UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	**CASE NO. 23-cr-00128**
v.	:	
	:	
ZACHARIAH BOULTON,	:	
	:	
Defendant.	:	

NOTICE OF FILING

For the purpose of illustrating the government's consistent and diligent efforts to produce voluminous discovery materials arising out of the breach of the United States Capitol on January 6, 2021 (the "Capitol Breach"), the government has filed status memoranda describing the efforts of the Capitol Breach Discovery Team on a regular basis since July 2021. We request that those memoranda, attached hereto and listed below, be made part of the record in this case:

1. Memorandum Regarding Status of Discovery as of July 12, 2021 (and Exhibit A);
2. Memorandum Regarding Status of Discovery as of August 23, 2021;
3. Memorandum Regarding Status of Discovery as of September 14, 2021;
4. Memorandum Regarding Status of Discovery as of October 21, 2021;
5. Memorandum Regarding Status of Discovery as of November 5, 2021; and
6. Memorandum Regarding Status of Discovery as of February 9, 2022.

Respectfully submitted,
MATTHEW M. GRAVES
United States Attorney
DC Bar No. 481052

By: /s/

Melanie Krebs-Pilotti
Antitrust Division, Detailed to USAO-DC
CA Bar No. 241484
United States Attorney's Office
601 D Street, N.W.
Washington, D.C. 20530
Telephone No. 202-870-7457
Email: melanie.krebs-pilotti2@usdoj.gov

UNITED STATES' MEMORANDUM
REGARDING STATUS OF DISCOVERY AS OF JULY 12, 2021

The United States files this memorandum for the purpose of describing the status of discovery. As an initial matter, substantial discovery has already been provided in this case. However, as set forth below, because the defendant's criminal acts took place at the same general time and location as many other charged crimes, the government's investigation into the breach of the United States Capitol on January 6, 2021 (the "Capitol Breach") has resulted in the accumulation and creation of a massive volume of data that may be relevant to many defendants. The government is diligently working to meet its unprecedented overlapping and interlocking discovery obligations by providing voluminous electronic information in the most comprehensive and useable format.

The Capitol Breach

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 for the 2020 U.S. Presidential Election, a mob stormed the U.S. Capitol by breaking doors and windows and assaulting members of law enforcement, as others in the crowd encouraged and assisted those acts. Thousands of individuals entered the U.S. Capitol and U.S. Capitol grounds without authority, halting the Joint Session and the entire official proceeding of Congress for hours until the United States Capitol Police ("USCP"), the Metropolitan Police Department ("MPD"), and other law enforcement agencies from the city and surrounding region were able to clear the Capitol of rioters and to ensure the safety of elected officials. This event in its entirety is hereinafter referred to as the "Capitol Breach."

Scope of Investigation

The investigation and prosecution of the Capitol Breach will be the largest in American history, both in terms of the number of defendants prosecuted and the nature and volume of the evidence. In the six months since the Capitol was breached, over 500 individuals located throughout the nation have been charged with a multitude of criminal offenses, including but not limited to 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. There are investigations open in 55 of the Federal Bureau of Investigation's 56 field offices.

Voluminous Materials Accumulated

The government has accumulated voluminous materials that may contain discoverable information for many, if not all, defendants. An illustrative list of materials accumulated by the government includes:

- Thousands of hours of closed circuit video ("CCV") from sources including the USCP, MPD, and United States Secret Service, and several hundred MPD Automated Traffic Enforcement camera videos;
- Footage from Cable-Satellite Public Affairs Network (C-SPAN) and other members of the press;
- Thousands of hours of body worn camera ("BWC") footage from MPD, Arlington County Police Department, Montgomery County Police Department, Fairfax County Police Department, and Virginia State Police;
- Radio transmissions, event chronologies, and, to a limited extent, Global Positioning Satellite ("GPS") records for MPD radios;
- Hundreds of thousands of tips, including at least 237,000 digital media tips;

- Location history data for thousands of devices present inside the Capitol (obtained from a variety of sources including two geofence search warrants and searches of ten data aggregation companies);
- Subscriber and toll records for hundreds of phone numbers;
- Cell tower data for thousands of devices that connected to the Capitol's interior Distributed Antenna System (DAS) during the Capitol Breach (obtained from the three major telephone companies);
- A collection of over one million Parler posts, replies, and related data;
- A collection over one million Parler videos and images (approximately 20 terabytes of data);
- Damage estimates from multiple offices of the U.S. Capitol;
- A multitude of digital devices and Stored Communication Act ("SCA") accounts; and
- Responses to grand jury subpoenas, of which over 6,000 have been issued, seeking documents such as financial records, telephone records, electronic communications service provider records, and travel records.

We are still collecting and assembling materials from the numerous entities who were involved in the response to the Breach, and we are still investigating – which means the amount of data (phones, devices, legal process, investigative memoranda) is growing.

Voluminous Legal Process and Investigative Memoranda

In addition to the materials collected, tens of thousands of documents have been generated in furtherance of the investigation, to include interviews of subjects, witnesses, tipsters and officers; investigations into allegations concerning officer conduct on January 6; source reports; evidence collection reports; evidence analysis reports; chain-of-custody documents; legal documents including preservation letters, subpoenas, 2703(d) orders, consent forms, and search warrants; and memoranda of investigative steps taken to evaluate leads or further investigations.

Interrelated Crimes and Discovery

The Capitol Breach involves thousands of individuals inside and outside the Capitol, many of whom overwhelmed and assaulted police. (According to a Washington Post analysis of the events, "the mob on the west side eventually grew to at least 9,400 people, outnumbering officers by more than 58 to one.") *See* *https://www.washingtonpost.com/investigations/interactive/2021/dc-police-records-capitol-riot/?itid=sf_visual-forensics*. The cases clearly share common facts, happening in generally the same place and at the same time. Every single person charged, at the very least, contributed to the inability of Congress to carry out the certification of our Presidential election.

These circumstances have spawned a situation with overlapping and interlocking discovery obligations. Many defendants may be captured in material that is not immediately obvious and that requires both software tools and manual work to identify, such as video and photos captured in the devices and SCA accounts of other subjects. Accordingly, the defense is generally entitled to review all video or photos of the breach whether from CCV, BWC or searches of devices and SCA accounts. Notably, we have received a number of defense requests for access to such voluminous information, and requests for the government to review the entirety of the law enforcement files related to this investigation. For example, in support of a motion to compel access to all of the footage, one such counsel stated:

> The events of January 6, 2021 were memorialized to an extent rarely, if ever, experienced within the context of federal criminal cases. The Government itself has a wealth of surveillance video footage. Virtually every attendee in and around the Capitol on January 6, 2021 personally chronicled the events using their iPhone or other similar video device. Many of the attendees posted their video on one or more social media platforms. Many held their videos close to their vests resulting in little if any publication of same. News media outlets from around the world captured video footage. Independent media representative from around the world captured video footage. Intelligence and law enforcement personnel present at the Capitol on January 6, 2021 also captured video footage of events of the day. By

> the Government's own admission, the Government has an overwhelming amount of video footage of the events of January 6, 2021. During the handlings of January 6 cases, the Government has garnered and continues to garner access to added video footage from, among other sources, the general public and the defendants themselves. ***Upon information and belief, the Government is not capable of vetting, cataloging and determining materiality of the video footage such as to ensure that disclosure of same is timely made in all cases to which the footage is material for disclosure purposes.*** The "information and belief" in this regard is a function of the undersigned counsel's personal knowledge relative to footage given to the Government, familiarity with other January 6 cases both as counsel for other January 6 defendants and as counsel familiar with other counsel representing January 6 defendants and the understanding that the footage provided to the Government does not appear to have been produced to other defendants whose cases warrant similar disclosure by the Government of material evidence. ***Defendant has requested the Government confirm whether there is a single repository for all video footage amassed relative to the events at the Capitol on January 6, 2021 and, further, has requested access to same for inspection and examination for determination of materiality and disclosure of the Government's protocol to determine materiality.***

United States v. Jacob Chansley, 21-cr-00003 (RCL) (Document No. 58)(emphasis added). Examples of additional similar discovery requests we have received in Capitol Breach cases are quoted in Exhibit A, attached hereto.

Early Establishment of Discovery Team

Shortly after the Capitol Breach, the U.S. Attorney's Office established a Capitol Breach Discovery Team to create and implement a process for the production of discovery in January 6 cases. The Discovery Team is staffed by federal prosecutors who have experience in managing complex investigations involving voluminous materials, Department of Justice experts in project management and electronic discovery management, and a lead discovery agent from the Federal Bureau of Investigation. Members of the Discovery Team consult regularly with Department of Justice subject matter experts, including Associate Deputy Attorney General and National Criminal Discovery Coordinator Andrew Goldsmith. As discussed further below, members of

the Discovery Team also meet and confer on a regular basis with Federal Public Defender ("FPD") leadership and electronic discovery experts.

Recognition of Need for Vendor Promptly Addressed

Following the Capitol Breach, the United States recognized that due to the nature and volume of materials being collected, the government 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. The government drafted a statement of work, solicited bids, evaluated them, and selected a vendor. This was an unprecedented undertaking which required review at the highest levels of the Department of Justice and was accomplished as quickly as possible.

On or about May 28, 2021, the government contracted Deloitte Financial Advisory Services, LLP ("Deloitte"), a litigation support vendor with extensive experience providing complex litigation technology services, to assist in document processing, review and production of materials related to the Capitol Breach. As is required here, Deloitte furnishes secure, complex, and highly technical expertise in scanning, coding, digitizing, and performing optical character recognition – as well as processing, organizing, and ingesting a large volume of Electronically Stored Information ("ESI") and associated metadata in document review platforms – which is vital to the United States' ability to review large data/document productions and is essential to our ability to prosecute these cases effectively.

Implementation of Contract with Deloitte

We have already begun transferring a large volume of materials to Deloitte (as of July 7, 2021, over 200 disks of data and 34,000 USCP records), who is populating the database. Specific processing workflows and oversight are being established between the United States Attorney's Office and the vendor. We have already coordinated with Deloitte to use various tools to identify standard categories of Personal Identifying Information ("PII") and to redact them. Once the database is accessible, we will begin systematically reviewing materials for potentially discoverable information, tagging when possible (e.g., video by a location or type of conduct, interviews describing a particular event), and redacting when necessary. Among other things, the vendor is also building a master evidence tracker to assist us in keeping records of what is provided to us and what is ultimately produced, which is part of our approach to a defensible discovery protocol.

Systematic Reviews of Voluminous Materials

We are implementing and continuing to develop processes and procedures for ensuring that voluminous materials have been and will continue to be systematically reviewed for information that, *inter alia,* may be material to the defense, e.g.:

- Comparing all known identifiers of any charged defendant against tips, Parler data, ad tech data, cell tower data, and geofence data; and
- Searching all visual media (such as CCV, BWC, social media or device search results) – the collection of which grows on a regular basis – against known images of charged defendants.

Certain Specific Defense Requests

Multiple defense counsel have inquired about investigations into officers who were *alleged* to have been complicit in the January 6 Capitol Breach. We have received copies of investigations into officer conduct, have finished reviewing them, and plan to disclose the relevant materials shortly.

Complexities Require Careful Consideration

Producing discovery in a meaningful manner and balancing complex legal-investigative and technical difficulties takes time. We want to ensure that all defendants obtain meaningful access to voluminous information that may contain exculpatory material, and that we do not overproduce or produce in a disorganized manner. That means we will review thousands of investigative memoranda, even if there is a likelihood they are purely administrative and not discoverable, to ensure that disclosures are appropriate.

