IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. JULIAN PAUL ASSANGE, *Defendant*.	CRIMINAL NO.: 1:18-CR-111

AFFIDAVIT IN SUPPORT OF REQUEST FOR EXTRADITION
OF JULIAN PAUL ASSANGE ON SECOND SUPERSEDING INDICTMENT

I, Gordon D. Kromberg, being duly sworn, depose and state:

1. I make this affidavit in support of this Extradition Request of the United States of America to the United Kingdom of Great Britain and Northern Ireland for the extradition of Julian Paul Assange (ASSANGE), who is believed to be a citizen of Australia and Ecuador. This Extradition Request seeks ASSANGE's extradition on charges alleged in a Second Superseding Indictment filed in this case on June 24, 2020, as described further below.

2. I have made four previous declarations in support of the request for extradition of Julian Paul Assange, and incorporate here the description of my background and qualifications that I included in the first of those previous declarations. See Gordon Kromberg, Declaration in Support of Request for Extradition of Julian Paul Assange ¶¶ 1-4 (Jan. 17, 2020) (hereafter, "Kromberg First Declaration"); Gordon Kromberg, Supplemental Declaration in Support of Request for Extradition of Julian Paul Assange ¶¶ 1-3 (Feb. 19, 2020) (hereafter, "Supplemental Kromberg Declaration"); Gordon Kromberg, Second Supplemental Declaration in Support of Request for Extradition of Julian Paul Assange ¶ 1 (Mar. 12, 2020) (hereafter, "Second

Supplemental Kromberg Declaration"); Gordon Kromberg, Third Supplemental Declaration in Support of Request for Extradition of Julian Paul Assange ¶ 1 (Mar. 24, 2020) (hereafter, "Third Supplemental Kromberg Declaration").[1]

3. In the course of my duties as an Assistant United States Attorney, I have become familiar with the evidence and charges in the case of *United States v. Julian Assange*, Case Number 1:18-CR-111, pending in the U.S. District Court for the Eastern District of Virginia. This affidavit does not detail all of the evidence against ASSANGE that is known to me, but only the evidence necessary to establish a basis for this Extradition Request. I have confirmed the facts of this affidavit with agents of the Federal Bureau of Investigation (FBI) who are assigned to investigate this matter.

SUMMARY OF THE EXTRADITION REQUEST

4. This Extradition Request arises from a longstanding investigation that the United States has conducted of ASSANGE for illegal acts that he committed in connection with a website known as WikiLeaks. As described below, the United States previously filed charges against ASSANGE related to his illegal conduct in obtaining, conspiring and attempting to obtain, and disseminating classified information from Bradley (now Chelsea) Manning, an intelligence analyst in the U.S. Army. Recently, the United States obtained a Second Superseding Indictment that expands two of the charges, holding ASSANGE responsible for his participation in broader unlawful conspiracies to obtain national defense information from, and engage in computer hacking with, other individuals in addition to Manning.

[1] The Third Supplemental Kromberg Declaration bears the mistaken date of March 12, 2020.

5. On December 21, 2017, a federal magistrate judge in Alexandria, Virginia, issued a criminal complaint charging ASSANGE with conspiracy to commit unlawful computer intrusion, in violation of Title 18, U.S. Code, Section 371, based on ASSANGE's agreement with Manning to crack an encrypted password hash stored on U.S. Department of Defense computers connected to a classified network. On March 6, 2018, a federal grand jury in Alexandria, Virginia, returned an Indictment charging ASSANGE with the same offense. The United States submitted a provisional arrest request to the United Kingdom in connection with this charge.

6. As I have detailed in a prior affidavit, ASSANGE was actively attempting to evade justice in the United States during this time. *See* Second Supplemental Kromberg Declaration ¶¶ 15-17. Specifically, in June 2012, ASSANGE fled to the Embassy of Ecuador in London, and for almost seven years, ASSANGE hid in the Embassy of Ecuador to avoid prosecution in the United States. *See id.* ¶¶ 16-17. ASSANGE remained in the Embassy of Ecuador from June 2012 until on or about April 11, 2019, when U.K. law enforcement arrested ASSANGE in the Embassy of Ecuador.

7. Soon after ASSANGE's arrest, on May 23, 2019, a federal grand jury in Alexandria, Virginia, returned a Superseding Indictment charging ASSANGE with 18 counts. As I have explained in a prior affidavit, the Superseding Indictment charged ASSANGE for his complicity in illegal acts to obtain or receive voluminous databases of classified information from Manning, his agreement with Manning and attempt to obtain classified information through computer hacking, and his publication of certain classified documents that were provided by Manning and contained the un-redacted names of innocent people who risked their safety and freedom to provide information to the United States and its allies, including local Afghans and

Iraqis, journalists, religious leaders, human rights advocates, and political dissidents from repressive regimes. *See* First Kromberg Declaration ¶ 6.

8. The next month, on or about June 6, 2019, the United States submitted, via the diplomatic channels, a request that the United Kingdom extradite ASSANGE based on the charges in the Superseding Indictment. As **Attachment A** to this affidavit, I have attached a copy of the original papers submitted in support of the request for ASSANGE's extradition, including an affidavit, dated June 4, 2019 (hereinafter, "Initial Extradition Affidavit").[2]

9. After the grand jury returned the Superseding Indictment, the United States continued to investigate ASSANGE's criminal conduct, including criminal conduct that was not alleged in the Superseding Indictment or any of the other prior charging instruments against him. In my training and experience, it is lawful, and indeed common, for U.S. prosecutors to continue investigating a defendant's criminal conduct even after he has been arrested and charged. For example, the arrest and detention of the defendant often permit law enforcement to take more overt investigative steps that might previously have been unavailable due to concerns that they would cause the target and co-conspirators to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates.

10. On June 24, 2020, a federal grand jury in Alexandria, Virginia, returned a Second Superseding Indictment against ASSANGE. Like the prior Superseding Indictment, the Second Superseding Indictment charges ASSANGE with 18 counts. The Second Superseding Indictment does not add or remove any counts against ASSANGE. Nor does the Second

[2] In addition to the initial extradition request, I have attached as **Attachment B**, **Attachment C**, **Attachment D**, and **Attachment E** the four declarations that I previously submitted in support of ASSANGE's extradition, as referenced above in Paragraph 2. For the avoidance of any doubt, I hereby incorporate those declarations in support of this Extradition Request, except where clarified or context suggests otherwise herein.

