FILED
IN OPEN COURT
JUN 24 2020
CLERK U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

| | |
|---|---|
| UNITED STATES OF AMERICA<br><br>v.<br><br>JULIAN PAUL ASSANGE,<br><br>Defendant. | Criminal No. 1:18-cr-111 (CMH)<br><br>Count 1: 18 U.S.C. § 793(g)<br>Conspiracy To Obtain and Disclose National Defense Information<br><br>Count 2: 18 U.S.C. § 371<br>Conspiracy to Commit Computer Intrusions<br><br>Counts 3, 4: 18: 18 U.S.C. §§ 793(b) and 2<br>Obtaining National Defense Information<br><br>Counts 5-8: 18 U.S.C. §§ 793(c) and 2<br>Obtaining National Defense Information<br><br>Counts 9-11: 18 U.S.C. §§ 793(d) and 2<br>Disclosure of National Defense Information<br><br>Counts 12-14: 18 U.S.C. §§ 793(e) and 2<br>Disclosure of National Defense Information<br><br>Counts 15-17: 18 U.S.C. § 793(e)<br>Disclosure of National Defense Information |

**SECOND SUPERSEDING INDICTMENT**

June 2020 Term – at Alexandria, Virginia

THE GRAND JURY CHARGES THAT:

GENERAL ALLEGATIONS

**A. ASSANGE and WikiLeaks**

1. From at least 2007,[1] JULIAN PAUL ASSANGE ("ASSANGE") was the public

[1] When the Grand Jury alleges in this Superseding Indictment that an event occurred on a particular date, the Grand Jury means to convey that the event occurred "on or about" that date.

face of "WikiLeaks," a website he founded with others as an "intelligence agency of the people." To obtain information to release on the WikiLeaks website, ASSANGE recruited sources and predicated the success of WikiLeaks in part upon the recruitment of sources to (i) illegally circumvent legal safeguards on information, including classification restrictions and computer and network access restrictions; (ii) provide that illegally obtained information to WikiLeaks for public dissemination; and (iii) continue the pattern of illegally procuring and providing classified and hacked information to WikiLeaks for distribution to the public.

2. 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. ASSANGE designed WikiLeaks to focus on information restricted from public disclosure by law, precisely because of the value of that information. WikiLeaks's website explicitly solicited censored, otherwise restricted, and "classified" materials. As the website stated, "WikiLeaks accepts *classified, censored,* or otherwise *restricted* material of *political, diplomatic, or ethical significance.*"

3. To recruit individuals to hack into computers and/or illegally obtain and disclose classified information to WikiLeaks, the WikiLeaks website posted a detailed list of "The Most Wanted Leaks of 2009," organized by country. The post stated that documents or materials nominated to the list must "[b]e 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."

4. 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.

5. 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."

6. In October 2009, ASSANGE spoke at the "Hack in the Box Security Conference" in Malaysia. ASSANGE told the audience, "I was a famous teenage hacker in Australia, and I've been reading generals' emails since I was 17." ASSANGE referenced the conference's "capture the flag" hacking contest, and noted that WikiLeaks had its own list of "flags" that it wanted captured—namely, the list of "Most Wanted Leaks" posted on the WikiLeaks website. To recruit sources to engage in computer hacking and steal classified information for publication by WikiLeaks, ASSANGE encouraged his audience to obtain and provide to WikiLeaks information responsive to that list.

7. As of November 2009, WikiLeaks's "Most Wanted Leaks" for the United States included the following:

a. "Bulk Databases," including an encyclopedia used by the United States intelligence community, called "Intellipedia," and the unclassified, but non-public, CIA Open Source Center database; and

b. "Military and Intelligence" documents, including documents that the list described as classified up to the **SECRET** level, for example, "Iraq and Afghanistan Rules of Engagement 2007-2009 (SECRET)"; operating and interrogation procedures at Guantanamo Bay, Cuba; documents relating to Guantanamo detainees; CIA detainee interrogation videos; and information about certain weapons systems.

**B. Chelsea Manning**

8. From 2009 to 2010, Chelsea Manning, then known as Bradley Manning, was an intelligence analyst in the United States Army who was deployed to Forward Operating Base Hammer in Iraq.

9. In connection with the duties of an intelligence analyst, Manning had access to United States Department of Defense computers connected to the Secret Internet Protocol Network, a United States government network used for classified documents and communications. As explained below, Manning also was using the computers to download classified records to transmit to WikiLeaks. Army regulations prohibited Manning from attempting to bypass or circumvent security mechanisms on government-provided information systems and from sharing personal accounts and authenticators, such as passwords.

10. Manning held a "TOP SECRET" security clearance, and signed a classified information nondisclosure agreement, acknowledging that the unauthorized disclosure or retention or negligent handling of classified information could cause irreparable injury to the United States or be used to the advantage of a foreign nation.

*i. Manning and the Most Wanted Leaks*

11. Beginning by at least November 2009, Manning responded to ASSANGE's solicitation of classified information made through the WikiLeaks website. For example, WikiLeaks's "Military and Intelligence" "Most Wanted Leaks" category, as described above, solicited CIA detainee interrogation videos. On November 28, 2009, Manning in turn searched the classified network search engine, "Intelink," for "retention+of+interrogation+videos." The next day, Manning searched the classified network for "detainee+abuse," which was consistent with the "Most Wanted Leaks" request for "Detainee abuse photos withheld by the Obama administration" under WikiLeaks's "Military and Intelligence" category.