Legal-Investigative Considerations

We must also carefully ensure we are adequately protecting the privacy and security interests of witnesses and subjects from whom those materials were derived. For example, we cannot allow a defendant's PII to be disseminated – without protection – to hundreds of others. Similarly, we cannot allow personal contact information for Congressional members, staffers, and responding police officers – targets and victims of these crimes – whose phones may have connected to the Capitol's DAS network to inadvertently be produced. We also must protect Law Enforcement Sensitive materials by ensuring they are carefully reviewed for discoverability and, if they are discoverable, that they are disclosed in an appropriate manner. We continue to develop workable paradigm for disclosing a vast amount of Capitol CCV while ensuring that the Capitol's security is maintained. We are also scrupulously honoring defendants' attorney-client

privilege by employing a filter team that is continually reviewing devices and accounts for potentially privileged communications.

Technological Considerations

A large volume of the information that has been collected consists of 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.

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.

Involving Defense Counsel in Voluminous Discovery Plan

The Discovery Team regularly meets with FPD leadership and technical experts with respect to discovery issues. Given the volume of information that may be discoverable, FPD is providing input regarding formats that work best with the review tools that Criminal Justice Act panel attorneys and Federal Defender Offices have available to them. Due to the size and complexity of the data, we understand they are considering contracting with third party vendors to assist them (just as the United States Attorney's Office has done for this matter). So as to save defense resources and to attempt to get discovery more quickly to defense counsel, there were efforts made to see if FPD could use the same vendor as the United States Attorney's Office to set up a similar database as the government is using for reviewing the ESI, but for contractual and technical reasons we have recently learned that was not feasible. We are in the on-going process of identifying the scope and size of materials that may be turned over to FPD with as much detail as possible, so that FPD can obtain accurate quotes from potential database vendors. It is hoped that any databases or repositories will be used by FPD offices nationwide that are working on Capitol Breach cases, counsel that are appointed under the Criminal Justice Act, and retained counsel for people who are financially unable to obtain these services. A database will be the most organized and economical way of ensuring that all counsel can obtain access to, and conduct meaningful searches upon, relevant voluminous materials, e.g., thousands of hours of body worn camera and Capitol CCV footage, and tens of thousands of documents, including the results of thousands of searches of SCA accounts and devices.

Compliance with Recommendations Developed by the Department of Justice and Administrative Office of the U.S. Courts Joint Working Group on Electronic Technology

As is evidenced by all of the efforts described above, the United States is diligently working to comply with the *Recommendations for Electronically Stored Information (ESI)*

Discovery Production developed by the Department of Justice and Administrative Office of the U.S. Courts Joint Working Group on Electronic Technology in the Criminal Justice System in February 2012.[1] *See https://www.justice.gov/archives/dag/page/file/913236/download.* For example, we are: (1) including individuals with sufficient knowledge and experience regarding ESI; (2) regularly conferring with FPD about the nature, volume and mechanics of producing ESI discovery; (3) regularly discussing with FPD what formats of production are possible and appropriate, and what formats can be generated and also maintain the ESI's integrity, allow for reasonable usability, reasonably limit costs, and if possible, conform to industry standards for the format; (4) regularly discussing with FPD ESI discovery transmission methods and media that promote efficiency, security, and reduced costs; and (5) taking reasonable and appropriate measures to secure ESI discovery against unauthorized access or disclosure.

[1] These *Recommendations* are explicitly referenced in the Advisory Committee Note to Rule 16.1. Importantly, the two individuals primarily responsible for developing the Recommendations are Associate Deputy Attorney General Andrew Goldsmith, who (as noted earlier) is working closely with the prosecution's Discovery Team, and Sean Broderick, the FPD's National Litigation Support Administrator, who is playing a similar role for the D.C. Federal Defender's Office on electronic discovery-related issues. Messrs. Goldsmith and Broderick have a long history of collaborating on cost-effective ways to address electronic discovery-related issues, which undoubtedly will benefit all parties in this unprecedented undertaking.

EXHIBIT A
Additional Examples of Defense Discovery Requests

1	"Videos in the government's possession that filmed the interior of the capital building from approximately 2:50 PM to 3:35 PM on January 6, 2021."
2	"[A]ll photographs or video footage obtained or confiscated by the government from outside sources during the investigation of this case are material to the defense's preparation."
3	"Our position is that the government must identify any evidence it believes to capture [defendant], regardless of whether it intends to rely on the same in its case in chief."
4	"Copies of any and all documents, photographs, and video received by the U.S. Attorney's office and/or Metropolitan Police Department or any other law enforcement agency from any law enforcement officer or prosecutor from any other jurisdiction regarding this case."
5	"I write to request that the United States review the contents of the FBI's "I" drive and disclose any and all exculpatory evidence identified therein."
6	"Network news outlets aired footage of one or more Officers directing protestors towards doors and seemingly invited them to enter the building -- this is Brady material for our clients."
7	"The discovery I'm requesting is all video and/or audio footage in which Capitol Police and any other Gov't officials or agents remove barriers and/or interact with protestors who entered the Capitol or gained access to the patios or other structures connected to the Capitol building complex."
8	"This request also includes any video footage, including from cameras owned by MPD (crime and red light) and DDOT (which are operated and maintained by MPD, and to which MPD has access), as well as any footage that government actors reviewed. This request also includes any video footage from MPD District where the defendant was taken, and all body worn camera footage that may have captured any portion of the alleged incident, investigation or arrest of my client." "The request includes all Body Worn Camera (BWC) footage from all offices involves in any and all searchers, arrests, and investigations associated with this case and/ or labels with the CCN Number associated with this case; information that will permit undersigned counsel to identify the officer wearing the BWC; metadata related to any and all BWC footage; information from the AUSA's office and/or MPD specifying any edits or redactions made to the footage and the corresponding justifications. Please also provide the access logs for the BWC footage for any and all officers involved in this case."
9	"All **photographs**, including those of the defendant, **sketches, diagrams, maps, representations or exhibits** of any kind, that relate to this case, regardless of whether the government intends to introduce them in its case-in-chief . . .Including all video recordings related to the January 6, 2021 events."
10	"I further request that you review all documentation related to or generated in connection with this case that may be outside of the government's official case file (e.g., materials in the FBI's "I-Drive" or other similar repositories of investigation documents in the possession of federal or local agencies or law enforcement authorities."

EXHIBIT A
Additional Examples of Defense Discovery Requests

11	"Any evidence (whether or not reduced to writing) that law enforcement or Capitol employees allowed any protestors into the building. Such evidence might include (without limitation) moving barricades, opening doors, instructing protestors they could enter, failing to intervene when protestors entered, etc…"
12	"Any evidence that concerns any Capitol police officers who were suspended and/or disciplined for removing barriers, opening doors, etc. on January 6th."
13	"I am also concerned about the thousands or tens of thousands videos the government has received from public sources, particularly how the government is searching, indexing, and storing these videos, and whether the government is withholding any video footage in its possession; Based on my review of the discovery thus far, there is official video surveillance and publicly sourced video footage that is exculpatory to the defendants. Many of those videos show [defendant] and other[s] peacefully walking around the Capitol. In these videos, they, like thousands of others, are doing nothing illegal with the possible exception of being present in the building, all of which is potentially exculpatory."
14	"All information regarding any Capitol Police, MPD, National Guard, other law enforcement officer or other person in position of authority ("LEOs") who moved guard rails, opened or held doors open, stepped aside, allowed persons to enter or stay within the Capitol or otherwise did not direct, instruct or signify to the public -- implicitly or explicitly -- to vacate the Capitol or that the Capitol was closed to the public or restricted for public entry."
15	"Any audio or video footage of [defendant] relevant to any of the charges in the indictment that has not previously been provided, whether captured by body-cameras worn or phones carried by Metropolitan Police Department officers, by body-cameras worn or phones carried Capitol Police officers, or by phones or other recording devices carried by any other witness."
16	"For purposes of this letter, all photographs or video footage obtained or confiscated by the government from outside sources during the investigation of this case are material to the defense's preparation. Please provide notice of any decision not to produce requested photographs, video footage, or recorded communications so that a judicial decision as to production may, if warranted, be sought. Please also provide all photographs, video footage, and recorded communications relating to the *Brady* and *Giglio* requests articulated below."

UNITED STATES' MEMORANDUM
REGARDING STATUS OF DISCOVERY AS OF AUGUST 23, 2021

The United States files this memorandum for the purpose of describing our overall approach to discovery, and our discovery plan in relation to voluminous sets of data that the government collected in its investigation of the Capitol Breach cases, among which may be interspersed information the defense may consider material or exculpatory. The materials upon which this memorandum is focused include, for example, thousands of hours of video footage from multiple sources (e.g., Capitol surveillance footage, body-worn-camera footage, results of searches of devices and Stored Communications Act ("SCA") accounts, digital media tips, Parler video, and unpublished news footage), and hundreds of thousands of investigative documents including but not limited to interviews of tipsters, witnesses, investigation subjects, defendants, and members of law enforcement. Further, we write to provide the Court with the status of our implementation of that plan as of August 23, 2021.

I. The Government's Approach to Discovery is Intended to Ensure that All Arguably Exculpatory Materials are Produced in a Comprehensive, Accessible, and Useable Format.

The government has always understood the magnitude and complexity of the discovery project presented by the January 6 attack on the Capitol. We have taken a very expansive view of what may be material or potentially exculpatory and thus discoverable in Capitol Breach cases. Defense counsel in Capitol Breach cases have made requests including any and all information that captures an individual defendant's conduct or statements; shows people "peacefully walking around the Capitol"; or suggests that a member (or members) of law enforcement allowed people to enter or remain in the Capitol or on restricted grounds, acted friendly or sympathetic to the rioters, or otherwise failed to do their jobs. Of course, there may be additional types of information a defendant may consider material or exculpatory, but since

the government does not know the defense theory in any particular case, it is impossible to for the government to determine what other types of information a defendant may believe to be material.

To the extent the type of information described above may exist, it may be interspersed among the voluminous sets of data referenced above. Given the volume of material, and because "[d]efendants are in a better position to determine what evidence they believe is exculpatory and will help in their defense,"[1] it is our intent to provide the defense with all data that may contain such information, but in a manner that will facilitate search, retrieval, sorting, and management of that information.

II. Our General Plan for Production of Voluminous Materials Involves Two Separate Platforms.

We have developed and begun implementing a plan to use two primary platforms to process and produce discoverable voluminous materials: one for documents (e.g., items such as law enforcement investigation files and business records) and one for digital materials (e.g., video footage). (These two platforms have frequently been referred to as our "database" although, in fact, they are two separate information repositories hosted by unrelated vendors.) We are working collaboratively with Federal Public Defender ("FPD") leadership and electronic discovery experts, including Sean Broderick, the National Litigation Support Administrator for

[1] *United States v. Meek,* No. 19-cr-00378-JMS-MJD, 2021 WL 1049773 *5 (S.D. Ind. 2021). *See also United States v. Ohle*, No. S3 08 CR 1109 (JSR), 2011 WL 651849 *4 (S.D.N.Y. 2011)(not reported in F.Supp.2d)("placing a higher burden on the Government to uncover such evidence would place prosecutors in the untenable position of having to prepare both sides of the case at once. Indeed, the adversarial system presumes that the defense will be more highly motivated to uncover exculpatory evidence, so if anything the onus is on defense counsel to conduct a more diligent search for material potentially favorable to his client. This is especially true considering that, if exculpatory evidence exists, the defense is in the best position to know what such evidence might be and where it might be located.")

the Administrative Office of the U.S. Courts, Defender Services Office, to ensure that Federal Public Defender offices nationwide that are working on Capitol Breach cases, counsel that are appointed under the Criminal Justice Act, and retained counsel for people who are financially unable to obtain these services will have access to the same platforms, including technological functionality commensurate to that available to the government, for the purpose of receiving and reviewing discoverable materials.

