EXHIBIT A

U.S. Department of Justice

Special Counsel

March 30, 2022

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

Dear Counsel:

Pursuant to Federal Rule of Criminal Procedure 16(a)(1)(G), the government provides notice of its intention to call an expert witness at the upcoming trial of defendant Michael Sussmann to testify regarding Domain Name System ("DNS") data and other matters relevant to cyber investigations. As detailed below, the government hereby discloses that it intends to call FBI Unit Chief/Special Agent David Martin, who is currently assigned the FBI's Cyber Division, Technical Analysis Unit.

The government also provides attached hereto a copy of UC Martin's *curriculum vitae*.

I. Domain Name System Data and Analysis

As set forth in the Indictment, the data underlying the allegations that the defendant provided to the FBI and Agency-2 was purported DNS data. The primary purpose of UC Martin's testimony will be to describe for the jury the basic mechanics, architecture, and terminology of the DNS system and DNS data so that they can understand various technical concepts that appear in documents and other evidence that the Government will offer at trial. UC Martin's testimony will explain, for example, that DNS is a naming system for devices connected to the Internet that translates recognizable domain names, *e.g.,* http://www.google.com, to numerical IP addresses, *e.g.*, 123.456.7.89. He will further explain that a DNS "lookup" refers to an electronic request by a particular computer or device from another device or server. UC Martin will also describe how DNS lookups are initiated and processed, and how various DNS data and records are maintained on electronic servers and systems associated with DNS.

As part of his testimony, UC Martin will describe how certain private companies and entities maintain DNS "resolvers" and, in some cases, offer "DNS resolution services" to their customers. In explaining these concepts, he will also explain how DNS data is typically processed and stored by these and other entities. He will further describe how certain private parties can and do gain access to DNS data, and how certain companies collect and commercialize DNS data, including what is referred to as "passive DNS data."

UC Martin will also provide the jury with specific examples of DNS data in order to describe the interpretation and meaning of such data, including particular fields that appear within the data. He will further testify 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. He will also testify about the analytic significance and conclusions that can be drawn based on the provenance and origins (*e.g.*, collection source) of DNS data.

II. TOR

As part of his testimony, UC Martin will also explain the Onion Router ("TOR"), which is a free and open-source software for enabling anonymous communications. He will describe common terms used in connection with TOR, including the concept of a "TOR exit node." (As you are aware, a white paper that the defendant submitted to FBI General Counsel Baker contained assertions about the purported use of a TOR exit node by the Trump Organization and Alfa Bank.) UC Martin will explain common uses of TOR, as well as investigative steps and methods for analyzing online activities involving TOR.

III. Additional Testimony

You have indicated in recent discussions that you may seek to limit the testimony and evidence at trial concerning the purported DNS data solely to that which reflects the defendant's state of mind and subjective understanding of the purported DNS data at issue in this case. We therefore understand that you are not currently inclined to offer evidence, or engage in questioning, that would imply, assert, or seek to prove the authenticity of the relevant DNS data or the actual truth of the allegations at issue concerning a secret channel of communications between the Trump Organization and Alfa Bank. If the defense, however, does cross examine Government witnesses or calls its own witnesses to testify in a manner that seeks to establish or encourage particular conclusions in this regard, then the Government reserves the right to have UC Martin testify concerning:

- the authenticity *vel non* of the purported data supporting the allegations provided to the FBI and Agency-2;

- the possibility that such purported data was fabricated, altered, manipulated, spoofed, or intentionally generated for the purpose of creating the false appearance of communications;

- whether the DNS data that the defendant provided to the FBI and Agency-2 supports the conclusion that a secret communications channel existed between and/or among the Trump Organization, Alfa Bank, and/or Spectrum Health;

- whether DNS data provided to Agency-2 supports the conclusion that Donald Trump and/or his associates used one or more Russian-made phones in the

vicinity of Trump Tower, Trump's Central Park West Apartment Building, Spectrum Health, and the White House; and

- the validity and plausibility of the other assertions and conclusions set forth in the various white papers that the defendant provided to the FBI and Agency-2;

* * *

The government reserves the right to call additional expert witnesses and/or substitute expert witnesses. The government will comply with its obligations under Federal Rule of Criminal Procedure 16(a)(1)(G) and Federal Rules of Evidence 702, 703, and 705. The government will notify you in a timely fashion of any additional or substitute experts that the government intends to call at trial and provide you with a summary of the experts' opinions. The Government will supplement this notice as appropriate and as more information becomes available.

Finally, the government renews its request for reciprocal discovery, including any and all expert disclosures.