12. On November 30, 2009, Manning saved a text file entitled "wl-press.txt" to an external hard drive and to an encrypted container on Manning's computer. The file stated, "You can currently contact our investigations editor directly in Iceland +354 862 3481; 24 hour service; ask for 'Julian Assange.'" Similarly, on December 8 and 9, 2009, Manning ran several searches on Intelink relating to Guantanamo Bay detainee operations, interrogations, and standard operating procedures or "SOPs." These search terms were yet again consistent with WikiLeaks's "Most Wanted Leaks," which sought Guantanamo Bay operating and interrogation SOPs under the "Military and Intelligence" category.

*ii. Manning Steals and Provides to WikiLeaks Classified Information about Iraq, Afghanistan, and Guantanamo Bay*

13. Between January 2010 and May 2010, consistent with WikiLeaks's "Most Wanted Leaks" solicitation of bulk databases and military and intelligence categories, Manning downloaded four nearly complete databases from departments and agencies of the United States. These databases contained approximately 90,000 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. The United States had classified many of these records up to the **SECRET** level pursuant to Executive Order No. 13526 or its predecessor orders. Manning nevertheless provided the documents to WikiLeaks, so that WikiLeaks could publicly disclose them on its website.

14. No later than January 2010, Manning repeatedly used an online chat service, Jabber.ccc.de, to chat with ASSANGE, who used multiple monikers attributable to him.[2]

15. On March 7, 2010, Manning asked ASSANGE how valuable the Guantanamo Bay detainee assessment briefs would be. After confirming that ASSANGE thought they had value, on March 8, 2010, Manning told ASSANGE that Manning was "throwing everything [Manning had] on JTF GTMO [Joint Task Force, Guantanamo] at [ASSANGE] now." ASSANGE responded, "ok, great!"

16. On March 8, 2010, when Manning brought up the "osc," meaning the CIA Open Source Center, ASSANGE replied, "that's something we want to mine entirely, btw," which was consistent with WikiLeaks's list of "Most Wanted Leaks," which solicited "the complete CIA Open Source Center analytical database," an unclassified (but non-public) database.

17. On March 8, 2010, Manning used a Secure File Transfer Protocol ("SFTP") connection to transmit the detainee assessment briefs, classified **SECRET**, to a cloud drop box operated by WikiLeaks, with an X directory that WikiLeaks had designated for Manning's use.

18. On March 8, 2010, in response to Manning's comment that, after transmitting the detainee assessment briefs to ASSANGE and WikiLeaks, "thats all i really have got left," and to

[2] The Grand Jury will allege that the person using these monikers is ASSANGE without reference to the specific moniker used.

encourage Manning to continue to steal classified documents from the United States and provide them to WikiLeaks, ASSANGE replied, "curious eyes never run dry in my experience."

*iii. ASSANGE Agrees to Help Manning Crack a Password*

19. On March 8, 2010, ASSANGE told Manning that ASSANGE would have someone try to crack a password hash to enable Manning to hack into a U.S. government computer. Specifically, ASSANGE agreed to assist Manning in cracking a password hash stored on United States Department of Defense computers connected to the Secret Internet Protocol Network.

20. The encrypted password hash that Manning gave to ASSANGE to crack -- following ASSANGE's "curious eyes never run dry" comment -- was stored as a "hash value" in a computer file that was accessible only by users with administrative-level privileges. Manning did not have administrative-level privileges, and used special software, namely a Linux operating system, to access the computer file and obtain the encrypted password hash that Manning then provided to ASSANGE.

21. On March 10, 2010, ASSANGE requested more information from Manning related to the encrypted password hash, because he had so far been unable to crack it. Had ASSANGE and Manning successfully cracked the encrypted password hash, Manning may have been able to log onto computers under a username that did not belong to Manning. Such a measure would have made it more difficult for investigators to identify Manning as the source of unauthorized disclosures of classified information.

22. On March 10, 2010, after ASSANGE told Manning that there was "a username in the gitmo docs," Manning told ASSANGE, "any usernames should probably be filtered, period."

23. On March 10, 2010, in response to Manning's question whether there was "anything useful" in the "gitmo docs," ASSANGE responded, in part, that "these sorts of things are always motivating to other sources too." ASSANGE stated, "Hence the feeling is people can give us stuff for anything not as 'dangerous as gitmo' on the one hand, and on the other, for people who know more, there's a desire to eclipse."

24. Following ASSANGE's "curious eyes never run dry" comment, on March 22, 2010, Manning downloaded from the Secret Internet Protocol Network multiple Iraq rules of engagement files (consistent with WikiLeaks's "Most Wanted Leaks" solicitation), and provided them to ASSANGE and WikiLeaks. The rules of engagement files delineated the circumstances and limitations under which United States forces would initiate or continue combat engagement upon encountering other forces. WikiLeaks's disclosure of this information would allow enemy forces in Iraq and elsewhere to anticipate certain actions or responses by U.S. armed forces and to carry out more effective attacks.