A. We will Share Documents from Our Own Relativity Workspace to a Defense Relativity Workspace, and are Making Rolling Productions Via Alternative Means Until the Defense Workspace is Available.

1. Overview

Deloitte is hosting a Relativity database, or "workspace," for the government to manage and produce documents. Relativity is a cloud-based eDiscovery platform that offers functionalities including document organization, review, production, and analytics within a single environment, and is an industry leader in eDiscovery hosting. As further elaborated below, we are in the process of ingesting hundreds of thousands of documents into our Relativity workspace, so that we may review them, apply necessary redactions, and produce the documents as appropriate to the defense.

Ultimately, our plan is for all discoverable documents to be shared to a wholly separate defense Relativity workspace, also hosted by Deloitte, but wholly inaccessible to the government. Deloitte is currently creating such a defense workspace within Relativity for receipt of discoverable documents, and we are working toward a modification of our contract to fund the additional hosting and support of that database.[2]

[2] Hosting refers to storing and organizing documents in a case within a database for document review, organizing, searching, categorizing, and redacting, and providing users with accounts to access the database. Typically, providing discovery in a format that allows it to be loaded into a

A Relativity workspace will allow Capitol Breach defense teams to leverage Relativity's search and analytics capabilities to search the voluminous documents we expect to produce for information they believe may be material to their individual cases. Defense teams will be able to perform key term searches and metadata searches across hundreds of thousands of documents in the defense workspace. Further, in conjunction with any staff they designate to support their workspace, they will be able to design coding panes that allow them to "tag" items received in discovery as they deem relevant to their cases, e.g., by location ("Lower West Terrace") or defense theories of the case ("Police Let Defendants In"); and then generate search reports based on the results associated with a particular tag or multiple tags.[3]

As elaborated below, although Relativity significantly increases the pace at which we may review and process materials to make appropriate productions, performing these tasks correctly and comprehensively takes time. Nevertheless, we expect to begin making

---

database satisfies the government's discovery obligations. We understand that neither the Federal Public Defender nor the Criminal Justice Act panel has a vehicle in place through which they may engage in expedited contracting for the hosting and licensing services that are necessary to meet the demands of this unprecedented volume of materials. Thus, the government has agreed to provide the necessary hosting and licensing services through Deloitte. The government has been closely coordinating with FPD to ensure that when we modify our contract with Deloitte, we obtain sufficient licenses to cover the needs of current cases as well as those of cases that may be brought in the future.

[3] We believe that to ensure defendants have meaningful access to the defense Relativity workspace, FPD will require additional support for the workspace. As the Court is aware, "Even if the discovery is produced in an optimal way, defense counsel may still need expert assistance, such as litigation support personnel, paralegals, or database vendors, to convert e-discovery into a format they can use and to decide what processing, software, and expertise is needed to assess the [Electronically Stored Information]." *See Criminal e-Discovery: A Pocket Guide for Judges*, Chapter II (Common Issues in Criminal e-Discovery), at 12. The *Pocket Guide* serves as a supplement to the federal judiciary's bench book. We are engaging in frequent and productive discussions with FPD in the effort to resolve contractual and technical details related to the implementation of an adequate support plan.

documentary productions from Relativity within the next two weeks, as discussed in more detail below, and will do so on a rolling basis going forward. Until the defense Relativity workspace is operational and defense accounts are established documents will continue to be produced in individualized cases via other available methods – most frequently cloud-based file sharing through USAfx.

2. The Government is Steadily Populating its Own Relativity Database with Materials.

We have already populated our Relativity database with over 30,000 records from the U.S. Capitol Police ("USCP") and USCP reports related to allegations of misconduct by law enforcement in connection with the events of January 6, 2021. We are currently using our Relativity platform to process materials related to allegations of police misconduct, and plan to make those reports available within approximately the next two weeks. Capitol Breach prosecution teams will disseminate these materials once they become available. We are prioritizing these materials and Metropolitan Police Department ("MPD") use-of-force investigation files because many defendants have requested them.

We are steadily working to ingest into Relativity potentially discoverable documents that we requested and received from multiple law enforcement agencies, while ensuring that materials that are or may be protected by Federal Rule of Criminal Procedure 6(e) are adequately protected. Of course, Federal Bureau of Investigation ("FBI") files account for the majority of documentary evidence that we will need to ingest and review. The FBI estimates that there are approximately 750,000 investigative memoranda and attachments in its files associated with the Capitol Breach investigation. We intend to organize, deduplicate, and produce these materials as appropriate, using all of Relativity's tools to do so as quickly as possible. As discussed below,

however, these processes are not wholly automated, and will require both technical expertise and manual assistance.

3. <u>The Workflow in Processing Materials for Discovery Takes Time.</u>

The process of populating Relativity with potentially discoverable material, all in varied formats and from different sources, is complicated. It is *not* like copying and pasting a file, or even like duplicating a hard drive. Before the hundreds of thousands of investigative files at issue here are ever loaded to Relativity, they must be meaningfully organized into folder structures that will make sense to reviewers and recipients. The materials must also be quality-checked, e.g., we must ensure that we have the password for protected documents, that the documents were provided in a format that will open, and that we remove irrelevant software and system files that would only cloud the workspace and confuse reviewers. After materials are loaded to Relativity, we must customize the manner in which they are displayed so as to be meaningful to reviewers who will make discoverability determinations and apply appropriate redactions and sensitivity designations. Not all documents are created equal, e.g., financial records and forensic cell phone search reports cannot meaningfully be displayed in the same way.

All of these processes will be assisted by leveraging Relativity's tools as much as possible, such as by using keyword searches to identify items that must be excluded or redacted; and deduplication tools to recognize documents that have already been processed so that they are not analyzed or reproduced multiple times. Although these processes are time-consuming, they are necessary to avoid production of unorganized data dumps, unreadable files, and unusable databases; or a failure of the government to take adequate steps to prevent both victims and defendants' private information from being shared with hundreds of defendants.

B. We will Share Digital Evidence from Our Own Evidence.com Instance to a Defense Evidence.com Instance, and Make Rolling Productions as Digital Media is Processed.

Relativity was primarily designed as document review platform and not to manage terabytes of digital evidence. Although it is technologically possible to view and share video evidence within Relativity, in this case, the volume of video would significantly reduce Relativity's performance speed.

Accordingly, we will use evidence.com as a platform to manage, review, and share digital media evidence. Evidence.com is a cloud-based digital evidence management system designed by Axon Enterprise, Inc. ("Axon"), an industry leader in body-worn-camera systems. Axon refers to a singular environment of evidence.com as an "instance." The government has agreed to fund a defense instance of evidence.com and to provide the necessary licensing services through Axon. This instance will be managed and administered by FPD, and the government will have no ability to log into or retrieve information from this instance. As recently as Saturday, August 21, 2021, we consulted with representatives from Axon about our plan and we expect our contract with Axon will be modified expeditiously. As with Relativity, the government has been closely coordinating with FPD to ensure that we cover the needs of current cases as well as those of cases that may be brought in the future. We understand that legal defense teams will likely wish to share voluminous evidence with defendants. Axon has additional infrastructure referred to as my.evidence.com that will allow defense attorneys to share voluminous evidence with individual defendants.

We have already migrated over 2,900 body-worn-camera videos totaling over 2,300 hours (nearly 100 days) into our instance of evidence.com. For the reasons relayed above, from a technological perspective, we expect to be able to share this footage with FPD's evidence.com

instance within approximately the next two weeks. Before we can share voluminous video footage with FPD, we must also ensure that the footage is adequately protected. Based on a review of the body-worn-camera footage conducted by our Office, the footage displays approximately 1,000 events that may be characterized as assaults on federal officers. As these officers now, or in the future may, qualify as victims under the Crime Victims Rights Act, they have the "right to be reasonably protected from the accused" and the "right to be treated with fairness and with respect of the victim's dignity and privacy." 18 U.S.C. §§ 3771(a)(1) and (8).

When we share the footage, we also intend to share information we have developed that will help facilitate efficient defense review of body-worn-camera footage. For example:

- Individuals in our Office who reviewed all the body-worn-camera footage in our instance created a spreadsheet that identifies footage by agency, officer, video start time, a summary of events, and location of the camera in 15-minute increments. The locations are defined in zone map they created. We will share our zone map and the spreadsheet with the legal defense teams, subject to adequate protection.

- We obtained from MPD Global Positioning Satellite ("GPS") information for radios that may be of assistance in identifying the location of officers whose body-worn-camera footage is relevant to the defense. We will share this information with the legal defense teams, subject to adequate protection.

We will continue to ingest video evidence into evidence.com on a rolling basis, and to produce it regularly. As evidence.com was designed to function in coordination with body-worn-cameras designed by Axon, ingesting body-worn-camera footage into our instance was fairly simple. Other footage will need to be converted from proprietary formats before it can be ingested into evidence.com, and so processing will take longer.

At this time, the FBI is in the process of transmitting Capitol surveillance footage for ingestion into evidence.com. Because of the size of the footage, it will take several weeks to receive and ingest the footage. Based on our current understanding of the technical complexities involved, we expect to start rolling productions from 7,000 hours of footage that the USCP

provided the FBI within approximately the next four weeks. An additional 7,000 hours of footage is not relevant to this case and, therefore will not be produced.

III. Conclusion.

In sum, while we have not resolved every contractual or technical detail, and while our discovery plan continually evolves to address issues as they arise, we are making substantial progress in our diligent efforts to provide the defense comparable discovery review platforms for both documents and digital media, to populate those platforms, and to use alternative means to provide the most relevant discovery without delay. We are confident that our plan will come to fruition, and although we have not reached agreement on every aspect of this plan, we continue to have good faith, productive discussions with FPD regarding production of voluminous data. In the interim, we will diligently continue to transfer data to our vendors, process it for production, and make interim productions by other means until the defense platforms are in place. As we continue to implement our plan, we will continue to file status memoranda with the Court on a regular basis.

UNITED STATES' MEMORANDUM
REGARDING STATUS OF DISCOVERY AS OF SEPTEMBER 14, 2021

The United States files this memorandum for the purpose of describing the status of implementation of our discovery plan in relation to voluminous sets of data that the government collected in its investigation of the Capitol Breach cases, among which may be interspersed information the defense may consider material or exculpatory. The materials upon which this memorandum is focused include, for example, thousands of hours of video footage from multiple sources (e.g., Capitol surveillance footage, body-worn-camera footage, results of searches of devices and Stored Communications Act accounts, digital media tips, Parler video, and unpublished news footage), and hundreds of thousands of investigative documents including but not limited to interviews of tipsters, witnesses, investigation subjects, defendants, and members of law enforcement.

Capitol Breach Defense Discovery Liaison Established

The Federal Public Defender for the District of Columbia ("FPD") has agreed to serve as the Discovery Liaison for defense counsel in Capitol Breach cases. FPD will be the common point of contact between the U.S. Attorney's Office for the District of Columbia, the U.S. District Court for the District of Columbia, the Administrative Office of U.S. Courts, Defender Services Office, and defense counsel.

Status of Defense Access to Discovery Databases

As noted in our Memorandum Regarding Status of Discovery as of August 23, 2021 (the "August 23 Memo"), incorporated herein by reference, under our discovery plan, we will use two primary platforms to process and produce discoverable voluminous materials, evidence.com for voluminous digital media materials (e.g., body-worn-camera footage and U.S. Capitol Police ("USCP") surveillance footage) and Relativity for documents (e.g., items such as law

enforcement investigation files and business records). Further, we will ensure that all Capitol Breach legal defense teams will have access to the same platforms, including technological functionality commensurate to that available to the government, for the purpose of receiving and reviewing discoverable materials.

