EXHIBIT A

U. S. Department of Justice

Special Counsel

Washington, D.C. 20530

May 6, 2022

Via Email

Michael Bosworth, Esq.
Sean M. Berkowitz, Esq.
Latham & Watkins LLP

Re: United States v. Michael A. Sussmann
Crim. No. 21-cr-00582 (CRC)

Dear Counsel:

We write to provide the following supplementary detail, in response to your request for additional specifics on the substance of Special Agent David Martin's expected testimony as outlined in Section I of our prior disclosure ("Domain Name System Data and Analysis").

With regard to Special Agent David Martin's expected testimony concerning the nature and types of conclusions that can – and cannot – be drawn about persons' or entities' online activities based on a review of DNS data, we expect Agent Martin to state, in substance and in part, and among other things:

- The mere existence of a DNS lookup does not in and of itself reflect or prove the existence of actual communications between IP addresses (such as emails).
- The mere existence of a DNS lookup also does not in and of itself reflect or prove the existence of an actual connection or exchange of substantive information between computers (*e.g.*, web browsing or file transfers).
- There are a number of other events and causes that can trigger or initiate DNS lookups, including security scanning by automated systems/software, spam filtering, and other Internet "noise."
- DNS communications can be "spoofed" through a process whereby a DNS lookup is made to appear falsely to originate from a particular IP address. In such a scenario, the automated response from the receiving IP address is directed to the "spoofed" domain/IP address.

With regard to Special Agent David Martin's expected testimony concerning the analytic significance and conclusions that can be drawn based on the provenance and origins (*e.g.*

collection source) of DNS data, we expect Agent Martin to state, in substance and in part, and among other things:

- The nature and strength of the conclusions that can be drawn from a given DNS dataset depend, in part, on the "visibility" of the collection source, namely, the percentage of all global DNS traffic that is available to the collection source.
- The more expansive the "visibility" of a collection source (*i.e.*, the greater percentage of global DNS traffic that is available to the source), the more conclusions (and stronger conclusions) can be drawn about a particular DNS dataset.
- For example, if a company collecting passive DNS data has access to 100% of the world's DNS traffic, then searches or queries across its data would permit the collector of the data to draw definitive conclusions about the number of DNS lookups between particular IP addresses/domains. If a company has access to 2% of the world's DNS traffic, then searches or queries across its data would permit the collector of the data to draw only limited conclusions.
- It is impossible to know the precise percentage of worldwide DNS data that a particular collection source covers.
- It nevertheless can be important for an analyst of DNS data to consider the collection source and the visibility of that source.

Sincerely,

JOHN H. DURHAM
Special Counsel

By: */S/ Brittain Shaw*
Jonathan E. Algor IV
Andrew J. DeFilippis
Michael Keilty
Brittain Shaw
Assistant Special Counsels