UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	**CASE NO. 1:21-MJ-00371**
v.	:	
	:	
TRACI J. SUNSTRUM	:	
	:	
Defendant.	:	

UNITED STATES' MEMORANDUM REGARDING STATUS OF DISCOVERY

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.

Discovery Provided

Early discovery has already been provided, which should be the most directly relevant materials to the defendant. The United States has either already turned over or will soon make available any grand jury materials; serials with officer notes; copies of the defendant's searched devices and accounts; copies of raw collections from the defendant's devices and accounts (only at counsel's request); the results of checks of defendant's known identifiers against voluminous data such as tips, tower dumps and geofence results; specific relevant clips of BWC and CCV; and summary reports containing images of the defendant identified by the FBI in reviewing various sources of footage (to include digital media tips, CCV, and BWC). We have also already arranged six opportunities for defense counsel and an investigator to walk through the crime scene, which required the USCP to obtain the approval of many different Congressional offices to obtain access to various areas that are relevant to the charges being brought.

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

[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.

promote efficiency, security, and reduced costs; and (5) taking reasonable and appropriate measures to secure ESI discovery against unauthorized access or disclosure.

Respectfully submitted,

CHANNING D. PHILLIPS
Acting United States Attorney

By: */s/ Jacob J. Strain*
JACOB J. STRAIN
Utah Bar No. 12680
Assistant United States Attorney
U.S. Attorney's Office for District of Columbia
555 4th Street, N.W.
Washington, D.C. 20530

By: /s/
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/
GEOFFREY A. BARROW
Capitol Breach Discovery Team, Detailee
DC Bar No. 462662
1000 Southwest Third Avenue, Suite 600
Portland, Oregon 97204
Geoffrey.Barrow@usdoj.gov
(503) 727-1000

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."