25. Following ASSANGE's "curious eyes never run dry" comment, between March 28, 2010, and April 9, 2010, and consistent with WikiLeaks's solicitation of bulk databases and classified materials of diplomatic significance, Manning further used a U.S. Department of Defense computer to download over 250,000 U.S. Department of State cables, which were classified up to the **SECRET** level. Manning uploaded these cables to ASSANGE and WikiLeaks through an SFTP connection to a cloud drop box operated by WikiLeaks, with an X directory that WikiLeaks had designated for Manning's use.

26. At the time ASSANGE agreed to receive and received from Manning for the purpose of public disclosure on WikiLeaks the classified Guantanamo Bay detainee assessment briefs, the U.S. Department of State Cables, and the Iraq rules of engagement files, ASSANGE

knew that Manning was unlawfully taking and disclosing them, and at the time ASSANGE agreed to assist Manning in cracking the encrypted password hash, ASSANGE knew that Manning was taking and illegally providing WikiLeaks with classified documents and records containing national defense information from classified databases. For example, not only had ASSANGE already received thousands of military-related documents, including the Afghanistan war-related significant activity reports and Iraq war-related significant activity reports, classified up to the **SECRET** level from Manning, but Manning and ASSANGE also had chatted about (i) military jargon and references to current events in Iraq, which showed that Manning was a government or military source; (ii) the "releasability" of certain information by ASSANGE; (iii) measures to prevent the discovery of Manning as ASSANGE's source, such as clearing logs and use of a "cryptophone"; and (iv) a code phrase to use if something went wrong.

27. On April 5, 2010, WikiLeaks released on its website the rules of engagement files that Manning provided. It entitled four of the documents as follows: "US Rules of Engagement for Iraq; 2007 flowchart," "US Rules of Engagement for Iraq; Refcard 2007," "US Rules of Engagement for Iraq, March 2007," and "US Rules of Engagement for Iraq, Nov 2006." All of these documents had been classified as **SECRET**, except for the "US Rules of Engagement for Iraq; Refcard 2007," which was unclassified but for official use only.

28. Manning was arrested on May 27, 2010.

29. In July 2010, at a conference in New York City of "Hackers on Planet Earth," a WikiLeaks associate urged attendees to leak to WikiLeaks. That WikiLeaks associate (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."

30. In July 2010, WikiLeaks published approximately 75,000 significant activity reports related to the war in Afghanistan, classified up to the **SECRET** level, illegally provided to WikiLeaks by Manning.

31. In October 2010, WikiLeaks published approximately 400,000 significant activity reports related to the war in Iraq, classified up to the **SECRET** level, illegally provided to WikiLeaks by Manning.

32. In November 2010, WikiLeaks started publishing redacted versions of U.S. State Department cables, classified up to the **SECRET** level, illegally provided to WikiLeaks by Manning.

33. In April 2011, WikiLeaks published approximately 800 Guantanamo Bay detainee assessment briefs, classified up to the **SECRET** level, illegally provided to WikiLeaks by Manning.

34. In August and September 2011, WikiLeaks published unredacted versions of approximately 250,000 U.S. State Department Cables, classified up to the **SECRET** level, which were illegally provided to WikiLeaks by Manning.

### C. Teenager, Manning, and NATO Country-1

35. 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.

36. In early 2010, ASSANGE 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.

37. Beginning in January 2010, Manning repeatedly searched for classified information about NATO Country-1.

38. On February 14, 2010, Manning downloaded classified State Department materials regarding the government of NATO Country-1. On February 18, 2010, WikiLeaks posted to its website a classified cable from the U.S. Embassy in NATO Country-1, that WikiLeaks received from Manning.

39. On March 5, 2010, ASSANGE told Manning about having received stolen banking documents from a source who, in fact, was Teenager.

40. 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.

41. In early 2010, 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.

42. 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.

43. On March 29, 2010, WikiLeaks posted to its website classified State Department materials regarding officials in the government of NATO Country-1, which Manning had downloaded on February 14, 2010.

44. On July 21, 2010, 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. 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.

45. 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."

46. In September 2010, 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**

47. 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."

48. Later in December 2010, "Laurelai," a hacker affiliated with Anonymous, who identified herself as a member of the hacking group "Gnosis," contacted Teenager. 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.

49. In January 2011, 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.

50. 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").

51. On February 7, 2011, Teenager messaged ASSANGE that Gnosis had hacked U.S. Cybersecurity Company.

52. 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.

53. On February 15, 2011, in a chat with a hacker with the moniker "elChe," Laurelai characterized herself as "part of WikiLeaks staff ... hacker part."

54. 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.

55. On February 17, 2011, Teenager told Laurelai that WikiLeaks was the world's largest hacking organization.

56. 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).

57. On March 6, 2011, Laurelai offered WikiLeaks (through Teenager) "unpublished zero days" (vulnerabilities that can be used to hack computer systems).

58. On March 15, 2011, 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.

59. In May 2011, 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."

60. 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 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.

61. On June 7, 2011, Sabu was arrested. Shortly thereafter, Sabu began cooperating with the FBI.

62. In June 2011, after LulzSec took credit for a purported DDoS attack against the CIA's public-facing website, 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."

63. 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.

64. 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."

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

66. In the fall of 2011, Teenager left WikiLeaks.

## E. Sabu, Hammond, and ASSANGE

67. 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").