Evidence.com

On September 3, 2021, the United States modified its contract with Axon Enterprise, Inc. ("Axon"), our evidence.com vendor. Pursuant to the modification, the government has funded a Capitol Breach defense instance of evidence.com and purchased licenses that will enable legal defense teams to gain access to a defense discovery database. The defense instance is managed and administered by FPD, and the government has no ability to log into or retrieve information from the defense instance. FPD is currently working with Defender Service's National Litigation Support Team to create a structure for distributing and tracking Axon licenses for defense counsel. As we stated in our previous memo, defense counsel can share evidence from the defense instance with individual defendants using a cloud-based file-sharing service offered by Axon called my.evidence.com (as well as provide downloaded video, except when prohibited by a sensitivity designation).

As a result of September 3, 2021 contract modifications, we are now technologically able to share approximately 2,300 hours of body-worn-camera videos to the defense instance of evidence.com. To ensure this enormous production is organized and meaningful for the defense, we are currently categorizing and tagging the videos. Further, to ensure that the videos (which display approximately 1,000 assaults upon officers and include occasional references to personal identifying information) are adequately protected, we are also exploring whether it is

technologically possible for downloading to be automatically suppressed when highly sensitive video is shared by defense counsel to defendants.

We are hopeful we will be able to transfer the body-worn-camera footage to the defense instance of evidence.com by the end of this week (Friday, September 17, 2021), and expect to produce it no later than the end of next week (Friday, September 24, 2021).[1]

We have uploaded approximately twenty percent of the relevant USCP surveillance footage to our instance of evidence.com (i.e., in excess of one terabyte of video, consisting of about 140 cameras, 4,900 files, and 1,600 hours of footage). We are nearly finished applying sensitivity designations to these files. We expect to be able to share them to the defense instance next week.

FPD anticipates updating defense counsel with the status of their work to distribute and track Axon licenses approximately one week after the first significant production of discovery is loaded into the defense instance evidence.com platform.

Relativity

Deloitte Financial Advisory Services, LLP ("Deloitte"), our Relativity vendor, has established a Capitol Breach defense Relativity workspace. We continue to work toward a modification of our contract to fund the additional hosting and support of that database. Modifying the Deloitte contract presents multiple contractual, technical, and legal challenges that were not posed by the Axon contract, but we are moving with as much haste as possible given the various complexities. We believe that by October, the contract modifications will be

[1] As elaborated in our August 23 Memo, we will also provide information we have developed that will help facilitate defense review of the footage.

completed, thus allowing for defense access to the Relativity database.[2] To give the Court a sense of just some of the challenges that we are addressing, they include formulating concrete plans describing the staffing and technological safeguards that will be put into place to eliminate the possibility of work product being shared from one workspace to another. We must also ensure the modification, which must be fairly detailed under applicable government contracting rules and regulations, will be sufficient to support hundreds of defense cases, and are working closely with FPD in support of that effort. As this undertaking by FPD is also unprecedented, handling the contract modification correctly takes time. FPD will work with Defender Service's National Litigation Support Team to create a structure for distributing and tracking Relativity licenses and anticipates updating defense counsel with the status of their work approximately one week after the contract is modified to provide access to FPD. Finally, we must ensure that in making available hundreds of thousands of documents to hundreds of legal defense teams, we are careful to ensure that materials are properly scoped pursuant to the terms of any applicable warrants, and that access to the database is restricted in a manner that will ensure our compliance with applicable privacy laws. We are currently consulting with Department of Justice experts in privacy and discovery to ensure that these issues are properly handled.

Until the defense Relativity workspace is accessible, as we stated in our August 23 Memo, we will continue to provide voluminous documents from our Relativity database through individualized productions. (Any productions we make will also be added to the defense Relativity workspace.) On Friday, September 10, 2021, the Discovery Team made available for production in all Capitol Breach cases approximately 850 pages consisting of redacted reports

[2] To be clear, while we expect the defense Relativity database will be partially populated in October, we do not expect it to be complete at that time.

from USCP investigations of alleged wrongdoing by USCP officers on January 6, 2021. We anticipate providing Metropolitan Police Department internal investigation reports (approximately 600 pages) by next week. We are still reviewing the approximately 30,000 files in Relativity that were provided to us by USCP.

As the Discovery Team continues to receive additional documents, we cull them of any materials potentially protected by Federal Rule of Criminal Procedure 6(e) and provide the remainder (a majority) to Deloitte for ingestion into our Relativity database for discovery review. At this time, we have provided Deloitte the following additional documents for ingestion into our Relativity database:

- Discovery productions (approximately 11,500 records) that have been made in complex Capitol Breach cases (e.g., multi-defendant conspiracies involving Oathkeepers and Proud Boys);[3] and
- Approximately 24,000 Federal Bureau of Investigation records.

This week, we also expect to provide Deloitte discovery productions that have been made in 75 individual cases (approximately 32,000 documents).[4] As we have described in our prior discovery status memos, the process of populating Relativity with potentially discoverable material is complicated and takes time.

Incarcerated Defendants

In collaboration with FPD, we are developing proposals to increase access by incarcerated defendants to voluminous materials, which we expect to share with the D.C. Department of Corrections and to discuss within the next two weeks.

[3] Although these productions were already made in the relevant cases, they will ultimately be made accessible to all Capitol Breach defendants through the defense Relativity workspace.

[4] Although these productions were already made in the relevant cases, they will ultimately be made accessible to all Capitol Breach defendants through the defense Relativity workspace.

Conclusion

In sum, while we have not resolved every contractual or technical detail, and while our discovery plan continually evolves to address issues as they arise, we are making substantial progress in our diligent efforts to provide the defense comparable discovery review platforms for both documents and digital media, to populate those platforms, and to use alternative means to provide the most relevant discovery without delay. We are confident that our plan will come to fruition, and although we have not reached agreement on every aspect of this plan, we continue to have good faith, productive discussions with FPD regarding production of voluminous data. In the interim, we will diligently continue to transfer data to our vendors, process it for production, and make interim productions by other means until the defense platforms are in place. As we continue to implement our plan, we will continue to file status memoranda with the Court on a regular basis.

UNITED STATES' MEMORANDUM
REGARDING STATUS OF DISCOVERY AS OF OCTOBER 21, 2021

The United States files this memorandum for the purpose of describing the status of implementation of our discovery plan in relation to voluminous sets of data that the government collected and continues to collect in its investigation of the Capitol Breach cases, among which may be interspersed information the defense may consider material or exculpatory. The materials upon which this memorandum is focused include, for example, thousands of hours of video footage from multiple sources (e.g., Capitol surveillance footage, body-worn-camera footage, results of searches of devices and Stored Communications Act ("SCA") accounts, digital media tips, Parler video, and news footage), and hundreds of thousands of investigative documents including but not limited to interviews of tipsters, witnesses, investigation subjects, defendants, and members of law enforcement.

Status of Defense Evidence.com Database

On September 3, 2021, the United States modified its contract with Axon Enterprise, Inc. ("Axon"), our evidence.com vendor. Pursuant to the modification, the government funded a Capitol Breach defense instance of evidence.com and purchased licenses that will enable legal defense teams to gain access to evidence.com and view voluminous video evidence. The defense instance is managed and administered by the Federal Public Defender for the District of Columbia ("FPD"), who is acting as the Discovery Liaison for defense counsel in Capitol Breach cases, and the government has no ability to log into or retrieve information from the defense instance.

In conjunction with the Defender Service's National Litigation Support Team, FPD created a structure for distributing and tracking evidence.com licenses for defense counsel. As of October 18, 2021, FPD has sent emails to all Capitol Breach defense counsel with instructions on

how to request a license for the legal defense team to view videos in evidence.com. FPD also developed a "Quick Start Guide" that it simultaneously circulated to all Capitol Breach defense counsel, with instructions for registering an account, logging into evidence.com, and further describing how video discovery may be shared with their clients through the evidence.com platform consistent with the standard Capitol Breach protective order.

Status of Production of Video Footage

The following video footage has been shared to the defense instance of evidence.com and is accessible to any Capitol Breach defense counsel who requests a license:

- 16,925 U.S. Capitol Police ("USCP") Closed Circuit Video ("CCV") files consisting of approximately 4,800 hours (over four terabytes) of footage from 515 cameras located inside the U.S. Capitol Visitor Center and on the Capitol grounds. To assist the defense in locating relevant USCP CCV, we have also produced (via USAfx) 15 camera maps of the interior of Capitol Visitor's Center and the interior of the Capitol.

- 1,676 Metropolitan Police Department ("MPD") body-worn-camera ("BWC") files consisting of approximately 1,600 hours of footage recorded by over 900 officers between 1:00 p.m. and 6:00 p.m. on January 6, 2021. To assist the defense in locating officers who may have recorded body-worn-camera footage at a particular location and time, we also produced (via USAfx) a spreadsheet created by the Discovery Team based on MPD radio Global Positioning Satellite records.

Status of Defense Relativity Workspace

On October 13, 2021, the United States modified its contract with Deloitte Financial Advisory Services, LLP ("Deloitte") to fund a Capitol Breach Relativity workspace and purchase licenses that will enable legal defense teams to gain access to the database. FPD is now consulting with Deloitte concerning the construction and organization of the defense workspace and creating a structure for distributing Relativity licenses to defense counsel. FPD will notify Capitol Breach defense counsel on how to obtain Relativity license access once the defense workspace is constructed and organized and is ready to be populated with documents.

Status of Production of Documents

Since our last filing describing the status of discovery as of September 14, 2021, the following materials and a corresponding index have been made available for sharing with Capitol Breach defense counsel via USAfx:

- 42 files that consist of MPD internal investigation reports and exhibits (739 pages);
- 31 files consisting of digital exhibits to previously produced USCP Office of Professional Responsibility ("OPR") reports;[1] and
- USCP radio communications and draft transcripts.

Contents of Government Relativity Database

Our Relativity database currently contains over 33,000 records from USCP, 23,000 records from MPD, and 56,000 records from the FBI's main Capitol Breach file (of which about 29,000 pertain to individual defendants and are likely to overlap with materials already produced in the specific cases to which they are most directly relevant).

[1] On September 10, 2021, we made available via USAfx 35 files consisting of 28 reports from USCP OPR investigations of alleged wrongdoing by USCP officers on January 6, 2021.

Manner of Productions Going Forward

In terms of the manner in which discovery will be produced going forward:

- We will continue to utilize evidence.com to produce voluminous video footage in all Capitol Breach cases.

- Until Relativity access is available to Capitol Breach defense counsel, limited productions such as those described above will continue to be made available to counsel via USAfx, as well as produced to the defense Relativity workspace.

- Once defense counsel have access to Relativity, it will become the primary method for producing voluminous documents. However, we will still continue to make organized productions and issue discovery letters to defense counsel describing materials that have been added to the defense database.

- Certain materials, because of their nature or volume, will only be produced to the defense Relativity workspace. E.g., case-specific discovery that has been provided in *other* defendants' cases and the results of searches of devices and SCA accounts. Those materials will become accessible to defense counsel once FPD distributes licenses for Relativity.

Incarcerated Defendants

In collaboration with FPD, we have developed a proposal to increase access by incarcerated defendants to discovery materials by providing access to e-discovery (by providing limited evidence.com and Relativity access to inmates via wi-fi and increasing the number of computers available for discovery review). FPD and our office had a productive meeting with representatives from the D.C. Department of Corrections ("DOC") about the e-discovery proposal on Wednesday, October 20, 2021. At the meeting, representatives of DOC indicated they would explore with the Director whether a pilot e-discovery program consistent with our proposal, beginning with Capitol Breach defendants, may be implemented consistent with the DOC's security concerns and Internet capacity. We are meeting again on October 27, 2021, at which time we expect to obtain requested technical and logistical information from the DOC that would be essential to implementing our joint proposal.