Superseding Indictment increase the maximum penalty to which ASSANGE was already subject under the prior Superseding Indictment. The Second Superseding Indictment continues to charge ASSANGE for the same offenses arising from his illegal acts in obtaining, conspiring and attempting to obtain, and disseminating classified national defense information from Manning. For the avoidance of doubt, the entirety of the previous request is incorporated herein, except where clarified, or context suggests otherwise herein.[3]

11. The Second Superseding Indictment differs from the Superseding Indictment in the following significant ways:

a. The Second Superseding Indictment alleges additional General Allegations, including allegations relating to ASSANGE's and his co-conspirators' efforts to recruit and agreement with hackers to commit computer intrusions to benefit WikiLeaks, and efforts to recruit individuals to violate the law in disclosing classified information to benefit WikiLeaks;

b. The Second Superseding Indictment expands the dates and scope of Count 1 (Conspiracy to Obtain and Disclose National Defense Information), thereby encompassing ASSANGE's and his co-conspirators' agreement to recruit individuals to violate the law in obtaining and disclosing classified information to benefit WikiLeaks, and to publish classified information containing source names to certain individuals not authorized to receive it as well as the public;

c. The Second Superseding Indictment moves the prior Count 18 (Conspiracy to Commit Computer Intrusion) to Count 2 and expands the dates, scope, and objects of the conspiracy, thereby encompassing ASSANGE's and his co-conspirators' efforts to recruit and agreement with other hackers—in addition to Manning—to commit computer intrusions to benefit WikiLeaks;

d. The Second Superseding Indictment moves Count 2 in the Superseding Indictment to Count 18; and

e. The Second Superseding Indictment includes language in Counts 15, 16, and 17 clarifying that ASSANGE violated the law by distributing the significant activity reports and State Department cables that named human

[3] For example, Paragraphs 58, 82, 83, 85, and 87 of the Initial Extradition Affidavit are not incorporated herein.

sources to persons not authorized to receive them, in addition to publishing and causing the documents to be published publicly on the internet.

12. As set forth below, I provide a summary of the evidence supporting the additional facts and the revised charges alleged in the Second Superseding Indictment. Because the Second Superseding Indictment continues to allege facts and charges that were included in the prior Superseding Indictment, I will incorporate by reference the Initial Extradition Affidavit to avoid unnecessary repetition.

SUMMARY OF THE ADDITIONAL FACTS OF THE CASE

13. The charges concern one of the largest compromises of classified information in the history of the United States. As summarized in the Initial Extradition Affidavit, ASSANGE conspired with U.S. Army Intelligence Analyst Bradley (now Chelsea) Manning to obtain, receive, and communicate certain classified materials and to crack an encrypted password hash stored on a U.S. Department of Defense computer connected to a network used for classified documents and communications. Paragraphs 5 to 8 of the Initial Extradition Affidavit are adopted as if fully set forth here, except that Paragraph 7 is amended to note that the password hash discussed therein was an encrypted password hash.

14. ASSANGE, however, did not just conspire with Manning to steal and disclose classified information. The evidence shows that, from the time ASSANGE started WikiLeaks, he and others at WikiLeaks sought to recruit individuals with access to classified information to unlawfully disclose such information to WikiLeaks, and sought to recruit - - and worked with - - hackers to conduct malicious computer attacks for purposes of benefiting WikiLeaks. In other words, before ASSANGE first communicated with Manning about providing classified information or hacking computers, ASSANGE already was engaged in a conspiracy with others to do so as well. Moreover, after Manning was arrested, ASSANGE sought to recruit other

hackers and leakers of classified information, by publicizing his willingness to help such individuals avoid identification and arrest.

15. Among the individuals with whom ASSANGE conspired were Jeremy Hammond, "Sabu," and "Laurelai," all of whom were hackers located in the United States at the time they committed the overt acts alleged in the Second Superseding Indictment. These individuals are discussed further below. In addition, several of the computers that are listed in the Second Superseding Indictment as targets and intended targets of computer intrusions were computers located in the United States and owned by U.S. business and/or U.S. government entities.

A. Background on ASSANGE and WikiLeaks

16. From at least 2007,[4] ASSANGE was the public face of WikiLeaks, a website he founded with others as an "intelligence agency of the people." The nature and operation of WikiLeaks are set forth in Paragraphs 11 to 13 of the Initial Extradition Affidavit, and those Paragraphs are adopted as if fully set forth here, except that WikiLeaks not only continued to explicitly solicit "classified" materials until September 2010, but also continued to do so up through in or about 2015. In sum, ASSANGE and WikiLeaks repeatedly sought, obtained, and disseminated information that the United States classified due to the serious risk that unauthorized disclosure could harm the national security of the United States. And, ASSANGE designed WikiLeaks to focus on information restricted from public disclosure by law, precisely because of the value of that information.

17. As explained in Paragraphs 14 and 15 of the Initial Extradition Affidavit, which is incorporated by reference, the WikiLeaks website included a detailed list of "The Most Wanted Leaks of 2009." This list explained that the sought after documents or materials must "[b]e

[4] As with the Initial Extradition Affidavit, all dates in this affidavit are approximate.

likely to have political, diplomatic, ethical or historical impact on release . . . and be plausibly obtainable to a well-motivated insider or outsider," and must be "described in enough detail so that . . . a visiting outsider not already familiar with the material or its subject matter may be able to quickly locate it, and will be motivated to do so."

18. ASSANGE used the "Most Wanted Leaks" as a means to recruit individuals to hack into computers and/or illegally obtain and disclose classified information to WikiLeaks. For instance, as evidenced by a video available on the internet, in August 2009, ASSANGE and a WikiLeaks associate (WLA-2) spoke at the "Hacking at Random" conference in the Netherlands. ASSANGE sought to recruit those who had or could obtain authorized access to classified information and hackers to search for, steal and send to WikiLeaks the items on the "Most Wanted Leaks" list that was posted on WikiLeaks's website. To embolden potential recruits, ASSANGE told the audience that, unless they were "a serving member of the United States military," they would have no legal liability for stealing classified information and giving it to WikiLeaks because "TOP SECRET" meant nothing as a matter of law.

19. Moreover, as evidenced by video available on the internet, at the Hacking at Random conference, WLA-2 invited members of the audience who were interested in helping WikiLeaks to attend a follow-on session, where they could discuss where the items on the Most Wanted Leaks list could be found and how they could be obtained. At that follow-on session, ASSANGE explained how WikiLeaks had exploited "a small vulnerability" inside the document distribution system of the United States Congress to obtain reports of the Congressional Research Service that were not available to the public, and he asserted that "[t]his is what any one of you would find if you were actually looking."

20. Likewise, as described in Paragraph 16 of the Initial Extradition Affidavit, which is incorporated by reference, ASSANGE spoke at the "Hack in the Box Security Conference" in Malaysia in October 2009. ASSANGE told the audience, "I was a famous teenage hacker in Australia, and I've been reading generals' emails since I was 17." ASSANGE again referenced the "Most Wanted Leaks" list for purposes of recruiting individuals to engage in computer hacking and to steal classified information for publication by WikiLeaks.