68. On December 29, 2011, in a chat with other hackers on an IRC channel called "#Lulzxmas," a hacker affiliated with LulzSec/AntiSec, Jeremy Hammond, told the others that information hacked from Intelligence Consulting Company was being sent to Wikileaks.

69. On December 29, 2011, in a chat with other hackers on the "#Lulzxmas" IRC channel, 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."

70. In December 2011, 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.

71. 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."

72. In January 2012, 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, Sabu used Jabber to chat with this WikiLeaks leader, who used various monikers on Jabber.ccc.de that are attributed to ASSANGE for reasons including but not limited to the following[3]:

a. When Sabu suggested that it had to be "boring" to stay at Ellingham Hall "every day with an ankle bracelette [sic] to look at all day," ASSANGE responded that he 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...." ASSANGE said that he was very busy, but trusted only himself to deal with sources. He said that 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.

[3] For the remainder of the Second Superseding Indictment, the Grand Jury will allege that the person using these monikers is ASSANGE without reference to the specific moniker used.

b. On January 16, 2012, Sabu asked ASSANGE how "the case [was] going." In response, ASSANGE said, "[i]t's a huge legal-political quagmire" and also said, "[i]f I'm going down it sure hasn't been without a fight."

c. On January 16, 2012, ASSANGE told Sabu that he was making a television show in which he would be interviewing "ultimate insiders and outsiders on the fate of the world." ASSANGE told Sabu that, on his show, he would interview guests including presidents, the leader of Hezbollah, and participants in the Occupy Movement. On February 21, 2012, ASSANGE told Sabu that he had, the previous day, interviewed a former Guantanamo Bay prisoner who now ran the website cageprisoners.org. [4]

73. On January 16, 2012, and in response to a message from Sabu that stated, "If you have any targets in mind by all means let us know," ASSANGE 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.

74. On January 21, 2012, ASSANGE 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.

---

[4] 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.

75. On February 21, 2012, and in response to Sabu's request, ASSANGE provided Sabu with a computer script to search for emails hacked from Intelligence Consulting Company.

76. On February 21, 2012, 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*.

77. On February 22, 2012, Hammond told Sabu that, at ASSANGE's "indirect" request, Hammond had spammed the Intelligence Consulting Company again.

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

79. On February 27, 2012, Hammond told Sabu, "we started giving JA" materials that had been obtained from other hacks.

80. On February 27, 2012, Hammond told Sabu that ASSANGE was talking to elChe.

81. On February 28, 2012, 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.

82. In March 2012, Hammond was arrested.

## F. ASSANGE's Efforts to Recruit System Administrators

83. 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.

84. 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.

85. In June 2013, a WikiLeaks associate ("WLA-4") traveled with Snowden from Hong Kong to Moscow.

86. On December 31, 2013, at the annual conference of the Chaos Computer Club ("CCC") in Germany, 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."

87. 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. . . ."

**G. ASSANGE and WikiLeaks Continue to Recruit**

88. On May 6, 2014, at a re:publica conference in Germany, 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."

89. 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.

90. In an interview on May 25, 2015, 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.

91. On June 18, 2015, at an event sponsored by the Rosa Luxemburg Foundation in Germany, 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.

92. 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 a list of "The Most Wanted Leaks of 2009," which stated that documents or materials nominated to the list must "[b]e 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."

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

93. 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.

94. The significant activity reports from the Afghanistan and Iraq wars that ASSANGE disseminated and published included names of local Afghans and Iraqis who had provided information to U.S. and coalition forces. The State Department cables that WikiLeaks disseminated and published included names of persons throughout the world who provided information to the U.S. government in circumstances in which they could reasonably expect that their identities would be kept confidential. 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, and the political conditions within their countries, at great risk to their own safety. By disseminating and publishing these documents without redacting the human sources' names or other identifying information, ASSANGE created a grave and imminent risk that the innocent people he named would suffer serious physical harm and/or arbitrary detention.

95. On July 30, 2010, the *New York Times* published an article entitled "Taliban Study WikiLeaks to Hunt Informants." The article stated that, after the release of the Afghanistan war significant activity reports, a member of the Taliban contacted the *New York Times* and stated, "We are studying the report. We knew about the spies and people who collaborate with U.S. forces. We will investigate through our own secret service whether the people mentioned are really spies working for the U.S. If they are U.S. spies, then we know how to punish them." When confronted about such reports, ASSANGE said, "The Taliban is not a coherent outfit, but we don't say that it is absolutely impossible that anything we ever publish will ever result in harm—we cannot say that."

96. On May 2, 2011, United States armed forces raided the compound of Osama bin Laden in Abbottabad, Pakistan. During the raid, they collected a number of items of digital media, which included the following: (1) a letter from bin Laden to another member of the terrorist organization al-Qaeda in which bin Laden requested that the member gather the Department of Defense material posted to WikiLeaks, (2) a letter from that same member of al-Qaeda to bin Laden with information from the Afghanistan War Documents provided by Manning to WikiLeaks and released by WikiLeaks, and (3) Department of State information provided by Manning to WikiLeaks and released by WikiLeaks.