We understand there are four defendants who are currently proceeding *pro se*, three of whom are detained. We are currently developing a plan for access to voluminous materials by *pro se* defendants and will inform the Court once we have finalized our approach, after collaboration with FPD.

Future Productions

Among the documents we expect future productions to include are:

- The remainder of USCP CCV (4,204 files), which is mainly comprised of footage that has been deemed Highly Sensitive, e.g., footage of the interior of the Capitol;[2]
- The remainder of MPD BWC footage (largely consisting of footage outside the 1:00 to 6:00 p.m. timeframe), and BWC footage from Arlington County Police (124 files), Fairfax County Police (24 files), Montgomery County Police (60 files), and Virginia State Police (48 files);
- U.S. Secret Service surveillance camera footage (143 videos);
- Video recordings made by officers of MPD's Electronic Surveillance Unit;
- Camera map for Capitol grounds;
- Supplemental exhibits to USCP OPR reports;
- USCP After Action Reports;
- MPD Aerial Surveillance Unit Photos;
- Permits for Demonstrations at the U.S. Capitol;
- Additional MPD internal investigation reports;
- MPD and Virginia State Police radio transmissions;
- Legal process pertaining to the collection of geolocation data from Google, Inc. and various additional providers;
- BWC Spreadsheet and zone maps (work product created to assist in review of BWC footage);
- Statements made by members of law enforcement during interviews arising out of the Capitol Breach investigation;
- Discoverable MPD, USCP and FBI records and memoranda currently (or shortly to be ingested) into Relativity;
- Case-specific discovery of other defendants (i.e., discovery already produced to the defendant for whom it is directly relevant, but which will be made accessible to all defendants);
- Results of searches of devices and SCA accounts; and

[2] To be clear, we are not producing via evidence.com footage that constitutes "Security Information" pursuant to 2 U.S.C. § 1979, i.e., the 17 hours of CCV footage that relate to the evacuation of Congressional Members. The disclosure of this footage will be handled separately.

- Custodial statements of (other) defendants.

Substantial Completion of Discovery

We understand that the Court would like us to project when production of voluminous materials will be substantially complete. As an initial matter, to reach the point where we can assess a potential date of substantial completion, the government has taken and continues to make substantial efforts, including:

- Appointing a Capitol Breach Discovery Coordinator in January;
- Assembling a Capitol Breach Discovery Team consisting of experienced attorneys, project managers, and litigation technology professionals;
- Collecting information from multiple sources involved in the response to and investigation of the Capitol Breach;
- Collaborating with FPD to develop a standard protective order for Capitol Breach cases;
- Identifying database solutions for making terabytes of video and documents accessible to hundreds of defendants, funding defense databases and obtaining licenses for all Capitol Breach defense counsel, and collaborating with FPD to execute these solutions;
- Reviewing specific discovery requests by defense counsel to ensure the appropriate materials are prioritized for production;
- Creating protocols and procedures to ensure that (a) case-specific discovery is provided, (b) defendants will receive complete copies of unscoped devices and SCA accounts upon request; (c) devices and SCA accounts are systematically filtered for attorney-client communications; and (d) relevant scoped data and custodial interviews will be uploaded to the government's discovery databases for production to all; and
- Creating proposals for increasing access to discovery by incarcerated defendants.

We will soon begin to load into Relativity several hundred thousand FBI records (a substantial portion of which may not be directly related to any charged defendants). These materials that have been undergoing pre-processing to ensure, among other things, that any materials that might be subject to protection under Federal Rule of Criminal Procedure Rule 6(e) are segregated for processing internally. Once these documents are loaded in Relativity, we will be able to better assess and execute our plan for reviewing them and producing them in discovery. We are also currently engaged in a concerted effort to consolidate scoped search

results from thousands of devices and SCA accounts for ingestion by Deloitte. We thus expect to be in a better position to provide the Court an estimate of the time necessary for substantial completion within the next two weeks.

As many documents may not be discoverable or may be duplicative, neither the Court nor defense counsel should expect the size of the productions to the defense to mimic the size of the government's Relativity workspace.

Conclusion

In sum, we have made substantial progress in our diligent efforts to provide the defense comparable discovery review platforms for both documents and digital media, to populate those platforms, and to use alternative means to provide the most relevant discovery without delay. We will diligently continue to transfer data to our vendors, process it for production, and make interim productions by other means until the defense platforms are in place. As we continue to implement our plan, we will continue to file status memoranda with the Court on a regular basis.

UNITED STATES' MEMORANDUM
REGARDING STATUS OF DISCOVERY AS OF NOVEMBER 5, 2021

The United States files this memorandum for the purpose of describing the status of implementation of our discovery plan in relation to voluminous sets of data that the government collected and continues to collect in its investigation of the Capitol Breach cases, among which may be interspersed information the defense may consider material or exculpatory. The materials upon which this memorandum is focused include, for example, thousands of hours of video footage from multiple sources (e.g., Capitol surveillance footage, body-worn-camera footage, results of searches of devices and Stored Communications Act ("SCA") accounts, digital media tips, Parler video, and news footage), and hundreds of thousands of investigative documents including but not limited to interviews of tipsters, witnesses, investigation subjects, defendants, and members of law enforcement.

Status of Production of Video Footage

Since our last status memorandum filed on October 21, 2021, the following video footage has been shared to the defense instance of evidence.com and is accessible to any Capitol Breach defense counsel who requests a license from the Federal Public Defender ("FPD"):

- 142 files consisting of U.S. Secret Service (USSS) surveillance exterior camera footage from January 6, 2021.
- 4,204 files consisting of U.S. Capitol Police Closed Circuit Video ("USCP CCV") footage from 123 cameras. The contents of footage shared includes video from the interior of the U.S. Capitol.
- 24 files consisting of approximately 4 hours of body-worn-camera ("BWC") footage recorded by 11 Fairfax County Police officers. The footage begins on January 6, 2021, at 3:39 p.m. (and depicts the officers traveling to Washington, D.C.). The footage from the Capitol begins at 5:18 p.m.
- 60 files consisting of approximately 37 hours of BWC footage recorded by 22 Montgomery County Police officers. The footage begins on January 6, 2021, at 3:03 pm.

At this juncture, over 23,000 files consisting of USCP CCV, BWC and USSS surveillance footage have been made available to the defense instance of evidence.com

Status of Defense Relativity Workspace

As we stated in our prior memorandum, the United States modified its contract with Deloitte Financial Advisory Services, LLP ("Deloitte") on October 13, 2021, to fund a Capitol Breach Relativity workspace and purchase licenses that will enable legal defense teams to gain access to the database. FPD is now consulting with Deloitte concerning the construction and organization of the defense workspace and a structure for distributing Relativity licenses to defense counsel. FPD will notify Capitol Breach defense counsel on how to obtain Relativity licenses once the defense workspace is constructed and organized and is ready to be populated with documents.

In furtherance of FPD's efforts to construct the defense Relativity environment, on Friday, November 5, 2021, we will produce to the defense workspace a sample production consisting of 844 files of varied formats that are representative of many of the items we intend to produce. FPD and its vendor will use these files to create standard views, layouts, and coding panes to optimize defense attorney review of the voluminous documents we ultimately will provide.

Status of Production of Documents

Since our last status memorandum filed on October 21, 2021, the following materials and a corresponding index have been made available for sharing with Capitol Breach defense counsel via USAfx:

- A camera map of the Capitol Grounds. The camera map is work product that was created at the request of the Discovery Team to assist the defense in viewing USCP CCV. All camera locations depicted are approximate.

- Ten aerial surveillance images received from the Metropolitan Police Department ("MPD").
- Six demonstration permits received from the USCP.
- A spreadsheet containing the filenames/titles, starting times, video length, and date of the USSS video. This spreadsheet is work product that was created by the Discovery Team to assist the defense in viewing USSS video.
- 30 digital audio files consisting of 30 hours of MPD radio transmissions (Special Operations Division ("SOD") channel), beginning on January 6, 2021, at 12:00 a.m. and ending January 7, 2021 at 6:00 a.m.
- A 673-page transcript of the MPD radio transmissions (SOD channel), and an index that associates the Bates number for each audio file with the relevant pages of the transcript.
- USCP after-action reports (176 pages, redacted).
- 159 documents largely consisting of Federal Bureau of Investigation reports of interview of law enforcement officers about their experiences on January 6, 2021, and accompanying exhibits (being produced on November 5, 2021).

Contents of Government Relativity Database

As of our last filing, we stated that our Relativity database contained, *inter alia*, over 23,000 records from MPD. Using Relativity's deduplication tools, we were able to eliminate about 4,000 records as duplicates. We will continue to deduplicate materials that we collect in this investigation to make the database as efficient as possible.

Incarcerated Defendants

As a preliminary matter, the Department of Corrections ("DOC") has significantly expanded its existing electronic evidence review program. Under that program, defense attorneys may request that clients be allowed to review voluminous or electronic evidence on a laptop computer provided by the DOC. When a defense attorney sends electronic evidence (e.g., CDs, DVDs or USB flash drives) to the DOC's Litigation Support Unit, the receiving inmate is placed on a waitlist to review the discovery. When a laptop becomes available, the inmate may review the discovery for up to two weeks at a time, while housed in a single cell. If the inmate requires more than two weeks to review the evidence and there is a waitlist, the review will end and s/he will be added to the waitlist to re-enter the program for another two-week review period.

The DOC recently received fifteen new laptops to support its current program, bringing the total number of available laptops to twenty-three. Based on materials provided by the DOC, as of October 27, 2021, there were twenty-eight inmates on the waitlist. Accordingly, not later than November 24, 2021, every person who was on the list as of October 27 should have had an opportunity to review his or her discovery. (To be clear, the waitlist is not limited to January 6 defendants – it contains a mix of inmates from Superior Court and a variety of District Court cases.)

In addition to the DOC's current program, in collaboration with FPD and the DOC, we have developed multiple proposals to increase access by incarcerated defendants to discovery materials. The first proposal involves utilizing educational tablets that are already available for review of video footage shared by defense counsel through my.evidence.com. At this time, FPD and the government are engaged in technical discussions with American Prison Data Systems ("APDS") (the provider of the educational tablets) and Axon Enterprise, Inc. (the company that owns evidence.com), as to whether they can enable access to my.evidence.com on the tablets. APDS expects it will take at least several weeks (from November 4, 2021), to design a potential solution.

The second, independent proposal involves a pilot program in which the DOC would provide Internet connectivity and security to a room designated for discovery review in the Correctional Treatment Facility. Depending on the size of the room ultimately selected, it will accommodate ten to fifteen new laptops on which inmates will be able to review documents produced from the defense Relativity workspace to a separate Relativity workspace accessible to inmates.[1] Ideally, inmates will also be able to use Relativity to share notes about discovery materials with their attorneys. This discovery room would be staffed by a contractor who

[1] Based on the combined previous experience of representatives of APDS, FPD and the Department of Justice, the educational tablets are not a feasible solution for document review.

possesses appropriate information technology skills and experience. FPD and the government are collaborating with our respective vendors to develop an appropriate staffing solution. We intend to meet with the DOC again next week.

Substantial Completion of Discovery

Among the documents we plan to produce on a rolling basis between now and December 31, 2021 are:

- Those portions of the USCP CCV footage designated as "Security Information" pursuant to 2 U.S.C. § 1979 that do not relate to the evacuation of Congressional Members.
- The remainder of MPD BWC footage (largely consisting of footage outside the 1:00 to 6:00 p.m. timeframe), and BWC footage from Arlington County Police (124 files), and Virginia State Police (48 files);
- Video recordings made by officers of MPD's Electronic Surveillance Unit;
- Supplemental exhibits to USCP OPR reports;
- Additional MPD internal investigation reports;
- Virginia State Police and USSS radio transmissions;
- Legal process pertaining to the collection of geolocation data from electronic communications services providers;
- BWC Spreadsheet and zone maps (work product created to assist in review of BWC footage);
- Discoverable MPD, USCP and FBI records and memoranda currently in Relativity;
- Case-specific discovery of other defendants (i.e., discovery already produced to the defendant for whom it is directly relevant, but which will be made accessible to all defendants);
- Results of searches of devices and SCA accounts;
- Custodial statements of (other) defendants.
- Footage obtained from news media; and
- Grand jury transcripts and exhibits.

