UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	**CASE NO. 1:21-cr-00218-APM**
v.	:	
	:	
CLARK, ET AL.,	:	
	:	
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 drafted 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 August 23, 2021;
2. Memorandum Regarding Status of Discovery as of September 14, 2021; and
3. Memorandum Regarding Status of Discovery as of October 21, 2021.

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

By: */s/ Emily A. Miller*
EMILY A. MILLER
Capitol Breach Discovery Coordinator
DC Bar No. 462077
555 Fourth Street, N.W., Room 5826
Washington, DC 20530
Emily.Miller2@usdoj.gov
(202) 252-6988

By: */s/ Anne Veldhuis*
Anne Veldhuis
Trial Attorney, Detailee
CA Bar No. 298491
450 Golden Gate Ave. Room. 10-010
San Francisco, CA 94102
anne.veldhuis@usdoj.gov
415-307-6722

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results of searches of devices and Stored Communications Act ("SCA") accounts, digital media tips, Parler video, and unpublished news footage), and hundreds of thousands of investigative documents including but not limited to interviews of tipsters, witnesses, investigation subjects,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. The Workflow in Processing Materials for Discovery Takes Time.

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.