B. Chelsea Manning

21. From 2009 to 2010, Chelsea Manning, then known as Bradley Manning, was an intelligence analyst in the U.S. Army who was deployed to Forward Operating Base Hammer in Iraq. Paragraphs 17 to 37 and 46 to 48 of the Initial Extradition Affidavit detail Manning's duties as an intelligence analyst, Manning's access to classified documents and communications, ASSANGE's and Manning's agreement to steal and disclose classified information to WikiLeaks, ASSANGE's and Manning's overt acts in furtherance of their conspiracy, and the evidence establishing that Manning exchanged instant message communications with ASSANGE who was using a particular Jabber account. Those Paragraphs are incorporated by reference here in their entirety, except Paragraph 31(c), which is amended to state that on March 8, 2010, Manning told ASSANGE - - in reference to the Guantanamo Bay detainee assessment briefs - - that "after this upload, that's all I really have got left," and, in response to this statement (which indicated that Manning had no more classified documents to unlawfully disclose), ASSANGE replied, "curious eyes never run dry in my experience."

22. As evidenced by a video available on the internet, in July 2010, at a conference in New York City of "Hackers on Planet Earth," a WikiLeaks associate (WLA-3) urged attendees to leak to WikiLeaks. WLA-3 said that WikiLeaks had "never lost a source," told the audience that it should reject the thought that someone else was more qualified than them to determine whether

a document should be kept secret, and urged attendees to assist WikiLeaks and emulate others who had broken the law to disseminate classified information. WLA-3 ended his request for assistance with the slogan, "Think globally, hack locally."

23. As demonstrated by evidence obtained from WikiLeaks' website, WikiLeaks published documents that Manning had unlawfully provided. Specifically, in July 2010, WikiLeaks published approximately 75,000 significant activity reports related to the war in Afghanistan, classified up to the **SECRET** level; in October 2010, WikiLeaks published approximately 400,000 significant activity reports related to the war in Iraq, classified up to the **SECRET** level; in November 2010, WikiLeaks started publishing redacted versions of U.S. Department of State Cables, classified up to the **SECRET** level; in April 2011, WikiLeaks published approximately 800 Guantanamo Bay detainee assessment briefs, classified up to the **SECRET** level; and in August and September 2011, WikiLeaks published un-redacted versions of approximately 250,000 U.S. Department of State Cables, classified up to the **SECRET** level.

C. Teenager, Manning, and NATO Country-1

24. Information provided by a human source, which has been corroborated by the Jabber Communications between ASSANGE and Manning, shows that, in early 2010, around the same time that ASSANGE was working with Manning to obtain classified information, ASSANGE met a 17-year old in NATO Country-1 ("Teenager"), who provided ASSANGE with data stolen from a bank. ASSANGE thereafter asked Teenager to commit computer intrusions and steal additional information, including audio recordings of phone conversations between high-ranking officials of the government of NATO Country-1, including members of the Parliament of NATO Country-1.

25. Evidence obtained from a forensic examination of Manning's computer media shows that, beginning in January 2010, Manning repeatedly searched for classified information about NATO Country-1.

26. On February 14, 2010, as Manning admitted at court-martial, Manning downloaded classified State Department materials regarding the government of NATO Country-1. Evidence obtained from WikiLeaks' website shows that, on February 18, 2010, WikiLeaks posted a classified cable from the U.S. Embassy in NATO Country-1, that WikiLeaks received from Manning.

27. The Jabber Communications between ASSANGE and Manning show that, on March 5, 2010, ASSANGE told Manning about having received stolen banking documents from a source who, in fact, was Teenager. Then, five days later, on March 10, 2010, after ASSANGE told Manning that ASSANGE had given an "intel source" a "list of things we wanted" and the source had agreed to provide and did provide four months of recordings of all phones in the Parliament of the government of NATO Country-1, ASSANGE stated, "So, that's what I think the future is like ;)," referring to how he expected WikiLeaks to operate.

28. In early 2010, according to a human source and as corroborated by the Jabber Communications between ASSANGE and Manning, a source provided ASSANGE with credentials to gain unauthorized access into a website that was used by the government of NATO Country-1 to track the location of police and first responder vehicles, and agreed that ASSANGE should use those credentials to gain unauthorized access to the website.

29. The Jabber Communications between ASSANGE and Manning show that, on March 17, 2010, ASSANGE told Manning that ASSANGE used the unauthorized access to the

website of the government of NATO Country-1 for tracking police vehicles (provided to ASSANGE by a source) to determine that NATO Country-1 police were monitoring ASSANGE.

30. Evidence obtained from WikiLeaks' website shows that, on March 29, 2010, WikiLeaks posted classified State Department materials regarding officials in the government of NATO Country-1, which Manning had downloaded on February 14, 2010.

31. According to a human source, after ASSANGE and Teenager failed in their joint attempt to decrypt a file stolen from a NATO Country-1 bank, Teenager asked a U.S. person to try to do so on July 21, 2010. Information provided by this U.S. person, as well as records of online chats, corroborate that Teenager asked the U.S. person to try to decrypt the stolen file. In 2011 and 2012, that individual, who had been an acquaintance of Manning since early 2010, became a paid employee of WikiLeaks, and reported to ASSANGE and Teenager.

32. According to a human source, and as corroborated by the records of online chats between ASSANGE and that source, no later than the summer of 2010, ASSANGE put Teenager in charge of operating, administering, and monitoring WikiLeaks's Internet Relay Chat ("IRC") channel. Because WikiLeaks's IRC channel was open to the public, ASSANGE regarded it as both a means of contacting new sources and a potential "den of spies." ASSANGE warned Teenager to beware of spies, and to refer to ASSANGE sources with "national security related information."

33. In September 2010, according to a human source, and as corroborated by the records of online chats between ASSANGE and that source, ASSANGE directed Teenager to hack into the computer of an individual formerly associated with WikiLeaks and delete chat logs containing statements of ASSANGE. When Teenager asked how that could be done, ASSANGE wrote that the former WikiLeaks associate could "be fooled into downloading a trojan," referring

to malicious software, and then asked Teenager what operating system the former-WikiLeaks associate used.

D. Anonymous, Gnosis, AntiSec, and LulzSec

34. In December 2010, media outlets reported that hackers affiliated with a group known as "Anonymous" launched distributed denial of service attacks ("DDoS" attacks) against PayPal, Visa, and MasterCard in retaliation for their decisions to stop processing payments for WikiLeaks. Anonymous called these attacks "Operation Payback."