Very truly yours,

JOHN H. DURHAM
Special Counsel

By: /s/_____
Jonathan E. Algor
Andrew J. DeFilippis
Michael Keilty
Brittain Shaw
Assistant Special Counsels

CURRICULUM VITAE

David M. Martin, GSE
Unit Chief
Federal Bureau of Investigation
Cyber Technical Analysis Unit
PHONE: 703-633-6932
dmmartin@fbi.gov

PROFESSIONAL EXPERIENCE

Feb 2022 – Present

Unit Chief
FBI Cyber Division
Cyber Technical Analysis Unit
Chantilly, VA

Lead a team of over 50 FBI employees and contractors responsible for the FBI Cyber Division's Advanced Digital Forensics, Malware Automation, Data and Network Analysis, and New and Emerging Technology programs. Responsible for establishing unified ingest and processing system for all FBI Cyber technical data, establishing best practices and performing technical review of all reporting produced by CTAU.

Nov 2021 – Feb 2022

Supervisory Special Agent / Acting Unit Chief
FBI Cyber Division
Cyber Technical Analysis Unit
Chantilly, VA

Program manager for the Advanced Digital Forensics program, which provides digital forensics and malware reverse-engineering services for the most complex computer intrusion cases across all FBI field offices and conducts technical review of Cyber intelligence products. Managed personnel, prioritized cases, and reviewed reports for accuracy, completeness, and investigative value.

Oct 2017 – Nov 2021

Supervisory Special Agent
Cyber Action Team Director
FBI Cyber Division
Cyber Technical Operations Unit
Chantilly, VA

Established the vision and direction for CAT while directing all operations and deployments. Managed the selection, training and readiness of CAT personnel and the procurement, development and maintenance of a wide range of specialized equipment and software needed to accomplish the team's mission.

Sep 2015 – Sept 2017 **Supervisory Special Agent**
FBI Cyber Division
Technical Operations Unit
Chantilly, VA

Managed the development and implementation multiple technical operations using a variety of techniques and technical platforms to target criminal and nation-state cyber threat actors. Served as a Team Lead on CAT and led multiple domestic and foreign deployments

July 2009 – Sep 2015 **Special Agent**
Detroit Cyber Task Force
FBI Detroit Field Office
Detroit, MI

Conducted investigations into matters criminal and national security computer intrusions, intellectual property rights, online child involving computer intrusions that affect the security of the United States or are conducted in violation of Federal Statutes. Prepared cases for presentation to the United States Attorney's Office for prosecution. Testified before Federal Grand Juries and in Federal District Court. Conducted forensic examinations on computer evidence; analyzed network traffic, log files and unknown binary files for evidence of computer intrusion activity.

Dec 2002 – July 2009 **Senior Police Officer / Acting Sergeant**
Littleton Police Department
Littleton, CO

Responsible for responding to emergencies, investigating criminal and suspicious activity, making arrests and issuing citations as a Patrol officer and the primary relief supervisor for a patrol shift. I held ancillary duties as a SWAT Operator, Crisis Intervention Team member, Field Training Instructor, Firearms Instructor, Defensive Tactics Instructor and Computer Automation Instructor.

April 2001 – July 2002 **Computer Crime Specialist**
Colorado Bureau of Investigation
Lakewood, CO

Assisted in computer crime investigations, including child sexual exploitation, internet fraud, and other felonies involving the use of a computer. Conducted forensic examinations of computer evidence. Developed and maintained software applications, hardware and computer networks for the Investigations Division.

EDUCATION

Oct 2014 – July 2017 **SANS Technology Institute**
Baltimore, MD
Master of Science in Information Security Engineering

Sept 1998 – June 2002 **University of Denver**
Denver, CO
Bachelor of Science in Computer Science and Psychology
Minors in Math and Business Administration

PROFESSIONAL TRAINING

Aug 2021	Hacking and Securing Cloud Infrastructure Black Hat, Online (32 Hours)
Aug 2019	Splunk Administration Splunk, Reston VA (40 Hours)
Aug 2017	IDA Pro Basic and Advanced Black Hat, Las Vegas NV (32 Hours)
Oct 2016	SEC 566 – Implementing and Auditing the Critical Security Controls SANS Institute, Online (36 hours)
June 2016	MGT 525 - IT Project Management SANS Institute, Washington, DC (36 hours)
Aug 2014	SEC 504 - Hacker Techniques, Exploits and Incident Handling SANS Institute, Boston, MA (48 hours)
July 2014	FOR 610 - Reverse Engineering Malware: Malware Analysis Tools and Techniques SANS Institute, Online (48 Hours)
Feb 2014	FOR 508 - Advanced Computer Forensic Analysis and Incident Response SANS Institute, Online (48 Hours)
Aug 2013	FOR 408 - Computer Forensic Investigations: Windows In-Depth SANS Institute, Online (48 Hours)
Aug 2012	Forensic Toolkit Bootcamp Access Data, Baltimore, MD (24 Hours)
May 2012	Digital Extraction Technician (DExT) / CART Technician FBI Computer Analysis and Response Team (CART), Quantico, VA (72 Hours)
Dec 2011	SEC 503 - Intrusion Detection In-Depth SANS Institute, Washington, DC (48 Hours)
July 2011	CYD 3450 – Intrusion Response Mandiant, St. Louis, MO (32 Hours)
May 2011	CYD 3350 – Network Traffic Analysis Mandiant, Richmond, VA (24 Hours)
April 2011	CYD 3310 – Advanced Network Investigation Techniques – UNIX Mandiant, Denver, CO (24 Hours)