97. The following are examples of significant activity reports related to the Afghanistan and Iraq wars that ASSANGE disseminated and published without redacting the names of human sources who were vulnerable to retribution by the Taliban in Afghanistan or the insurgency in Iraq:

a. Classified Document C1 was a 2007 threat report containing details of a planned anti-coalition attack at a specific location in Afghanistan. Classified Document C1 named the local human source who reported the planned attack. Classified Document C1 was classified at the **SECRET** level.

b. Classified Document C2 was a 2009 threat report identifying a person who supplied weapons at a specific location in Afghanistan. Classified Document C2 named the local human source who reported information. Classified Document C2 was classified at the **SECRET** level.

c. Classified Document D1 was a 2009 report discussing an improvised explosive device ("IED") attack in Iraq. Classified Document D1 named local human

sources who provided information on the attack. Classified Document D1 was classified at the **SECRET** level.

d. Classified Document D2 was a 2008 report that named a local person in Iraq who had turned in weapons to coalition forces and had been threatened afterward. Classified Document D2 was classified at the **SECRET** level.

98. The following are examples of State Department cables that ASSANGE disseminated and published without redacting the names of human sources who were vulnerable to retribution.

a. Classified Document A1 was a 2009 State Department cable discussing a political situation in Iran. Classified Document A1 named a human source of information located in Iran and indicated that the source's identity needed to be protected. Classified Document A1 was classified at the **SECRET** level.

b. Classified Document A2 was a 2009 State Department cable discussing political dynamics in Iran. Classified Document A2 named a human source of information who regularly traveled to Iran and indicated that the source's identity needed to be protected. Classified Document A2 was classified at the **SECRET** level.

c. Classified Document A3 was a 2009 State Department cable discussing issues related to ethnic conflict in China. Classified Document A3 named a human source of information located in China and indicated that the source's identity needed to be protected. Classified Document A3 was classified at the **SECRET** level.

d. Classified Document A4 was a 2009 State Department cable discussing relations between Iran and Syria. Classified Document A4 named human sources of

information located in Syria and indicated that the sources' identities needed to be protected. Classified Document A4 was classified at the **SECRET** level.

e. Classified Document A5 was a 2010 State Department cable discussing human rights issues in Syria. Classified Document A5 named a human source of information located in Syria and indicated that the source's identity needed to be protected. Classified Document A5 was classified at the **SECRET** level.

99. 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.

100. In an interview in August 2010, ASSANGE called it "regrettable" that sources disclosed by WikiLeaks "may face some threat as a result." But, in the same interview, ASSANGE insisted that "we are not obligated to protect other people's sources, military sources or spy organization sources, except from unjust retribution," adding that in general "there are numerous cases where people sell information . . . or frame others or are engaged in genuinely traitorous behavior and actually that is something for the public to know about."

101. ASSANGE also knew that his dissemination and publication of the State Department cables endangered sources whom he named as having provided information to the State Department and other agencies of the United States. In a letter dated November 27, 2010 from the State Department's legal adviser to ASSANGE and his lawyer, ASSANGE was informed, among other things, that publication of the State Department cables would "[p]lace at risk the lives of countless innocent individuals—from journalists to human rights activists and bloggers to soldiers to individuals providing information to further peace and security." Prior to his dissemination and publication of the unredacted State Department cables, ASSANGE claimed

that he intended "to gradually roll [the cables] out in a safe way" by partnering with mainstream media outlets and "read[ing] through every single cable and redact[ing] identities accordingly." Nonetheless, while ASSANGE and WikiLeaks published some of the cables in redacted form beginning in November 2010, they disseminated and published over 250,000 cables in August and September 2011, in unredacted form, that is, without redacting the names of the human sources.

## I. U.S. Law to Protect Classified Information

102. Executive Order No. 13526 and its predecessor orders define the classification levels assigned to classified information. Under the Executive Order, information may be classified as "**SECRET**" if its unauthorized disclosure reasonably could be expected to cause serious damage to the national security, and information may be classified as "**CONFIDENTIAL**" if its unauthorized disclosure reasonably could be expected to cause damage to the national security. Further, under the Executive Order, classified information can generally only be disclosed to those persons who have been granted an appropriate level of United States government security clearance and possess a need to know the classified information in connection to their official duties.

103. At no point was ASSANGE a citizen of the United States, nor did he hold a United States security clearance or otherwise have authorization to receive, possess, or communicate classified information.

## COUNT 1

(Conspiracy to Obtain and Disclose National Defense Information)

A. The general allegations of this Superseding Indictment are re-alleged and incorporated into this Count as though fully set forth herein.

Illegal Objects of the Conspiracy

B. Between in or about 2009 and continuing until in or about 2015, in an offense begun and committed outside of the jurisdiction of any particular state or district of the United States, the defendant, JULIAN PAUL ASSANGE, who will be first brought to the Eastern District of Virginia, knowingly and unlawfully conspired with other co-conspirators, known and unknown to the Grand Jury, to commit the following offenses against the United States:

1. To obtain documents, writings, and notes connected with the national defense, for the purpose of obtaining information respecting the national defense—including detainee assessment briefs related to detainees who were held at Guantanamo Bay; U.S. State Department cables; and Iraq rules of engagement files classified up to the **SECRET** level—and with reason to believe that the information was to be used to the injury of the United States and the advantage of any foreign nation, in violation of Title 18, United States Code, Section 793(b);