35. Later in December 2010, according to a human source, and as corroborated by the records of online chats obtained from a forensic examination of a computer belonging to "Laurelai," a hacker affiliated with Anonymous, Laurelai contacted Teenager and identified herself as a member of the hacking group "Gnosis." Laurelai subsequently introduced Teenager to another member of Gnosis, who went by the online moniker "Kayla." Teenager told Laurelai that he [Teenager] was "in charge of recruitments" for WikiLeaks and stated, "I am under JULIAN ASSANGE's authority and report to him and him only." First Laurelai and later Kayla indicated to Teenager their willingness to commit computer intrusions on behalf of WikiLeaks.

36. In January 2011, according to a human source, and as corroborated by the records of online chats between ASSANGE and that source, Teenager told ASSANGE, "a group of Hackers offered there servicses [sic] to us called Gnosis." ASSANGE approved of the arrangement and told Teenager to meet with Gnosis.

37. Records of online communications recovered from Laurelai's computer show that on February 6, 2011, Laurelai told Kayla that they should show to Teenager materials that Kayla had obtained by hacking a U.S. cybersecurity company ("U.S. Cybersecurity Company").[5]

38. On February 7, 2011, according to a human source, and as corroborated by the records of online chats between ASSANGE and that source, Teenager messaged ASSANGE that Gnosis had hacked U.S. Cybersecurity Company. Then, on February 11, 2011, Teenager provided ASSANGE with computer code that Kayla had hacked from U.S. Cybersecurity Company and told ASSANGE it came from Gnosis's hack of that company.

39. Records of online communications recovered from Laurelai's computer show that on February 15, 2011, in a chat with a hacker with the moniker "elChe," Laurelai characterized herself as "part of WikiLeaks staff … hacker part." The next day, on February 16, 2011, Laurelai asked Kayla whether Laurelai could tell Teenager about Kayla's penetration of a hosting service, so that WikiLeaks could determine if WikiLeaks needed information hosted there.

40. On February 17, 2011, according to communications provided by a human source, Teenager told Laurelai that WikiLeaks was the world's largest hacking organization.

41. Records of online communications recovered from Laurelai's computer show that on March 1, 2011, Laurelai told Kayla to let Laurelai know if Kayla found any "@gov" passwords" so that Laurelai could then send them to WikiLeaks (through Teenager). Five days later, on March 6, 2011, according to communications provided by a human source, Laurelai

[5] The identities of the victims discussed in the Second Superseding Indictment and this affidavit are known to U.S. law enforcement, but have been anonymized in accordance with Section 9-6.200 of the Justice Manual. It is the policy of the Department of Justice to not publicly disclose victims' identities before trial if there is any reason to believe that such disclosure would endanger the safety of the victim or any other person or lead to efforts to obstruct justice. The Department of Justice, however, intends to disclose the identity of the victims listed herein to ASSANGE in discovery pursuant to a protective order.

offered WikiLeaks (through Teenager) "unpublished zero days" (vulnerabilities that can be used to hack computer systems).

42. On March 15, 2011, according to communications recovered from both Laurelai's computer and a human source, Laurelai emailed WikiLeaks (through Teenager) a list of approximately 200 purported passwords to U.S. and state government email accounts, including passwords (hashed and plaintext) that purported to be for accounts associated with information technology specialists at government institutions.

43. In May 2011, as established later upon their arrests, members of Anonymous, including several who were involved in "Operation Payback" from December 2010, formed their own hacking group, which they publicly called "LulzSec." These members included Kayla, "Sabu," and "Topiary."

44. On May 24, 2011, a television network (the "Television Network") aired a documentary about WikiLeaks that included an allegation that ASSANGE intentionally risked the lives of the sources named in WikiLeaks publications. Approximately five days later, on May 29, 2011, LulzSec members publicly claimed that, as retaliation for the Television Network's negative coverage of WikiLeaks, they hacked into the Television Network's computers and published passwords used by its journalists, affiliates, and employees.

45. FBI records show that, on June 7, 2011, Sabu was arrested. Shortly thereafter, Sabu began cooperating with the FBI.

46. In June 2011, after LulzSec took credit for a purported DDoS attack against the CIA's public-facing website, as evidenced by at least WikiLeaks' official Twitter account, ASSANGE decided that WikiLeaks should publicly support LulzSec. From the official WikiLeaks Twitter account, WikiLeaks tweeted: "WikiLeaks supporters, LulzSec, take down

CIA . . . who has a task force into WikiLeaks," adding, "CIA finally learns the real meaning of WTF."

47. According to a human source, and as corroborated by records provided by that source and evidence obtained from a cooperating witness, after receiving ASSANGE's approval to establish a relationship between WikiLeaks and LulzSec, Teenager made contact with Topiary on June 16, 2011, by going through Laurelai. To show Topiary that Teenager spoke for WikiLeaks so that an agreement could be reached between WikiLeaks and LulzSec, Teenager posted to YouTube (and then quickly deleted) a video of his computer screen that showed the conversation that he was then having with Topiary. The video turned from Teenager's computer screen and showed ASSANGE sitting nearby. The FBI captured that video.

48. According to records of chats involving a cooperating witness and captured by the FBI, Teenager told Topiary, "[m]y main purpose here is mainly to create some kind of a connection between lulzsec and wikileaks." Topiary agreed to this partnership, stating, "if we do get a /massive/ cache of information, we'd be happy to supply you with it." Teenager later added, "WikiLeaks cannot publicly be taking down websites, but we might give a suggestion of something or something similar, if that's acceptable to LulzSec."

49. On June 19, 2011, LulzSec publicly posted a release, stating that it was launching a movement called "AntiSec" that would engage in cyberattacks against government agencies, banks, and cybersecurity firms. According to a cooperating witness, from this point forward, people affiliated with the groups often used the names LulzSec and AntiSec interchangeably.

50. According to a human source, as corroborated by chat records between a cooperating witness and Assange, in the fall of 2011, Teenager left WikiLeaks.

E. Sabu, Hammond, and ASSANGE

51. On December 25, 2011, media outlets reported that hackers claiming an affiliation with Anonymous and LulzSec announced they had hacked the servers of a private intelligence consulting company ("Intelligence Consulting Company").

52. As evidenced by a chat involving a cooperating witness that the FBI recorded, on December 29, 2011, a hacker affiliated with LulzSec/AntiSec, Jeremy Hammond, told other hackers on an IRC channel called "#Lulzxmas" that information hacked from Intelligence Consulting Company was being sent to WikiLeaks. In this same chat, Hammond informed elChe and others in the group, "JA almost done copying the files." Hammond also told elChe that there should be "no leaks about this partnering."

53. In December 2011, in a communication the FBI recorded, Hammond told Sabu that he had been partnering with an individual at WikiLeaks who Hammond believed to be ASSANGE. Hammond explained that he had (a) received from that individual a message that WikiLeaks would tweet a message in code; (b) seen that shortly thereafter, the WikiLeaks Twitter account tweeted, "rats for Donavon"; (c) received another message from that individual believed to be ASSANGE, explaining that the tweet contained an anagram for a particular term that such individual specified; and (d) the term specified contained a reference to the name of Intelligence Consulting Company. The FBI captured that "rats for Donavan" tweet.

