U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

MEMORANDUM

To: Case File, *USvEpstein*, 2018R01618

From: [redacted], [redacted], [redacted]

Subject: Search Warrant Responsiveness Review Protocol for Image and Video Files from Epstein Devices

Date: October 19, 2020

==========

This memorandum is intended to memorialize the protocol for conducting a responsiveness review of image and video files obtained pursuant search warrants in the above-referenced investigation.

BACKGROUND

In July of 2019, the Federal Bureau of Investigation ("FBI") executed multiple search warrants on the New York residence of Jeffrey Epstein. During those searches, the FBI seized dozens of electronic devices. Pursuant to the warrants authorizing those searches, the FBI extracted data from those electronic devices. In August of 2019, the FBI executed a search warrant on the Virgin Islands residence of Jeffrey Epstein. During that search, the FBI seized approximately dozens of additional electronic devices. The FBI subsequently obtained a warrant authorizing the search of those devices.

During the initial review of data from the devices seized during the New York and the Virgin Islands searches, the FBI and U.S. Attorney's Office identified materials relevant to its investigation of Ghislaine Maxwell. On June 26, 2020, the FBI obtained a new warrant (the "Warrant") authorizing review of the data from a total of 62 devices seized from both the New York and Virgin Islands searches of Epstein's residence (the "Devices"). Following the issuance of the Warrant, the FBI provided the U.S. Attorney's Office with copies of all documents extracted from the Devices. The U.S. Attorney's Office then began conducting a privilege review of those documents, some of which has been completed and some of which remains ongoing. Upon completion of the privilege review, the AUSAs responsible for the prosecution have been conducting a responsiveness review by running search terms designed to capture documents that are responsive to the Warrant.

On July 2, 2020, Maxwell was arrested on Indictment 20 Cr. 330 (AJN), charging her with crimes involving the sexual abuse of minors. Judge Nathan has ordered that all discovery be

completed by November 9, 2020. The AUSAs responsible for the prosecution are in the process of producing responsive documents from the Devices to Maxwell.

In addition to documents, the FBI also extracted image and video files from some of the Devices. The FBI and U.S. Attorney's Office intend to review those image and video files for materials that are responsive to the Warrant. In order to meet the November 9, 2020 discovery deadline, this review needs to be completed **by October 31, 2020** to allow adequate time to stamp and load responsive files onto drives for production to the defense.

RESPONSIVENESS REVIEW:

The purpose of this responsiveness review protocol is to guide the review and seizure of image and video files obtained pursuant to the Warrant. Before any member of the review team undertakes the work set forth herein, he/she must review the search warrant and accompanying affidavit pursuant to which the materials were produced or seized.

Each member of the review team will be assigned to conduct a file-by-file review of the images and videos from a particular subset of the Devices. Files falling into any of the following categories shall be considered responsive to the Warrant:

- Any image or video of Jeffrey Epstein
- Any image or video of Ghislaine Maxwell
- Any image or video of any female appearing to be under the age of 30
- Any travel documents, such as passports, visas, or immigration forms
- Any screenshots of communications with or regarding females
- Any screenshots of social media posts featuring or regarding females

Upon identifying any file that falls within one of the above categories, the reviewer shall take the following steps:

- If the image or video contains partial or full nudity, mark the file RESPONSIVE – HIGHLY CONFIDENTIAL
- If the image contains no nudity of any kind, mark the file RESPONSIVE – CONFIDENTIAL

Reviewers from the U.S. Attorney's Office should complete this review as follows:

- Create a local folder (not on a shared network drive) for each device reviewed, identified by the device's "NYC" serial number.
- Within each device folder, create one subfolder entitled RESPONSIVE – HIGHLY CONFIDENTIAL, and one subfolder entitled RESPONSIVE – CONFIDENTIAL.
- Review the files from each assigned device on the drive provided. Copy any responsive files into the appropriate subfolder for each device reviewed.
- Upon completion of review, all folders entitled RESPONSIVE – HIGHLY CONFIDENTIAL will be copied onto an external drive and provided to the FBI for secure storage. HIGHLY CONFIDENTIAL materials should **not** be saved onto the U.S. Attorney's Office network or produced directly to defense counsel. The FBI will maintain HIGHLY CONFIDENTIAL materials and make them available to the defense for review.

- Upon completion of review, all folders entitled RESPONSIVE – CONFIDENTIAL will be kept separated by device number and produced as CONFIDENTIAL discovery to defense counsel.

Reviewers from the FBI should use the CAIR system to complete this review.[1] Upon completion of the review, the FBI will take the following steps:

- Securely save all files marked RESPONSIVE – HIGHLY CONFIDENTIAL within the FBI, keeping the files separated by device. The case agent will memorialize this process and the location of these materials in a 302 report.
- Provide a copy of all files marked RESPONSIVE – CONFIDENTIAL to the U.S. Attorney's Office, keeping the files separated by device. The U.S. Attorney's Office will produce these files as discovery to the defense.

At the conclusion of the review, the U.S. Attorney's Office will delete or return all copies of the full image and video files from all Devices. Also at the conclusion of the review, the FBI will lock off access to the full data extractions of all Devices. This process will ensure that the FBI and U.S. Attorney's Office will **only** be able to review, access, and use the portions of the Devices identified as responsive to the Warrant for further investigation and prosecution. If it is determined that there is a need to review items not identified as responsive, the FBI will need to seek a new warrant to review the full contents of any of the Devices.

If reviewers have any questions or would like to discuss the protocol or review, they should contact AUSA [redacted] by calling [redacted] cellphone at [redacted], or emailing her at [redacted]. Reviewers are encouraged to contact AUSA [redacted] at any time and with any questions or concerns, no matter how small.

[1] All other data review in connection with the above-referenced warrants should be conducted using Relativity. The CAIR database should not be used to conduct a responsiveness review of emails or documents.