By the end of January 2022, we intend to provide the discoverable portions of several hundred thousand FBI records (a substantial portion of which may not be directly related to any charged defendants). These materials that have been undergoing pre-processing to ensure, among other things, that any materials that might be subject to protection under Federal Rule of Criminal Procedure Rule 6(e) are segregated for processing internally. As many documents may

not be discoverable or may be duplicative, neither the Court nor defense counsel should expect the size of the productions to the defense to mimic the size of the government's Relativity workspace. We are also currently concluding a concerted effort to consolidate scoped search results from devices and SCA accounts for ingestion by Deloitte.

By the end of January, we also intend to provide the defense an inventory of any materials that have not been loaded into either the evidence.com or Relativity workspaces to facilitate a defendant's ability to request any specific material s/he deems potentially relevant. We invite defense counsel to make specific requests as soon as possible, so that we may consider such requests in prioritizing our order of production. At that point the defense will either have or have access to the vast majority of potentially relevant materials in our possession. Given the scope of the existing investigation and its on-going nature, we expect that we will continue to obtain materials, which we will produce expeditiously.

Conclusion

In sum, we have made substantial progress in our effort to provide the defense comparable discovery review platforms for both documents and digital media, to populate those platforms, and to use alternative means to provide the most relevant discovery without delay. We will diligently continue to transfer data to our vendors, process it for production, and make interim productions by other means until the defense platforms are in place. As we continue to implement our plan, we will continue to file status memoranda with the Court on a regular basis.

UNITED STATES' MEMORANDUM
REGARDING STATUS OF DISCOVERY AS OF FEBRUARY 9, 2022

The United States files this memorandum for the purpose of describing the status of implementation of our Capitol Siege[1] global discovery plan, i.e., our plan for producing or making accessible to all defense teams voluminous data collected by the government in relation to the Capitol Siege investigation, so they may identify information they deem relevant.[2] Under our global discovery plan, the data that is being made accessible to all defendants far exceeds the information to which any defendant is entitled under Federal Rule of Criminal Procedure 16, the Jencks act, or our *Brady* obligations.[3] We are making such vast quantities of data available due

[1] The "Capitol Siege" refers to the events of January 6, 2021, when thousands of individuals entered the U.S. Capitol and U.S. Capitol grounds without authority, halting the Joint Session and the entire official proceeding of Congress for hours until the United States Capitol Police ("USCP"), the Metropolitan Police Department ("MPD"), and other law enforcement agencies from the city and surrounding region were able to clear the Capitol of rioters and to ensure the safety of elected officials.

[2] By way of illustration, the data subject to the global discovery plan includes items such as:

1. Investigations into all allegations of officer misconduct arising out of January 6, 2021 (regardless of whether sustained);
2. Thousands of hours of surveillance footage from the USCP, MPD, the United States Secret Service ("USSS"), and the Senate and House floors, and body-worn-camera ("BWC") footage from multiple law enforcement agencies that responded on January 6, 2021;
3. Radio transmissions for multiple law enforcement agencies that responded on January 6, 2021;
4. Location history data for thousands of devices that connected to the Capitol's cellular network infrastructure, or whose presence within the restricted perimeter was captured in records obtained from Google and multiple data aggregation companies;
5. Thousands of tips;
6. Relevant materials from other subjects' case files, including results of searches of digital devices, Stored Communications Act ("SCA") accounts, and interviews of other subjects, witnesses, tipsters and victims (redacted of identifying information as appropriate); and
7. All reports and exhibits related to allegations of officer misconduct or complicity on January 6, 2021.

[3] *Brady v. Maryland*, 373 U.S. 83 (1963)

to the unique circumstances of this matter, i.e., literally hundreds of similar crimes being committed in the same place contemporaneously.

This memorandum addresses the status of:

1. Production of voluminous amounts of video to the Federal Public Defender ("FPD") instance of evidence.com (access available since October 18, 2021), and the multiple tools the government has provided to assist the defense in locating footage they may consider relevant;
2. The ability of inmates housed in the D.C. Department of Corrections ("DOC") to access those same materials through a separate DOC instance of evidence.com (beginning as of February 4, 2022);
3. Voluminous documents produced since our last status memorandum dated November 5, 2021;
4. The ability of legal defense teams to obtain access to FPD's Relativity workspace (beginning as of January 21, 2022), and the current contents of that database;
5. Manner of production of voluminous documents in view of defense counsel access to Relativity (beginning as of February 3, 2022);
6. Plans for an e-discovery room in the DOC;
7. Access by inmates to laptops made available through the DOC's e-discovery program;
8. Access to voluminous discovery by *pro se* defendants;
9. Challenges we are overcoming; and
10. Our plan for certain trials that may proceed before our discovery plan is substantially executed.

***

1. Status of Production of Video Footage to FPD Instance of Evidence.com

Since our last status memorandum describing the status of discovery (dated November 5, 2021), the following video footage has been shared to the defense instance of evidence.com and is accessible to any Capitol Siege defense counsel who requests a license from FPD:

1. 1,063 files consisting of approximately 714 hours of BWC footage recorded by 675 MPD officers.
2. 104 files consisting of approximately 102 hours of BWC and pole camera footage recorded by approximately 54 Arlington County Police Department ("ACPD") officers

At this juncture, just over 24,000 files consisting of USCP closed circuit video ("CCV") footage, BWC from multiple law enforcement agencies, and USSS surveillance footage have been made available to the defense instance of evidence.com. For context, the files provided via evidence.com amount to over nine terabytes of information and would take 102 days to view. Accordingly, solely to assist Capitol Siege defense teams in identifying video files they may consider relevant in specific cases, we have also produced the following analytical and mapping tools, all of which comprise substantial government work product:

1. MPD Radio Global Positioning Satellite ("GPS") Spreadsheet: The Discovery Team learned that radios provided to MPD officers by the D.C. Office of Unified Communications ("OUC") provide GPS location data when four or more satellites are visible to the radio. Under these circumstances, the data is transmitted: (1) every ten minutes; (2) when there is an emergency activation on the radio; and (3) each time an officer pushes the button to talk over the radio. The Discovery Team obtained MPD radio GPS records for January 6, 2021 and created a spreadsheet of data that may be plotted on a time-scaled map using commercially available GPS mapping software. In many instances, the subscriber alias for a radio is an individual officer's Computer Aided Dispatch ("CAD") number and last name. Since MPD BWC footage in evidence.com is also frequently saved under an officer's CAD number and name, a particular officer's radio location information can be used to search for BWC footage from the same time and location in evidence.com;

2. BWC Summary Spreadsheet and related zone maps: This 752-page spreadsheet was initially created by over sixty individuals as an investigative tool to assist prosecutors in locating relevant BWC footage from responding law enforcement agencies including MPD, Montgomery County Police Department, and Fairfax County Police

Department. With respect to over 2,800 BWC video files, the spreadsheet provides: (1) the name and CAD number of the officer associated with the video, (2) the video start time, (3) a short summary of notable events observed by the reviewer including potential crimes observed and the time the camera appears to enter the Capitol, if any; and (4) the apparent location of the camera between noon and midnight, using 15-minute periods of duration. The locations identified correspond to zone maps that section the interior of the Capitol, the Lower West Terrace, and the Capitol Grounds into smaller areas;

3. USSS video spreadsheet: The Discovery Team created a spreadsheet containing the filenames/titles, starting times, video length, and date of USSS video;

4. 15 camera maps of the interior of Capitol Visitor's Center and the interior of the Capitol, and one camera map of the Capitol grounds. The maps depict the general location of the cameras that are identified by unique number in each USCP CCV video filename;

5. ACPD spreadsheet: The Discovery Team created a spreadsheet listing start times of handheld camera video from Arlington County Police Department; and

6. A timeline of events drafted by the USCP, beginning December 16, 2020, memorializing critical events occurring in advance of and during the Capitol Siege.

2. <u>Status of Access to Evidence.com by Defendants Housed in the D.C. Department of Corrections</u>

Through an unprecedented collaboration among the government, FPD, FPD's National Litigation Support Team ("NLST"), American Prison Data Systems ("APDS"), the DOC, and Axon Enterprise, Inc. ("Axon"), as of February 2, 2022, a separate, stand-alone instance of evidence.com has been made available to allow in-custody Capitol Siege defendants who are pending trial to view video footage. This DOC instance of evidence.com is a mirror image of the FPD instance of evidence.com. The government and FPD have drafted a memorandum of understanding describing the contents of the DOC instance, the applicable technical settings, and the requirements for inmates to obtain access. In brief, the government will make a request for an inmate to gain access to the DOC instance of evidence.com once the assigned prosecutor

notifies the Capitol Siege Discovery Unit Chief that one of the following three things has occurred:

1. The inmate has signed Attachment A to the protective order;
2. The inmate has stated on the record in court that s/he has read the protective order, reviewed it with his/her attorney, understands the protective order, and agrees to abide by it; or
3. (a) A defense attorney has represented to the assigned prosecutor in writing that they have reviewed the protective order with their client and have been authorized to sign Attachment A on their client's behalf; and (b) the defense attorney also agrees that at the next scheduled hearing in which the client is present, s/he will put on the record that s/he signed Attachment A on the client's behalf after reviewing the protective order with him or her.

Based upon information provided by APDS, as of February 9, 2022, twenty Capitol Siege inmates should have received access to evidence.com over their APDS educational tablets.[4] As of today, assigned prosecutors are still waiting for defense counsel who represent an additional fifteen Capitol Siege defendants to confirm their respective client's agreement to abide by the terms of the protective order.

3. Status of Production of Documents to Date

Global productions made to defense counsel since November 5, 2021 (Global Production Nos. 8 to 11) have continued to focus on materials most frequently requested by defendants and include items (in addition to some of the tools referenced above) such as:

1. Two new USCP Office of Professional Responsibility ("OPR") reports and 16 associated exhibits;
2. Forty additional exhibits to previously produced USCP OPR reports;
3. One hundred sixty-two USCP Use of Force reports and exhibits;
4. A collection of MPD Use of Force reports and exhibits;
5. Sixty-five video files of the Capitol Siege recorded by MPD's Electronic Surveillance Unit and six related reports;
6. Ten video files of footage from the Senate floor from the Senate Recording Studio;
7. Ten video files of footage from the House floor from the House Recording Studio;
8. Sixty-four audio recordings of Virginia State Police radio communications;

[4] Although APDS attempted to make the link accessible on February 4, there were technological issues. As of February 9, we understand that those issues have been resolved.

9. Eight audio files of USCP radio communications and conference bridge;
10. A redacted transcript of the USCP Dignitary Protection Detail radio channel;
11. 18,484 anonymous tips received by MPD;
12. Documents relevant the interstate commerce element of charged offenses; and
13. USSS files related to Vice President Elect Kamala Harris and Vice President Michael Pence's whereabouts on January 6, 2021.

These materials are substantial. For example, the exhibits to USCP OPR and MPD Use of Force reports described above include approximately 94 audio-recorded interviews of officers and witnesses (35 USCP OPR interviews and 59 MPD use of force interviews).

4. Access to FPD Relativity Workspace

On Friday, January 21, 2022, FPD circulated instructions to defense attorneys on how to gain access to the FPD Relativity workspace. Capitol Siege defense attorneys were advised that since the Relativity database is in a FedRAMP,[5] secure environment, completing the process for obtaining access is time-consuming for FPD and its vendor. Thus, counsel should expect the process for gaining access to the database to take *at least* four to five business days from when counsel first submits a Relativity License Request Form.