54. On December 31, 2011, WikiLeaks tweeted "#antisec owning Law enforcement in 2012," as well as links to emails and databases that Hammond and AntiSec had obtained from hacking two U.S. state police associations. On January 3, 2012, WikiLeaks tweeted a link to information that LulzSec/AntiSec had hacked and published in 2011, stating, "Anonymous/Antisec/Luzsec releases in 2011." On January 6, 2012, WikiLeaks tweeted a link

to a spoofed email sent by Hammond to the clients of Intelligence Consulting Company, purporting to be the CEO of that company, stating, "AnonymousIRC email sent by #AntiSec to [Intelligence Consulting Company]'s customers #Anonymous #LulzSec."

55. In January 2012, in a communication recorded by the FBI, Hammond told Sabu that "JA" provided to Hammond a script to search the emails stolen from Intelligence Consulting Company, and that "JA" would provide that script to associates of Hammond as well. Hammond also introduced Sabu via Jabber to "JA." In January and February 2012, in communications recorded by the FBI, Sabu used Jabber to communicate with ASSANGE, who, at the time, used at least these two Jabber accounts: dpaberlin@jabber.ccc.de and ardeditor@jabber.ccc.de. For instance:

a. On January 16, 2012, in a communication recorded by the FBI, and in response to a message from Sabu that stated, "If you have any targets in mind by all means let us know," ASSANGE (who was using the Jabber account dpaberlin@jabber.ccc.de) initially responded that he could not "give target suggestions for the obvious legal reasons," but approximately 44 seconds later added, "But, for people that do bad things, and probably have that documented, there's ['Research and Investigative Firm']" and "lots of the companies" listed on a website whose address ASSANGE provided.

b. On January 21, 2012, in a communication recorded by the FBI, ASSANGE (who was using the Jabber account dpaberlin@jabber.ccc.de) suggested that, in the course of hacking Research and Investigative Firm, Sabu and other members of LulzSec/AntiSec should look for and provide to WikiLeaks mail and documents, databases and pdfs.

c. On February 21, 2012, in a communication recorded by the FBI, and in response to Sabu's request, ASSANGE (who was using the Jabber account ardeditor@jabber.ccc.de) provided Sabu with a computer script to search for emails hacked from Intelligence Consulting Company. In addition, in order to focus the hacking efforts of the hackers associated with Sabu, ASSANGE told Sabu that the most impactful release of hacked materials would be from the CIA, NSA, or the *New York Times*.

56. On February 22, 2012, in a communication recorded by the FBI, Hammond told Sabu that, at ASSANGE's "indirect" request, Hammond had spammed the Intelligence Consulting Company again.

57. On February 27, 2012, WikiLeaks began publishing emails that Hammond and others hacked from Intelligence Consulting Company.

58. On February 27, 2012, in a communication recorded by the FBI, Hammond told Sabu, "we started giving JA" materials that had been obtained from other hacks.

59. On February 27, 2012, in a communication recorded by the FBI, Hammond told Sabu that ASSANGE was talking to elChe.

60. On February 28, 2012, in a communication recorded by the FBI, Hammond complained to Sabu that the incompetence of his fellow hackers was causing him to fail to meet estimates he had given to ASSANGE for the volume of hacked information that Hammond expected to provide WikiLeaks, writing, "can't sit on all these targets dicking around when the booty is sitting there … especially when we are asked to make it happen with WL. We repeated a 2TB number to JA. Now turns out it's like maybe 100GB. Would have been 40-50GB if I didn't go and reget all the mail from [foreign cybersecurity company]." Hammond then stated that he needed help with ongoing hacks that his associates were committing against victims that included a U.S. law enforcement entity, a U.S. political organization, and a U.S. cybersecurity company.

61. In March 2012, Hammond was arrested.

F. Evidence that ASSANGE Used dpaberlin@jabber.ccc.de and ardeditor@jabber.ccc.de to Communicate with SABU

62. As summarized below, the user of the dpaberlin@jabber.ccc.de and ardeditor@jabber.ccc.de Jabber account made statements to Sabu that are distinctive and particular to ASSANGE. Those accounts thus can be attributed to ASSANGE.

63. For instance, on January 16, 2012, Sabu sent a message to the dpaberlin@jabber.ccc.de account asking how "the case [was] going." In response, the user of the account stated, "[i]t's a huge legal-political quagmire," and added, "[i]f I'm going down it sure hasn't been without a fight." Then, when Sabu suggested in a chat dated January 21, 2012, that it had to be "boring" to stay at Ellingham Hall "every day with an ankle bracelette [sic] to look at all day," dpaberlin@jabber.cccc.de responded that the user of the account was involved in:

> supreme court strategy, fowl theory, new crypto-systems for our guys, talking to sources, coordinating new releases, another 5 law suits, pr, tv series, press complaints, trying to get money back form [sic] old lawyers, working on new books, censorship projects, moving $/people around... about the same as any CEO of a medium sized international company with a lot of law suits....

According to press reports, by January 2012, Sweden had issued an arrest warrant for ASSANGE arising from allegations that he committed rape and molestation in 2010, and the UK Supreme Court was considering whether ASSANGE should be extradited to Sweden. ASSANGE had been released on bail in December 2010 and was residing at Ellingham Hall in the English county of Norfolk.

64. Also on January 21, 2012, the dpaberlin@jabber.ccc.de account stated to Sabu that the user of the account was very busy, but trusted only himself to deal with sources. The user of the account further stated the others who worked at WikiLeaks were good people, but

indicated that he lacked confidence that anyone at WikiLeaks other than himself could survive prosecution and prison without talking to law enforcement.

65. Also on January 16, 2012, dpaberlin@jabber.ccc.de told Sabu that dpaberlin@jabber.ccc.de was making a television show in which he would be interviewing "ultimate insiders and outsiders on the fate of the world." The user of the dpaberlin@jabber.ccc.de account further told Sabu that, on his show, he would interview guests including presidents, the leader of Hezbollah, and participants in the Occupy Movement. Then, about a week later, on January 23, 2012, WikiLeaks announced a new television series that would start in March 2012, in which ASSANGE would host conversations with key political players over the course of approximately ten weekly episodes. Airing on the Russia Today network, the guests interviewed by ASSANGE included the Presidents of Tunisia and Ecuador, the leader of Hezbollah, representatives of the Occupy Movement, and an individual who claimed to be a former Guantanamo Bay prisoner who ran the website cageprisoners.org in 2012. On February 21, 2012, the ardeditor@jabber.ccc.de account told Sabu that he had, the previous day, interviewed a former Guantanamo Bay prisoner who now ran the website cageprisoners.org.