2. To receive and obtain documents, writings, and notes connected with the national defense—including detainee assessment briefs related to detainees who were held at Guantanamo Bay; U.S. State Department cables; and Iraq rules of engagement files classified up to the **SECRET** level—for the purpose of obtaining information respecting the national defense, and knowing and with reason to believe at the time such materials were received and obtained, they had been and would be taken, obtained, and disposed of

by a person contrary to the provisions of Chapter 37 of Title 18 of the United States Code, in violation of Title 18, United States Code, Section 793(c);

3. To willfully communicate documents relating to the national defense—namely, detainee assessment briefs related to detainees who were held at Guantanamo Bay; U.S. State Department cables; Iraq rules of engagement files; and documents containing the names of individuals in Afghanistan, Iraq, and elsewhere around the world, who risked their safety and freedom by providing information to the United States and our allies, which were classified up to the **SECRET** level—from persons having lawful possession of or access to such documents, to persons not entitled to receive them, in violation of Title 18, United States Code, Section 793(d); and

4. To willfully communicate documents relating to the national defense—namely, (i) for Manning to communicate to ASSANGE the detainee assessment briefs related to detainees who were held at Guantanamo Bay, U.S. State Department cables, and Iraq rules of engagement files classified up to the **SECRET** level, and (ii) for ASSANGE to communicate documents classified up to the **SECRET** level containing the names of individuals in Afghanistan, Iraq, and elsewhere around the world, who risked their safety and freedom by providing information to the United States and our allies to certain individuals and the public—from persons in unauthorized possession of such documents to persons not entitled to receive them, in violation of Title 18, United States Code, Section 793(e).

C. In furtherance of the conspiracy, and to accomplish its objects, ASSANGE and his conspirators committed lawful and unlawful overt acts, including but not limited to, those described in the General Allegations Section of this Superseding Indictment.

(All in violation of Title 18, United States Code, Section 793(g))

## COUNT 2

(Conspiracy To Commit Computer Intrusions)

A. The general allegations of this Superseding Indictment are re-alleged and incorporated into this Count as though fully set forth herein.

Illegal Objects of the Conspiracy

B. Between in or about 2009 and continuing until in or about 2015, in an offense begun and committed outside of the jurisdiction of any particular state or district of the United States, the defendant, JULIAN PAUL ASSANGE, who will be first brought to the Eastern District of Virginia, knowingly and unlawfully conspired with other co-conspirators, known and unknown to the Grand Jury, to commit the following offenses against the United States:

1. To knowingly access a computer, without authorization and exceeding authorized access, 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 in violation of 18 U.S.C. §§ 1030(a)(1) and 1030(c)(1)(A);

2. To intentionally access a computer, without authorization and exceeding authorized access, and thereby 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, in violation of 18 U.S.C. §§ 1030(a)(2) and 1030(c)(2)(B);

3. 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, in violation of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B); and

4. 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, in violation of 18 U.S.C. §§ 1030(a)(5)(B) and 1030(c)(4)(A).

C. In furtherance of the conspiracy, and to accomplish its objects, ASSANGE and his conspirators committed lawful and unlawful overt acts, including but not limited to, those described in the General Allegations Section of this Indictment.

(All in violation of Title 18, United States Code, Sections 371)

## COUNT 3

(Unauthorized Obtaining of National Defense Information)
(State Department Cables)

A. The general allegations of this Superseding Indictment are re-alleged and incorporated into this Count as though fully set forth herein.

B. Between in or about November 2009 and in or about May 2010, in an offense begun and committed outside of the jurisdiction of any particular state or district of the United States, the defendant, JULIAN PAUL ASSANGE, who will be first brought to the Eastern District of Virginia, and others unknown to the Grand Jury, knowingly and unlawfully obtained and aided, abetted, counseled, induced, procured and willfully caused Manning to obtain documents, writings, and notes connected with the national defense, for the purpose of obtaining information respecting the national defense—namely, U.S. Department of State cables classified up to the **SECRET** level—and with reason to believe that the information was to be used to the injury of the United States or the advantage of any foreign nation.

(All in violation of Title 18, United States Code, Sections 793(b) and 2)

## COUNT 4

(Unauthorized Obtaining of National Defense Information)
(Iraq Rules of Engagement Files)

A. The general allegations of this Superseding Indictment are re-alleged and incorporated into this Count as though fully set forth herein.

B. Between in or about November 2009 and in or about May 2010, in an offense begun and committed outside of the jurisdiction of any particular state or district of the United States, the defendant, JULIAN PAUL ASSANGE, who will be first brought to the Eastern District of Virginia, and others unknown to the Grand Jury, knowingly and unlawfully obtained and aided, abetted, counseled, induced, procured and willfully caused Manning to obtain documents, writings, and notes connected with the national defense, for the purpose of obtaining information respecting the national defense—namely, Iraq rules of engagement files classified up to the **SECRET** level—and with reason to believe that the information was to be used to the injury of the United States or the advantage of any foreign nation.

(All in violation of Title 18, United States Code, Sections 793(b) and 2)

## COUNT 5

(Attempted Unauthorized Obtaining and Receiving of National Defense Information)

A. The general allegations of this Superseding Indictment are re-alleged and incorporated into this Count as though fully set forth herein.