March 2011	SEC 401 – Security Essentials Bootcamp Style SANS Institute, Phoenix, AZ (48 Hours)
Feb 2011	CYD 1125 – Cyber Stage 2 Training/Windows Intrusion Response Mandiant/FBI Academy, Quantico, VA (80 Hours)
Sep 2010	Basic Online Undercover Course FBI Innocent Images, Calverton, MD (40 Hours)
Sep 2010	CYD 2300 – Wireless Technology Mandiant, Calverton, MD (16 Hours)
July 2010	CYD 2200 – Network+ Certification FBI Cyber Division, Calverton, MD (40 Hours)
March 2010	CYD 1200 – A+ Certification FBI Cyber Division, Calverton, MD (80 Hours)
Jul-Nov 2009	New Agents Training FBI Academy, Quantico, VA (776 Hours)
2008	Law Enforcement Supervisory Institute Colorado Peace Officer Standards and Training, Centennial, CO (40 Hours)
2006	Field Training Instructor Certification Kaminsky and Associates, Littleton, CO (40 Hours)
2006	Internet Investigations and Windows Forensics Microsoft/Colorado Attorney General's Office (32 Hours)
2005	Interview and Interrogation John E. Reid and Associates, Aurora, CO (40 Hours)
2002	Computer Crime and Digital Evidence Techniques Colorado Association of Computer Crime Investigators, Golden, CO (16 Hours)

CERTIFICATIONS & AWARDS

July 2019	Countering Technical and Cyber Threats Award - National Counterintelligence and Security Center
Oct 2018	US Attorney's Award – United States Attorney's Office, Eastern District of Michigan
Oct 2017	Attorney General's Award for Excellence in Information Technology – US Department of Justice
May 2017	GIAC Security Expert (GSE) - Global Information Assurance Certification
Nov 2016	GIAC Critical Controls Certification (GCCC) - Global Information Assurance Certification
Aug 2016	GIAC Certified Project Manager (GCPM) - Global Information Assurance Certification

Sept 2014	GIAC Certified Incident Handler (GCIH) - Global Information Assurance Certification
July 2014	GIAC Reverse Engineering Malware (GREM) – Global Information Assurance Certification
May 2014	US Attorney's Award – United States Attorney's Office, Eastern District of Michigan
Feb 2104	GIAC Certified Forensic Analyst - GOLD (GCFA) - Global Information Assurance Certification
Aug 2013	GIAC Certified Forensic Examiner (GCFE) - Global Information Assurance Certification
May 2012	DExT / CART Tech Certification – FBI
April 2012	GIAC Certified Intrusion Analyst – GOLD (GCIA) - Global Information Assurance Certification
April 2011	GIAC Security Essentials Certification – GOLD (GSEC) - Global Information Assurance Certification
July 2010	Network+ Certification – CompTIA
March 2010	A+ Certification – CompTIA
June 2004	Medal of Valor – Littleton Police Department
July 2002	Director's Award – Colorado Bureau of Investigation

PUBLICATIONS & PRESENTATIONS

Oct 2019	Speaker: "Already Pwn3d: Deep Dive into Incident Response and Forensics Data," Splunk .conf 2019, Las Vegas NV
Feb 2017	Peer-reviewed research paper: "OS X as a Forensic Platform," SANS Institute
Dec 2016	Speaker: "Gh0st in the Dshell: Decoding Undocumented Protocols," SANS Cyber Defense Institute 2016, Washington DC.
June 2016	Peer-reviewed research paper: "Gh0st in the Dshell: Decoding Undocumented Protocols," SANS Institute
April 2016	Speaker: "Tracing the Lineage of DarkSeoul," SANS Northern Virginia 2016, Reston VA
March 2016	Peer-reviewed research paper: "Tracing the Lineage of DarkSeoul." SANS Institute