5. Manner of Production Going Forward

Approximately two weeks after Capitol Siege defense counsel were notified to apply for Relativity access, and after providing ample notice to defense counsel, the Discovery Team began making its global productions directly to the defense Relativity workspace and discontinued the practice of making voluminous productions via USAfx.[6] Using a defense

[5] The Federal Risk and Authorization Management Program (FedRAMP) was established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government. FedRAMP empowers agencies to use modern cloud technologies, with an emphasis on security and protection of federal information.

[6] We expect prosecutors will continue use USAfx to make productions in individual cases.

Relativity workspace to receive materials produced by the government in discovery will have several benefits for defense teams, including but not limited to avoiding any challenges they may have experienced in downloading large productions from USAfx.[7] They will no longer need to download productions to review them, as the materials will already be available for review in the database. Additional benefits will include the ability to perform keyword searches across the materials in the database, including searches of audio and video that has been "machine" transcribed.[8] Also, within the database, materials that are linked to each other (e.g., a report and multiple exhibits), will be easily identified as connected to each other for reviewing purposes, even if the materials were not initially provided in the same discovery production.[9] Notably, many of the materials we will be providing, such as thousands of tips or the results of searches of other defendants' devices and SCA accounts, would be of little value if produced in any other manner. In addition to the fact that they would likely exceed the capacity of our file transfer system or defense downloading capabilities – and thus require an enormous number of storage devices to be provided in every single case – there would be no way to search the contents universally.

[7] USAfx is merely a tool for file transfer using the Internet, while Relativity is an online search and review database. USAfx is not an optimal nor in many cases even a workable manner of transferring extremely large volumes of data.

[8] Machine transcription is an imperfect tool that is intended to assist defense teams in locating relevant information. On high-quality audio files (e.g., equivalent to a deposition or court hearing), machine-transcription is more accurate than on audio files that contain background noise or in which the speakers are not clearly enunciating (e.g., cell phone videos, custodial interviews, radio communications, voicemails).

[9] In e-discovery parlance, linked documents (such as a report and exhibits, or an email and attachments), are also known as a document "family."

Defendants will not be provided access to the FPD Relativity workspace, given the extensive volume of highly sensitive materials currently therein and those that we will produce in the future. Pursuant to the protective order issued in Capitol Siege cases, defense counsel may not permit defendants to view such materials unsupervised by defense counsel or an attorney, investigator, paralegal, or support staff person employed by defense counsel.[10] By way of illustration, highly sensitive materials currently in the database include allegations about officers' use of force or complicity with rioters (even if ultimately not sustained), and CCV camera maps of the Capitol and grounds containing information that, if further disclosed, could negatively impact the security of the U.S. Capitol. In the future, such materials will grow to include relevant materials derived from searches of subjects' digital devices and social media accounts; interviews with defendants, tipsters, witnesses, and victims; background information accumulated about investigation subjects; and financial, communications, and travel records pertaining to investigation subjects that may bear little or no relevance to most other defendants. Notably, such information may pertain to subjects who are not currently and who may never be charged.

Of course, we will continue to notify the defense of materials have been added to the FPD Relativity workspace so that counsel and defendants may collaborate to identify any materials a defendant should review in a particular case. Subject to the protective order, defense counsel can share such documents with their respective clients through a variety of mechanisms

[10] The protective order places the burden of demonstrating need for protection on the government, and it gives the assigned prosecutor ample flexibility to negotiate sensitivity designations and redactions with respect to individual documents in specific cases. It further permits defendants to contest any sensitivity designation when no agreement may be reached.

including Internet-based file transfer systems or traditional storage devices, such as hard drives, flash drives, and discs.[11]

At this juncture, the defense Relativity workspace contains Global Productions 8 to 11, and portions of Global Production No. 2 (all of which were already made accessible to defense teams via USAfx). We are in the process of transferring Global Production Nos. 1 through 7 to the defense Relativity workspace and anticipate that process will be completed this week.

Among the materials the government expects to provide in the near future are:

1. The remainder of discoverable documents we received from the USCP and MPD in response to requests by the Discovery Team.[12]

2. Over 900 records pertaining to Federal Bureau of Investigation ("FBI") interviews of law enforcement officers. These records are currently being redacted to remove information such as officer's personal telephone numbers;

3. Search warrant documents related to the FBI's collection of: (a) cell tower data from Verizon, AT&T, and T-Mobile/Sprint; (b) Google account subscriber information and

[11] FPD and its vendor are also attempting to determine if it will be possible for defendants to view selected materials within the Relativity workspace, utilizing permissions that would ensure the selected materials are viewable only by the relevant client.

[12] We have nearly completed our assessment and review of approximately 56,000 records provided by the USCP and MPD. Discoverable documents from both data sets continue to be turned over to the defense on a rolling basis. Those discoverable materials not yet produced will be shared to the FPD Relativity workspace as soon as the on-going review and redaction process is completed.

Of approximately 22,000 MPD records we received, we determined that approximately 19,300 were unique (not duplicates) and needed review. Of those, approximately 18,200 have been reviewed and deemed discoverable – they are now in the redaction process. There are still approximately 1,000 MPD records undergoing review. The remainder have been deemed not discoverable.

Of approximately 34,000 USCP records we received, we removed a large number of files from the review process because: (1) they consisted of unscoped digital devices or social media accounts, or (2) they were duplicative. At this juncture, of the remaining approximately 13,200 documents, approximately 3,000 documents are still undergoing review, and approximately 4,200 are in the process of being redacted.

location data from the Capitol and restricted perimeter, i.e., the Google geofence warrants; (c) anonymized location data collected by ten data aggregation companies; and (d) basic subscriber information for Facebook/Instagram accounts linked to the anonymized advertising identifiers obtained pursuant to the data aggregation warrants. These materials are currently being redacted to remove law enforcement sensitive information, for example, the precise location of cellular network infrastructure that provided cellular service to the Capitol on January 6, 2021;

4. Archived Parler[13] posts and comments from around the period of January 6, 2021, hosted by the Internet Archive Project and retrieved by the FBI; and

5. Videos scraped from Parler that were deemed potentially relevant to the Capitol Siege after the FBI's review of thousands of videos from a two-week period encompassing January 6, 2021.

Finally, we currently have a surge team reviewing for discoverability and sensitivity an additional 26,000 FBI documents that were previously loaded into our Relativity database. Relevant documents will be provided after appropriate redactions are completed.

6. Status of Access to Documents in Defense Team Relativity Workspace by Inmates Housed in the D.C. Department of Corrections

We continue to collaborate with FPD and DOC with respect to the creation of an e-discovery room in the Correctional Treatment Facility in which Capitol Siege defendants can access materials provided to them by counsel from the defense team Relativity workspace. The government and FPD's vendors have worked together to establish a plan for production options

[13] Parler is social media website that was used by some individuals to coordinate in advance of the Capitol Siege. *See, e.g.,* Timberg, Craig and Harwell, Drew, "*Pro-Trump forums erupt with violent threats ahead of Wednesday's rally against the 2020 election*, The Washington Post, (Jan. 5, 2021), https://www.washingtonpost.com/technology/2021/01/05/parler-telegram-violence-dc-protests/; Frenkel, Sheera, *The Storming of Capitol Hill was Organized on Social Media,* The N.Y. Times, (Jan. 6, 2021), https://www.nytimes.com/2021/01/06/us/politics/protesters-storm-capitol-hill-building.html. Parler went offline on January 10, 2021, when Amazon Web Services canceled its hosting services. *See* Room, Tony and Lerman, Rachel, "*Amazon suspends Parler, taking pro-Trump site offline indefinitely*, The Washington Post, (Jan. 11, 2021), https://www.washingtonpost.com/technology/2021/01/09/amazon-parler-suspension/. Concerned that Parler was going to be taken offline, the government attempted to collect and preserve publicly available Parler posts, comments, and videos through a variety of methods.

and formats for detained defendants. Broadly, the options under consideration would allow counsel to share productions to detained defendants in one of two ways:

1. An HTML production format that would provide a "CSV"[14] file with metadata fields and links to the documents for review. The CSV file would also contain a column in which inmates could make notes about individual documents and send them back to counsel for review. The CSV would be delivered to inmates on a storage device or via a file transfer program.

2. Productions could be viewed within the Relativity workspace in the manner being considered per footnote 11.

Fifteen laptop computers that FPD ordered to support the proposed program are in transit to FPD. The government, FPD and DOC have made significant progress on a memorandum of understanding that will govern each party's duties and responsibilities in relation to such a program.

The implementation of this solution has met with some delays recently, in part due to the need to identify individuals who would be willing to staff the room. Under the agreement in principle, FPD will be responsible for providing necessary staffing of an e-discovery room. At a bare minimum, staff will be responsible for assigning computers for review and ensuring defendants are able to access the relevant programs.[15] Finding staff with the requisite computer skills who are willing to work full-time in a correctional setting is challenging, and that challenge is further exacerbated by the existence of the COVID-19 pandemic. In any event, even if staff were currently available, it is questionable whether the program could have been made accessible

[14] A CSV (comma-separated values) file is a text file that has a specific format which allows data to be saved in a table structured format. It can be opened in a wide variety of programs and is commonly opened in Microsoft Excel and appears as a spreadsheet.

[15] Ideally, such staff would be able to provide additional support including troubleshooting issues with computers and assistance with accessing and reviewing productions.

to large groups of inmates in recent months. Pursuant to medical stay-in-place protocols issued December 22, 2021, the DOC has suspended all in-person small group activities and volunteer services in the effort to combat the spread of COVID-19.[16]

7. Status of Access to Laptops Through DOC's E-Discovery Program

In the interim, the DOC's e-discovery laptop program has presented inmates with a reasonable alternative for viewing voluminous documentation. As described in our prior submissions, there are over 20 computers in the DOC's e-discovery program, and inmates may keep them for up to two weeks at a time once they are eligible. Based on the most recent version of the laptop waitlist (dated February 4, 2022), it appears there are approximately 18-22 inmates on the waitlist, and 14 of them were added no earlier than January 21, 2022.

8. *Pro Se* Defendants

The government and FPD continue to collaborate about a discovery plan for *pro se* defendants. Currently, subject to the terms of the protective order, standby counsel can use their own licenses for the FPD instance of evidence.com to share videos with non-detained *pro se* defendants, and detained *pro se* defendants can view video in the DOC instance. As we have previously made defense counsel aware, we have agreed to waive the requirement that a defendant be supervised while reviewing highly sensitive video in cases where access is provided through evidence.com and:

1. A protective order has been entered in the relevant case;
2. The defendant has executed the written acknowledgement to the protective order (or been subject to an equivalent admonishment by the Court); and
3. The ability of the defendant to download or reshare is suppressed by counsel before the video is shared to the defendant.

[16] We understand that the DOC imminently intends to revert to the modified stay-in-place protocols that were in effect prior to December 22, 2021.

For the reasons elaborated in part 5 above, the government will not agree to providing *pro se* defendants unfettered access to FPD's Relativity workspace. However, prosecutors assigned to *pro se* case will share production indexes with both defendants and their standby counsel. Standby counsel should discuss the materials on the production index with the *pro se* defendant, and subject to the protective order, s/he can share any materials requested utilizing the same mechanisms available to represented defendants described above. Further, in those instances where a *pro se* defendant wishes to view highly sensitive documents, standby counsel or his/her staff must supervise the defendant unless: (1) the defendant and the assigned prosecutor are able to reach a suitable compromise or (2) the Court orders otherwise.