B. Between in or about November 2009 and in or about May 2010, in an offense begun and committed outside of the jurisdiction of any particular state or district of the United States, the defendant, JULIAN PAUL ASSANGE, who will be first brought to the Eastern District of Virginia, and others unknown to the Grand Jury, knowingly and unlawfully attempted to receive and obtain documents, writings, and notes connected with the national defense—namely, information stored on the Secret Internet Protocol Network classified up to the **SECRET** level—for the purpose of obtaining information respecting the national defense, knowing and having reason to believe, at the time that he attempted to receive and obtain them, that such materials would be obtained, taken, made, and disposed of by a person contrary to the provisions of Chapter 37 of Title 18 of the United States Code.

(All in violation of Title 18, United States Code, Sections 793(c) and 2)

## COUNT 6

(Unauthorized Obtaining and Receiving of National Defense Information)
(Detainee Assessment Briefs)

A. The general allegations of this Superseding Indictment are re-alleged and incorporated into this Count as though fully set forth herein.

B. Between in or about November 2009 and in or about May 2010, in an offense begun and committed outside of the jurisdiction of any particular state or district of the United States, the defendant, JULIAN PAUL ASSANGE, who will be first brought to the Eastern District of Virginia, knowingly and unlawfully received and obtained documents, writings, and notes connected with the national defense—namely, detainee assessment briefs classified up to the **SECRET** level related to detainees who were held at Guantanamo Bay—for the purpose of obtaining information respecting the national defense, knowing and having reason to believe, at the time that he received and obtained them, that such materials had been and would be obtained, taken, made, and disposed of by a person contrary to the provisions of Chapter 37 of Title 18 of the United States Code.

(All in violation of Title 18, United States Code, Sections 793(c) and 2)

## COUNT 7

(Unauthorized Obtaining and Receiving of National Defense Information)
(State Department Cables)

A. The general allegations of this Superseding Indictment are re-alleged and incorporated into this Count as though fully set forth herein.

B. Between in or about November 2009 and in or about May 2010, in an offense begun and committed outside of the jurisdiction of any particular state or district of the United States, the defendant, JULIAN PAUL ASSANGE, who will be first brought to the Eastern District of Virginia, knowingly and unlawfully received and obtained documents, writings, and notes connected with the national defense—namely, U.S. Department of State cables classified up to the **SECRET** level—for the purpose of obtaining information respecting the national defense, knowing and having reason to believe, at the time that he received and obtained them, that such materials had been and would be obtained, taken, made, and disposed of by a person contrary to the provisions of Chapter 37 of Title 18 of the United States Code.

(All in violation of Title 18, United States Code, Sections 793(c) and 2)

## COUNT 8

(Unauthorized Obtaining and Receiving of National Defense Information)
(Iraq Rules of Engagement Files)

A. The general allegations of this Superseding Indictment are re-alleged and incorporated into this Count as though fully set forth herein.

B. Between in or about November 2009 and in or about May 2010, in an offense begun and committed outside of the jurisdiction of any particular state or district of the United States, the defendant, JULIAN PAUL ASSANGE, who will be first brought to the Eastern District of Virginia, knowingly and unlawfully received and obtained documents, writings, and notes connected with the national defense—namely, Iraq rules of engagement files classified up to the **SECRET** level—for the purpose of obtaining information respecting the national defense, knowing and having reason to believe, at the time that he received and obtained them, that such materials had been and would be obtained, taken, made, and disposed of by a person contrary to the provisions of Chapter 37 of Title 18 of the United States Code.

(All in violation of Title 18, United States Code, Sections 793(c) and 2)

## COUNT 9

(Unauthorized Disclosure of National Defense Information)
(Detainee Assessment Briefs)

A. The general allegations of this Superseding Indictment are re-alleged and incorporated into this Count as though fully set forth herein.

B. Between in or about November 2009 and in or about May 2010, in an offense begun and committed outside of the jurisdiction of any particular state or district of the United States, the defendant, JULIAN PAUL ASSANGE, who will be first brought to the Eastern District of Virginia, and others unknown to the Grand Jury, aided, abetted, counseled, induced, procured and willfully caused Manning, who had lawful possession of, access to, and control over documents relating to the national defense—namely, detainee assessment briefs classified up to the **SECRET** level related to detainees who were held at Guantanamo Bay—to communicate, deliver, and transmit the documents to ASSANGE, a person not entitled to receive them.

(All in violation of Title 18, United States Code, Sections 793(d) and 2)

## COUNT 10

(Unauthorized Disclosure of National Defense Information)
(State Department Cables)

A. The general allegations of this Superseding Indictment are re-alleged and incorporated into this Count as though fully set forth herein.

B. Between in or about November 2009 and in or about May 2010, in an offense begun and committed outside of the jurisdiction of any particular state or district of the United States, the defendant, JULIAN PAUL ASSANGE, who will be first brought to the Eastern District of Virginia, and others unknown to the Grand Jury, aided, abetted, counseled, induced, procured and willfully caused Manning, who had lawful possession of, access to, and control over documents relating to the national defense—namely, U.S. Department of State cables classified up to the **SECRET** level—to communicate, deliver, and transmit the documents to ASSANGE, a person not entitled to receive them.

(All in violation of Title 18, United States Code, Sections 793(d) and 2)

## COUNT 11

(Unauthorized Disclosure of National Defense Information)
(Iraq Rules of Engagement Files)

A. The general allegations of this Superseding Indictment are re-alleged and incorporated into this Count as though fully set forth herein.