66. The ardeditor@jabber.ccc.de account is further attributable to ASSANGE based on a message the account sent to Sabu on February 21, 2012, in which the user of ardeditor@jabber.ccc.de wrote that he was "concerned" about "dealing" with "this yoho guy." Markedly, yohoho@jabber.ccc.de was the Jabber account that Hammond was using to communicate with Sabu on January 12, 2012, in which Hammond explained that he was in communication with "JA" and stated that "JA" would "hit [Sabu] up" through Jabber.

G. ASSANGE's Efforts to Recruit System Administrators

67. In June 2013, media outlets reported that Edward J. Snowden had leaked numerous documents taken from the NSA and was located in Hong Kong. Later that month, an arrest warrant was issued in the United States District Court for the Eastern District of Virginia, for the arrest of Snowden, on charges involving the theft of information from the United States government.

68. To encourage leakers and hackers to provide stolen materials to WikiLeaks in the future, ASSANGE and others at WikiLeaks openly displayed their attempts to assist Snowden in evading arrest.

69. In June 2013, media outlets reported that a WikiLeaks associate ("WLA-4") traveled with Snowden from Hong Kong to Moscow.

70. On December 31, 2013, at the annual conference of the Chaos Computer Club ("CCC") in Germany, and as reflected in a video available on the internet, ASSANGE, WLA-3 and WLA-4 gave a presentation titled "Sysadmins of the World, Unite! A Call to Resistance." On its website, the CCC promoted the presentation by writing, "[t]here has never been a higher demand for a politically-engaged hackerdom" and that ASSANGE and WLA-3 would "discuss what needs to be done if we are going to win." ASSANGE told the audience that "the famous leaks that WikiLeaks has done or the recent Edward Snowden revelations" showed that "it was possible now for even a single system administrator to . . . not merely wreck[] or disabl[e] [organizations] . . . but rather shift[] information from an information apartheid system . . . into the knowledge commons." ASSANGE exhorted the audience to join the CIA in order to steal and provide information to WikiLeaks, stating, "I'm not saying don't join the CIA; no, go and join the CIA. Go in there, go into the ballpark and get the ball and bring it out."

71. At the same presentation, in responding to the audience's question as to what they could do, WLA-3 said "Edward Snowden did not save himself. . . . Specifically for source protection, [WLA-4] took actions to protect [Snowden] . . . . [I]f we can succeed in saving Edward Snowden's life and to keep him free, then the next Edward Snowden will have that to look forward to. And if we look also to what has happened to Chelsea Manning, we see additionally that Snowden has clearly learned. . . ."

H. ASSANGE and WikiLeaks Continue to Recruit

72. On May 6, 2014, at a re:publica conference in Germany, and as reflected in a video available on the internet, WLA-4 sought to recruit those who had or could obtain authorized access to classified information and hackers to search for and send the classified or otherwise stolen information to WikiLeaks by explaining, "[f]rom the beginning our mission has been to publish classified or in any other way censored information that is of political, historical importance."

73. On May 15, 2015, WikiLeaks tweeted a request for nominations for the 2015 "Most Wanted Leaks" list, and as an example, linked to one of the posts of a "Most Wanted Leaks" list from 2009 list that remained on WikiLeaks's website.

74. In an interview on May 25, 2015, and as reflected in a video of that interview available on the internet, ASSANGE claimed to have arranged distraction operations to assist Snowden in avoiding arrest by the United States:

> Let's go back to 2013. There was a worldwide manhunt for Edward Snowden . . . vast resources were put into trying to grab Edward Snowden or work out where he might go, if he was leaving Hong Kong, and grab him there.
>
> So we worked against that, and we got him out of Hong Kong and got him to Russia, and we were going to transit through Russia to get him to Latin America. Now, the U.S. government canceled his

> passport as he was en route, it seems, to Moscow, meaning that he then couldn't take his next flight, which had been booked through Cuba. And at that point, there became a question of, well, how else can he proceed? If he can't proceed by a commercial airline, are there other alternatives? And so, we looked into private flights, private jets, other unusual routes for commercial jets, and presidential jets. . . .
>
> There was an oil conference on in—there was an international oil conference in Moscow that week. Edward Snowden and our journalist, [WLA-4], still in the Moscow airport in the transit lounge, and so we thought, well, this is an opportunity, actually, to send Edward Snowden to Latin America on one of these jets. . . .
>
> We had engaged in a number of these distraction operations in the asylum maneuver from Hong Kong, for example, booking him on flights to India through Beijing and other forms of distraction, like Iceland, for example.

75. On June 18, 2015, at an event sponsored by the Rosa Luxemburg Foundation in Germany, and as reflected in a video available on the internet, WLA-3 and WLA-4 sought to recruit individuals to search for, steal, and send to WikiLeaks classified information by promising their audience that, if anyone in the audience could infiltrate organizations supporting the military, find the right "informational way to strike," and emulate Snowden, WikiLeaks would publish their information.

76. In June 2015, to continue to encourage individuals to hack into computers and/or illegally obtain and disclose classified information to WikiLeaks, WikiLeaks maintained on its website "The Most Wanted Leaks of 2009."

I. ASSANGE Revealed the Names of Human Sources and Created a Grave and Imminent Risk to Human Life.

77. During 2010 and 2011, ASSANGE disseminated and published via the WikiLeaks website the documents classified up to the **SECRET** level that he had obtained from Manning, as described above, including approximately 75,000 Afghanistan war-related significant activity reports, 400,000 Iraq war-related significant activity reports, 800 Guantanamo Bay detainee

assessment briefs, and 250,000 U.S. Department of State cables. Paragraphs 38 to 43 and 45 of the Initial Extradition Affidavit, which are incorporated here, describe these disclosures and the grave and imminent risk of harm that arose from their disclosure, except that, as noted previously, WikiLeaks published un-redacted versions of approximately 250,000 U.S. Department of State Cables in August and September 2011.

78. ASSANGE knew that his dissemination and publication of Afghanistan and Iraq war-related significant activity reports endangered sources, whom he named as having provided information to U.S. and coalition forces. Evidence of ASSANGE's knowledge is set forth in Paragraph 44 and 45 of the Initial Extradition Affidavit, and are incorporated here.

J. U.S. Law Regarding the Protection of Classified Information

79. Paragraphs 9 and 10 of the Initial Extradition Affidavit provide an overview of the basis under U.S. law for classifying information and explain that ASSANGE has never been authorized to receive, possess, or communicate classified information. Those Paragraphs are incorporated here.