9. Challenges We Are Overcoming

In November, we projected that by the end of January 2022, we would provide the discoverable portions of several hundred thousand FBI records. We were unable to meet this goal for several reasons. Our plan was to identify all data in the FBI's case management system associated with any Capitol Siege investigation subject, and then export that data for review in Relativity (after culling it of any material arguably protected by Federal Rule of Criminal Procedure 6(e)). Our request to extract this volume of data from the FBI's case management system was unprecedented. An FBI data scientist worked closely with the developers of the FBI's case management system to create a technological solution that would identify the relevant case materials and export the data for uploading to Relativity. In November 2021, we understood that the technological solution had been successfully deployed, and we expected to receive over 400,000 documents for further discovery processing at about that time. Upon subsequent review of the export, however, our technology experts recognized that the solution developed was not as successful as originally believed. Although the materials were identified

and exported, they were no longer organized in any logical fashion, i.e., by individual investigation and in chronological order. As a result, the government was required to develop additional technological solutions to ensure that documents were associated to appropriate case files and properly sequenced before they were loaded to Relativity. This was an iterative process that took time. Efforts to move quickly were also frustrated by COVID-related quarantines and snowstorms that limited access of key personnel to the technology labs necessary to complete their work. As a result of all the above, this entire process took far longer than was originally anticipated.

Ultimately, approximately 380,000 documents from the FBI's case management system were delivered to Deloitte on February 7, 2022.[17] Given the volume of material, it may take up to ten days for it to finish being uploaded. Once these materials complete uploading, they will require in-depth analysis and customization so that they may be produced to the FPD database in a standardized format, vastly facilitating future searching and review by defense teams. This process is required prior to any human review and is expected to take an additional several weeks. During this same period, we will also leverage Relativity's analytical tools to deduplicate files, potentially eliminating thousands of documents from the need for any further review. (A highly preliminary review suggests that approximately one-third to one-half of the documents may be duplicative in nature.) During this time, we also expect to identify certain types of documents that may be "bulk-coded" as for production without the need for additional human

[17] An additional 50,000 documents that were contained in results of searches for materials potentially protected by Rule 6(e) will be separately delivered directly to the government for review. Based on recent experience, our search terms were intentionally designed to be overinclusive and we expect that a sizeable portion of these materials will be sent to our Relativity database.

review. Once the remaining materials are ready for human review, we have a surge staffing plan in place to perform review and redactions, and to quality-check proposed productions.[18]

Another challenge we continue to confront is our plan to provide defense teams the ability to view materials scoped from other subjects' devices and SCA accounts, as well as law-enforcement recorded interviews of other investigation subjects. As of today, we have provided over 900 items in these categories to Deloitte for ingestion into the government's Relativity database. Processing and loading these materials is complicated because there are no cookie-cutter solutions that may be applied to all devices and interviews. There is a wide variability in the format of results obtained from searches of digital devices and SCA accounts. Similarly, subject interviews were recorded in proprietary player formats unique to the recording devices used. All this data requires thoughtful examination and decision-making to ensure it will be accessible, organized, and searchable once it is loaded to FPD's Relativity database. In addition, we are providing assigned prosecutors a short timeframe to verify there are no security concerns with the production of such items to a global database. At this juncture, almost 300 such items have been uploaded to the government's Relativity database, and we expect to begin providing them to FPD's Relativity database shortly. We are continuing to process and upload such items on a rolling basis.

10. <u>Short-Term Discovery Plan for Certain Trials</u>

The events of January 6 were historic, not only because they represented the first time that American citizens had stormed the Capitol, but because the amount of information and

[18] The extracted FBI case files discussed above represent the FBI's Capitol Siege case files as of approximately September 2021. The lessons learned from this first extraction have led to significant improvements in the overall process. We will begin the next extraction after we complete application of the technological solution to the 50,000 documents that were contained in results of searches for materials potentially protected by Rule 6(e).

evidence involved is unprecedented. As defendants are in a better position to determine what evidence they believe is exculpatory and will help in their defense, we maintain that our plan – to provide the defense with all data that may contain such information, but in a manner that will facilitate search, retrieval, sorting, and management of that information – continues to be reasonable and appropriate.[19] Notwithstanding the challenges arising from organizing and

[19] The government's approach is also consistent with the Recommendations for Electronically Stored Information (ESI) Discovery Production developed by the Department of Justice and Administrative Office of the U.S. Courts Joint Working Group on Electronic Technology in the Criminal Justice System. *See https://www.justice.gov/archives/dag/page/file/913236/download.* It is also the generally accepted approach for ensuring that arguably exculpatory materials are provided in cases involving voluminous information.

Notably, every circuit to address the issue has concluded that, where the government has provided discovery in a useable format, and absent bad faith such as padding the file with extraneous materials or purposefully hiding exculpatory material within voluminous materials, the government has satisfied its obligations under *Brady v. Maryland*, 373 U.S. 83 (1963) and progeny. *See United States v. Yi*, 791 F. App'x 437, 438 (4th Cir. 2020) ("We reject as without merit Yi's argument that fulfillment of the Government's obligation under *Brady* requires it to identify exculpatory material."); *United States v. Tang Yuk*, 885 F.3d 57, 86 (2d Cir. 2018) (noting that the "government's duty to disclose generally does not include a duty to direct a defendant to exculpatory evidence within a larger mass of disclosed evidence") (internal citations omitted); *United States v. Stanford*, 805 F.3d 557, 572 (5th Cir. 2015) ("We have previously rejected such 'open file' *Brady* claims where the government provided the defense with an electronic and searchable database of records, absent some showing that the government acted in bad faith or used the file to obscure exculpatory material."); *United States v. Gray*, 648 F.3d 562, 567 (7th Cir. 2011) ("The government is not obliged to sift fastidiously through millions of pages (whether paper or electronic). . . [and] is under no duty to direct a defendant to exculpatory evidence [of which it is unaware] within a larger mass of disclosed evidence.") (quotation marks and citations omitted); *Rhoades v. Henry*, 638 F.3d 1027, 1039 (9th Cir. 2011) (rejecting *Brady* claim on the ground that the defendant "points to no authority requiring the prosecution to single out a particular segment of a videotape, and we decline to impose one"); *United States v. Warshak,* 631 F.3d 266, 297 (6th Cir. 2010) ("As a general rule, the government is under no duty to direct a defendant to exculpatory evidence within a larger mass of disclosed evidence"); *United States v. Skilling*, 554 F.3d 529, 576 (5th Cir. 2009)(same), aff'd in part, vacated in part, remanded, 561 U.S. 358 (2010); *United States v. Pelullo*, 399 F.3d 197, 212 (3d Cir. 2005) ("*Brady* and its progeny . . . impose no additional duty on the prosecution team members to ferret out any potentially defense-favorable information from materials that are so disclosed."); *United States v. Jordan,* 316 F.3d 1215, 1253-54 (11th Cir. 2003) (concluding that the defendant's demand that the government "identify all of the *Brady* and *Giglio* material in its possession," "went far beyond" what the law requires).

producing unprecedented amounts of data that are frequently complex in nature, our plan is being executed promptly and in good faith. We have produced terabytes of organized and searchable data in hundreds of cases and continue to do so as quickly as possible.

In addition, we have developed a short-term discovery plan that will enable certain trials to proceed before our discovery plan is substantially executed. To be clear, this is not the plan we recommend, nor one that would be workable in multiple cases or complex cases. Time spent executing this plan will reduce resources available to execute the global plan described above. Pursuant to our short-term plan, we will create lists describing substantially all our holdings. Defense teams can review the lists to request specific items they believe may be relevant. We expect these lists will identify the physical and digital evidence that has been accumulated across all Capitol Siege investigations; and categories of potentially discoverable information from materials that are in our possession but have not yet been produced in global discovery, e.g., the FBI materials recently provided to Deloitte; small amounts of material from other law enforcement agencies that played a role on the January 6, 2021; damage estimates from the Architect of the Capitol; and grand jury transcripts.[20]

In addition, pursuant to this plan, assigned prosecutors will ensure that searches based on the defendant's personal and/or device identifiers, as relevant, have been or will be conducted within of the following sets of data, as appropriate:

[20] If additional materials requested by defense teams are extensive, we will likely need to request a continuance and tolling of the Speedy Trial Act to allow the defense adequate time to prepare for trial. This is especially true in the case of requests for the results of multiple other subjects' digital devices and SCA accounts that have not yet been scoped for relevant information. Further, if the requested materials have not been loaded and organized within our Relativity database yet, they will be turned over in their native format and the defendant will be unable to leverage FPD's Relativity's search tools to review them.

1. Cell tower data from Verizon, AT&T, and T-Mobile/Sprint Cell for devices that connected to the Capitol's cellular network infrastructure;

2. Google account subscriber information and location data from the Capitol and restricted perimeter obtained pursuant to the Google geofence warrants;

3. Location data obtained by the FBI from multiple data aggregation companies;

4. Basic subscriber information and call records obtained pursuant to applications made to twelve cell service providers under 18 U.S.C. 2703(d) for devices that, according to location data obtained pursuant to the Google geofence warrants, were present within the U.S. Capitol on January 6, 2021;

5. A repository of Archived Parler posts and comments from around the period of January 6, 2021, hosted by the Internet Archive Project and retrieved by the FBI;[21]

6. A repository of digital media tips maintained by the FBI; and

7. The government's discovery databases.

We will also perform searches of the data described above in response to defense counsel requests for materials that we are obligated to produce under Federal Rule Criminal Procedure 16, the Jencks Act, and our *Brady* obligations.[22]

Further, prosecutors will ensure that a facial recognition search has been performed within a repository of images and video that the FBI continually populates, so that all identifiable images of the defendant within that repository at a time close to trial are produced.

[21] Items 1-4 will never be provided *en masse* in global discovery because they contain highly sensitive personal identifying information for members of Congress, their staff, and law enforcement who were all lawfully present on January 6, 2021, and the process of locating that information and eliminating it from these results continues even today.

[22] We will not perform searches for materials that are not required pursuant to the above-described obligations. We advise defendants who wish to perform wider-ranging searches to wait for the substantial completion of our global discovery plan.

Finally, prosecutors will confirm that FBI case agents conduct searches of FBI databases before trial, to ensure that all relevant documents concerning a specific case or any witnesses have been identified and produced.

Conclusion

The government has taken its Capitol Siege discovery obligations seriously from the inception of this investigation and has made substantial efforts to produce vast quantities of information that is varied and frequently complex in nature in hundreds of cases. These efforts have included:

- Appointing a Capitol Siege Discovery Coordinator in January 2021;
- Assembling a Capitol Siege Discovery Team consisting of experienced attorneys, project managers, and litigation technology professionals;
- Collecting information from multiple sources involved in the response to and investigation of the Capitol Siege;
- Collaborating with FPD to develop a standard protective order for Capitol Siege cases;
- Identifying database solutions for making terabytes of video and documents accessible to hundreds of defendants;
- Funding defense databases and obtaining licenses for all Capitol Siege defense counsel, and collaborating with FPD to execute these solutions;
- Reviewing specific discovery requests by defense counsel to ensure the appropriate materials are prioritized for production;
- Creating protocols and procedures to ensure that (a) case-specific discovery is provided, (b) defendants will receive complete copies of their own unscoped devices and SCA accounts upon request; (c) devices and SCA accounts are systematically filtered for attorney-client communications; (d) relevant scoped digital data and custodial interviews will be uploaded to the government's discovery databases for production to all; and (e) increasing access to discovery by detained defendants.

We have now made substantial progress in our effort to provide the defense appropriate discovery review platforms for both documents and digital media, to populate those platforms, and to use alternative means to provide the most relevant discovery without delay. We will diligently continue to transfer data to our vendors, process it for production, and make productions as expeditiously as possible. As we continue to implement our plan, we will continue to file status memoranda with the Court on a regular basis.