IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, v. MATTHEW WILLIAM SCHWIER, Defendant.	Case No. 3:17-cr-00095-SLG

AMENDED PROTECTIVE ORDER

For the reason's set forth in the Court's Order re Motions for Reconsideration,[1]:

1. Not later than January 27, 2020, the government will provide a government-owned computer (the "TD Computer") at the Orange County Regional Computer Forensics Laboratory ("OCRCFL"), located at 3800 W. Chapman Avenue, Suite 800, Orange, CA 92868. The TD Computer shall be configured to the specifications provided by the defense on December 6, 2019.[2]
2. The only non-government persons who will have access to the TD Computer are Jeffrey Fischbach and Robert Herz

[1] *See* Docket 304.

[2] *See* Docket 280-1 at 1.

(collectively "the defense").

3. Beginning on January 28, 2020, the defense will have access to the TD Computer for 30 consecutive calendar days of testing Torrential Downpour versions 1.15 and 1.23, the versions used in the investigation in this matter. Actual testing days are expected to be Monday through Friday only, exclusive of federal holidays.

4. Government personnel will have access to the TD Computer only for the purposes of keeping the TD computer secure consistently with OCRFCL standard operating procedures. Government personnel will not observe the defense testing.

5. Installation of Torrential Downpour software onto the TD Computer will occur as follows:

   a. An FBI agent or Task Force Officer will keep exclusive possession of a USB drive or other removable media containing the Torrential Downpour software, except as provided in (b) and (c) below. The defense will not possess the Torrential Downpour software, other than on the TD Computer, except as provided in (b) and (c) below.

b. Prior to testing, the FBI agent or Task Force Officer will allow Mr. Fischbach to install Torrential Downpour versions 1.15 and 1.23 onto the TD Computer. The FBI agent or Task Force Officer will remain outside the Defense Review room while Mr. Fischbach installs the software.

c. After the installation, Mr. Fischbach will remove the USB drive or other removable media containing the TD Software from the TD Computer and return it to the FBI agent or Task Force Officer.

6. The defense may bring digital media, computers, cell phones, and an internet hotspot (*i.e*. one that is compatible to connect to the TD Computer via WiFi or a network card) into the OCRCFL room with the TD Computer.

7. The defense will only connect to the TD Computer as necessary to complete its testing. The TD Computer may access the internet through the network card or via WiFi.

8. The defense will not remove the TD Computer from the OCRCFL.

9. The defense will not copy Torrential Downpour to any device

other than the TD Computer. The defense will not receive Torrential Downpour source code.

10. Neither the defense nor the TD Computer will have access to law enforcement's database of hash values from known child pornography images, known as "ICAC COPS."

11. The defense will not tamper with or open the TD Computer.

12. The Court reaffirms its prior protective order, entered at Docket 231.

DATED this 13th day of January, 2020, at Anchorage, Alaska.

/s/ Sharon L. Gleason
UNITED STATES DISTRICT JUDGE