PROCEDURAL HISTORY OF THE CASE

80. Paragraphs 49 through 52 of the Initial Extradition Affidavit provide an overview of the charging process under the laws of the United States, and Paragraph 53 through 57 of the Initial Extradition Affidavit describe the previous charges filed against ASSANGE in this case. Those Paragraphs are incorporated here.

81. On June 24, 2020, a federal grand jury in Alexandria, Virginia, returned a Second Superseding Indictment, also bearing case number 1:18-CR-111, charging ASSANGE with the following crimes:

a. Count One: Conspiracy to Obtain and Disclose National Defense Information, in violation of Title 18, U.S. Code, Section 793(g), which punishable by a maximum penalty of 10 years of imprisonment;

b. Count Two: Conspiracy to Commit Computer Intrusion, in violation of Title 18, U.S. Code, Section 371, which is punishable by a maximum penalty of 5 years of imprisonment;

c. Counts Three, Four, and Eighteen: Unauthorized Obtaining of National Defense Information, in violation of Title 18, U.S. Code, Sections 793(b) and 2, which is punishable by a maximum penalty of 10 years of imprisonment;

d. Counts Five through Eight: Unauthorized Obtaining and Receiving of National Defense Information, in violation of Title 18, U.S. Code, Sections 793(c) and 2, which is punishable by a maximum penalty of 10 years of imprisonment;

e. Counts Nine through Eleven: Unauthorized Disclosure of National Defense Information, in violation of Title 18, U.S. Code, Sections 793(d) and 2, which is punishable by a maximum penalty of 10 years of imprisonment;

f. Counts Twelve through Fourteen: Unauthorized Disclosure of National Defense Information, in violation of Title 18, U.S. Code, Sections 793(e) and 2, which is punishable by a maximum penalty of 10 years of imprisonment; and

g. Counts Fifteen through Seventeen: Unauthorized Disclosure of National Defense Information, in violation of Title 18, U.S. Code, Section 793(e), which is punishable by a maximum penalty of 10 years of imprisonment.

82. It is the practice in the U.S. District Court for the Eastern District of Virginia for the Clerk of Court to retain the originals of all indictments. It is also the practice in the U.S. District Court for the Eastern District of Virginia not to make publicly available the signed version of the indictment. Rather, for the protection of the grand jury foreperson, an unsigned copy of the indictment is entered on the Court's docket as part of the official record of the case.

Therefore, I have obtained a copy of the Second Superseding Indictment (Case No. 1:18-CR-111) and attached it to this affidavit as **Attachment F**.

83. On June 24, 2020, the U.S. District Court for the Eastern District of Virginia issued an arrest warrant for ASSANGE for the offenses charged in the Second Superseding Indictment. It is the practice in the U.S. District Court for the Eastern District of Virginia for the Clerk of Court to retain the original arrest warrants. Therefore, I have obtained a copy of the arrest warrant and attached it to this affidavit as **Attachment G**.

84. The United States requests the extradition of ASSANGE for all the offenses charged in the Second Superseding Indictment. Each count charges a separate offense. Each offense is punishable under a statute that (1) was the duly enacted law of the United States at the time the offense was committed, (2) was the duly enacted law of the United States at the time the Superseding Indictment was filed, and (3) is currently in effect. Each offense is a felony offense punishable under United States law by more than one year of imprisonment. I have attached copies of the pertinent sections of these statutes and the applicable penalty provisions to this affidavit as **Attachment H**.

THE CHARGES AND PERTINENT U.S. LAW

Count 1: Conspiracy to Obtain and Disclose National Defense Information

85. Count One of the Second Superseding Indictment charges ASSANGE with Conspiracy to Obtain and Disclose National Defense Information, in violation of Title 18, U.S. Code, Section 793(g).

86. Paragraphs 59 through 63 of the Initial Extradition Affidavit describe the pertinent U.S. law related to this charge, and I incorporate those Paragraphs by reference as if fully set forth here.

87. As detailed in the Second Superseding Indictment, the United States will establish that, beginning in at least 2009, ASSANGE conspired with other individuals, in and out of WikiLeaks, to unlawfully obtain and disclose classified documents of the United States. In furtherance of the conspiracy, ASSANGE agreed with others to recruit and assist leakers and hackers to violate the law by stealing classified documents of the United States and providing them to WikiLeaks. As part of the conspiracy, ASSANGE agreed with Manning to unlawfully obtain classified documents stolen from the United States. ASSANGE encouraged Manning to steal classified documents from the United States and to provide them to ASSANGE and WikiLeaks. ASSANGE also agreed to assist Manning in cracking an encrypted password hash stored on U.S. Department of Defense computers connected to SIPRNet, a U.S. government network used for classified documents and communications.

88. Paragraph 64 of the Initial Extradition Affidavit sets forth a non-exhaustive list of the type of evidence that the United States will use at trial to prove Count One. I hereby incorporate that Paragraph by reference. In addition to the evidence discussed in that Paragraph, the United States will introduce evidence that includes, but is not limited to, recordings and transcripts of public statements made by ASSANGE and other WikiLeaks associates.

Count 2: Conspiracy to Commit Computer Intrusion

89. Count Two of the Second Superseding Indictment charges ASSANGE with Conspiracy to Commit Computer Intrusion, in violation of Title 18, U.S. Code, Section 371. The objects of the conspiracy charged in Count 2 are to knowingly access a computer without authorization and exceeding authorized access,

a. to obtain information that has been determined by the United States Government pursuant to an Executive order and statute to require protection against unauthorized disclosure for reasons of national defense and foreign relations,

namely, documents relating to the national defense classified up to the SECRET level, with reason to believe that such information so obtained could be used to the injury of the United States and the advantage of any foreign nation, and to willfully communicate, deliver, transmit, and cause to be communicated, delivered, or transmitted the same, to persons not entitled to receive it, and willfully retain the same and fail to deliver it to the officer or employee entitled to receive it;

b. to obtain information from a department and agency of the United States and from protected computers; committed in furtherance of criminal and tortious acts in violation of the laws of the United States and of any State, and to obtain information that exceeded $5,000 in value;

c. to knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause damage without authorization to protected computers resulting in (i) aggregated loss during a one-year period of at least $5,000 in value, (ii) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, and national security; and (iii) damage affecting 10 or more protected computers during a one-year period; and

d. to intentionally access protected computers without authorization, and as a result of such conduct, recklessly cause damage resulting in (i) aggregated loss during a one-year period of at least $5,000 in value, (ii) damage affecting a computer used by or for an entity of the United States Government in furtherance of the

administration of justice, national defense, and national security; and (iii) damage affecting 10 or more protected computers during a one-year period.

