.* at 596. The court also found it proper for the government to seek authorization from the court for disclosure to independent contractors and “make a functional showing” that such contractors fall within the ambit of Rule 6(e)(3)(A)(ii).

Courts in the Second and Tenth Circuits have likewise found that government contractors may be considered “government personnel” for Rule 6(e)(3)(A)(ii) purposes when they perform necessary prosecutorial functions that cannot reasonably be performed by traditional Civil Service employees and when they work under the control of government prosecutors. *United States v. Lartey*, 716 F.2d 955, 964 (2d Cir. 1983); *United States v. Anderson*, 778 F.2d 602, 605 (10th Cir. 1985). *But see In re Grand Jury Matter*, 607 F.Supp.2d 273 (D. Mass. 2009), in which the court denied the government’s motion for authority to disclose grand jury information to agents and employees of a “private consulting firm.” The court first concluded that the contractor, unlike the insurance fraud entity in *Pimental*, was not even a “quasi governmental entity” so that disclosure to it under Rule 6(e)(3)(a)(ii) was improper.

Deloitte’s employees should be viewed as “government personnel” authorized to access grand jury materials for the purpose of assisting prosecutors in the performance of their duties within the meaning of Rule 6(e)(3)(A)(ii). Deloitte’s personnel undergo similar clearance and background investigation procedures as employees at USAO-DC, and they operate under the control of attorneys who are investigating and prosecuting Capitol Breach cases. They execute confidentiality agreements and conflict-of-interest forms for each case on which they assist. Like the government contract employees in *Pimental*, *Lartey*, and *Anderson*, Deloitte contract personnel will perform highly technical litigation support and data processing services that are vital to

USAO-DC's ability to review voluminous data, produce discovery, and prepare for trial.

III. CONCLUSION

For the foregoing reasons, it is respectfully requested that this Court enter the attached proposed order permitting the disclosure of grand jury materials to Deloitte for purposes of technical litigation support and data processing services.

Submitted this _____ day of June, 2021.

CHANNING PHILLIPS
Acting United States Attorney

By: _____ /s/
Emily A. Miller
Capitol Breach Discovery Coordinator
D.C. Bar No. 462077
555 4th Street, N.W., Room 5826
Washington, D.C. 20530
202-252-6988
Emily.Miller2@usdoj.gov