90. In order to convict ASSANGE of conspiracy, in violation of Title 18, U.S. Code, Section 371, the United States must establish the elements set forth in Paragraph 86 of the Initial Extradition Affidavit. I hereby incorporate that Paragraph by reference. As detailed in the Second Superseding Indictment, the United States will establish that, beginning in at least 2009, ASSANGE conspired with other individuals, in and out of WikiLeaks, to access computers without authorization. In furtherance of the conspiracy, ASSANGE agreed with others to recruit computer hackers to access computers without authorization in order to obtain classified information and other valuable information to provide to ASSANGE and WikiLeaks, and to otherwise benefit ASSANGE and WikiLeaks. As part of the conspiracy, ASSANGE agreed to assist Manning in cracking an encrypted password hash stored on U.S. Department of Defense computers connected to SIPRNet, a U.S. government network used for classified documents and communications. In addition, ASSANGE gained unauthorized access to a government computer system of a NATO country, and personally and through a conduit, provided hacking targets (including targets in the United States) to members of hacking groups, among other overt acts specified in the Second Superseding Indictment.

91. Paragraph 88 of the Initial Extradition Affidavit sets forth a non-exhaustive list of the type of evidence that the United States will use at trial to prove Count Two (which was then numbered as Count 18). I hereby incorporate that Paragraph by reference. In addition to the evidence discussed in that Paragraph, the United States will introduce evidence that includes, but is not limited to, recordings and transcripts of public statements made by ASSANGE and other WikiLeaks associates, testimony from former computer hackers who communicated directly with

ASSANGE and/or other members of WikiLeaks, forensic evidence recovered from the computers of hackers who communicated directly with ASSANGE and/or other members of WikiLeaks, testimony from FBI agents who investigated the hacking groups Gnosis, LulzSec, AntiSec, and Anonymous and the computer intrusions those groups committed, and representative(s) from victim(s) of computer intrusions referenced in the Second Superseding Indictment.

Counts 3, 4, and 18: Unauthorized Obtaining of National Defense Information

92. Counts Three, Four, and Eighteen of the Second Superseding Indictment remain unchanged from the prior Superseding Indictment, except that Count Two of the prior Superseding Indictment is now Count Eighteen in the Second Superseding Indictment. I therefore incorporate by reference Paragraphs 65 through 69 of the Initial Extradition Affidavit, which describe the pertinent law, allegations, and evidence related to these charges.

Counts 5-8: Unauthorized Obtaining and Receiving of National Defense Information

93. Counts Five through Eight of the Second Superseding Indictment remain unchanged from the prior Superseding Indictment. I therefore incorporate by reference Paragraphs 70 through 73 of the Initial Extradition Affidavit, which describe the pertinent law, allegations, and evidence related to these charges.

Counts 9-11: Unauthorized Disclosure of National Defense Information

94. Counts Nine through Eleven of the Second Superseding Indictment remain unchanged from the prior Superseding Indictment. I therefore incorporate by reference Paragraphs 74 through 77 of the Initial Extradition Affidavit, which describe the pertinent law, allegations, and evidence related to these charges.

Counts 12-14: Unauthorized Disclosure of National Defense Information

95. Counts Twelve through Fourteen of the Second Superseding Indictment remain unchanged from the prior Superseding Indictment. I therefore incorporate by reference Paragraphs 78 through 80 of the Initial Extradition Affidavit, which describe the pertinent law, allegations, and evidence related to these charges.

Counts 15-17: Unauthorized Disclosure of National Defense Information

96. Counts Fifteen through Seventeen of the Second Superseding Indictment charge ASSANGE with Unauthorized Disclosure of National Defense Information, in violation of Title 18, U.S. Code, Section 793(e). Paragraph 81 of the Initial Extradition Affidavit describes the pertinent U.S. law related to this charge, and I hereby incorporate that Paragraph here.

97. To prove Counts Fifteen and Sixteen of the Second Superseding Indictment, the United States will establish that from in or around July 2010 to April 2019, ASSANGE distributed to persons not authorized to receive them, and published on WikiLeaks and caused to be published on the internet, Afghanistan war-related significant activity reports and Iraq war-related significant activity reports that were stolen from the United States and described information that U.S. and coalition forces had received, including information from local Afghans and Iraqis. These reports contained the names, and in some cases information about the locations, of local Afghans and Iraqis who had provided information to American and coalition forces. The evidence at trial will show that, by publishing these documents without redacting the sources' names or other identifying information of the sources, ASSANGE created a grave and imminent risk that the sources he named would suffer serious physical harm and/or arbitrary detention.

98. To prove Count Seventeen of the Second Superseding Indictment, the United States will establish that from in or around July 2010 to April 2019, ASSANGE distributed to persons not authorized to receive them, and published on WikiLeaks and caused to be published on the internet, diplomatic cables that were stolen from the U.S. Department of State. These cables, which generally were communications from U.S. Department of State employees living abroad to U.S. government officials in the United States, contained the names of hundreds of innocent people who provided information to the U.S. government. These sources included journalists, religious leaders, human rights advocates, and political dissidents who were living in repressive regimes and reported to the United States the abuses of their own government at great risk to their own safety. By publishing the names of these vulnerable people, ASSANGE outed them to their own governments and potentially put them in grave and immediate risk of being unjustly jailed, physically assaulted, or worse. At the time he distributed and published the un-redacted names of the U.S. Department of State's sources, ASSANGE was aware that doing so would cause serious risk to innocent human life.

99. Paragraph 84 of the Initial Extradition Affidavit sets forth a non-exhaustive list of the type of evidence that the United States will use at trial to prove Count 1. I hereby incorporate by reference that Paragraph here.

IDENTIFICATION INFORMATION

100. Paragraph 89 of the Initial Extradition Affidavit contains information identifying ASSANGE, and I hereby incorporate by reference that Paragraph here.

SURRENDER OF PROPERTY

101. Pursuant to Article 16 of the Annex to the U.S.-UK Extradition Instrument, it is requested that any items relevant to the charged offenses and found in ASSANGE's possession at the time of his arrest be delivered to the United States if he is found to be extraditable.

SUPPLEMENTING THE REQUEST

102. Should the British authorities decide this matter requires further information in order to reach a decision on extradition, I request the opportunity to present supplemental materials, pursuant to Article 10 of the U.S.-U.K. Extradition Treaty, prior to the rendering of the decision.

CONCLUSION

103. This affidavit is sworn to before a U.S. Magistrate Judge legally authorized to administer an oath for this purpose. I have thoroughly reviewed this affidavit and the attachments thereto, and attest that this evidence indicates that ASSANGE is guilty of the offenses charged in the superseding indictment.

Gordon D. Kromberg
Assistant United States Attorney
Office of the United States Attorney

Respectfully submitted and sworn to
via telephone on this 14th day of July 2020

Ivan D. Davis
United States Magistrate Judge
Eastern District of Virginia
UNITED STATES OF AMERICA