B. Between in or about November 2009 and in or about May 2010, in an offense begun and committed outside of the jurisdiction of any particular state or district of the United States, the defendant, JULIAN PAUL ASSANGE, who will be first brought to the Eastern District of Virginia, and others unknown to the Grand Jury, aided, abetted, counseled, induced, procured and willfully caused Manning, who had lawful possession of, access to, and control over documents relating to the national defense—namely, Iraq rules of engagement files classified up to the **SECRET** level—to communicate, deliver, and transmit the documents to ASSANGE, a person not entitled to receive them.

(All in violation of Title 18, United States Code, Sections 793(d) and 2)

## COUNT 12

(Unauthorized Disclosure of National Defense Information)
(Detainee Assessment Briefs)

A. The general allegations of this Superseding Indictment are re-alleged and incorporated into this Count as though fully set forth herein.

B. Between in or about November 2009 and in or about May 2010, in an offense begun and committed outside of the jurisdiction of any particular state or district of the United States, the defendant, JULIAN PAUL ASSANGE, who will be first brought to the Eastern District of Virginia, and others unknown to the Grand Jury, aided, abetted, counseled, induced, procured and willfully caused Manning, who had unauthorized possession of, access to, and control over documents relating to the national defense—namely, detainee assessment briefs classified up to the **SECRET** level related to detainees who were held at Guantanamo Bay—to communicate, deliver, and transmit the documents to ASSANGE, a person not entitled to receive them.

(All in violation of Title 18, United States Code, Sections 793(e) and 2)

## COUNT 13

(Unauthorized Disclosure of National Defense Information)
(State Department Cables)

A. The general allegations of this Superseding Indictment are re-alleged and incorporated into this Count as though fully set forth herein.

B. Between in or about November 2009 and in or about May 2010, in an offense begun and committed outside of the jurisdiction of any particular state or district of the United States, the defendant, JULIAN PAUL ASSANGE, who will be first brought to the Eastern District of Virginia, and others unknown to the Grand Jury, aided, abetted, counseled, induced, procured and willfully caused Manning, who had unauthorized possession of, access to, and control over documents relating to the national defense—namely, U.S. Department of State cables classified up to the **SECRET** level—to communicate, deliver, and transmit the documents to ASSANGE, a person not entitled to receive them.

(All in violation of Title 18, United States Code, Sections 793(e) and 2)

## COUNT 14

(Unauthorized Disclosure of National Defense Information)
(Iraq Rules of Engagement Files)

A. The general allegations of this Superseding Indictment are re-alleged and incorporated into this Count as though fully set forth herein.

B. Between in or about November 2009 and in or about May 2010, in an offense begun and committed outside of the jurisdiction of any particular state or district of the United States, the defendant, JULIAN PAUL ASSANGE, who will be first brought to the Eastern District of Virginia, and others unknown to the Grand Jury, aided, abetted, counseled, induced, procured and willfully caused Manning, who had unauthorized possession of, access to, and control over documents relating to the national defense—namely, Iraq rules of engagement files classified up to the **SECRET** level—to communicate, deliver, and transmit the documents to ASSANGE, a person not entitled to receive them.

(All in violation of Title 18, United States Code, Sections 793(e) and 2)

## COUNT 15

(Unauthorized Disclosure of National Defense Information)

A. The general allegations of this Superseding Indictment are re-alleged and incorporated into this Count as though fully set forth herein.

B. From in or about July 2010 and continuing until April 2019, in an offense begun and committed outside of the jurisdiction of any particular state or district of the United States, the defendant, JULIAN PAUL ASSANGE, who will be first brought to the Eastern District of Virginia, having unauthorized possession of, access to, and control over documents relating to the national defense, willfully and unlawfully caused and attempted to cause such materials to be communicated, delivered, and transmitted to persons not entitled to receive them.

C. Specifically, as alleged above, ASSANGE, having unauthorized possession of significant activity reports, classified up to the **SECRET** level, from the Afghanistan war containing the names of individuals, who risked their safety and freedom by providing information to the United States and our allies, communicated the documents containing names of those sources to persons not authorized to receive them by distributing them and then by publishing them and causing them to be published on the Internet.

(All in violation of Title 18, United States Code, Section 793(e))

## COUNT 16

(Unauthorized Disclosure of National Defense Information)

A. The general allegations of this Superseding Indictment are re-alleged and incorporated into this Count as though fully set forth herein.

B. From in or about July 2010 and continuing until April 2019, in an offense begun and committed outside of the jurisdiction of any particular state or district of the United States, the defendant, JULIAN PAUL ASSANGE, who will be first brought to the Eastern District of Virginia, having unauthorized possession of, access to, and control over documents relating to the national defense, willfully and unlawfully caused and attempted to cause such materials to be communicated, delivered, and transmitted to persons not entitled to receive them.

C. Specifically, as alleged above, ASSANGE, having unauthorized possession of significant activity reports, classified up to the **SECRET** level, from the Iraq war containing the names of individuals, who risked their safety and freedom by providing information to the United States and our allies, communicated the documents containing names of those sources to persons not authorized to receive them by distributing them and then by publishing them and causing them to be published on the Internet.

(All in violation of Title 18, United States Code, Section 793(e))

## COUNT 17

(Unauthorized Disclosure of National Defense Information)

A. The general allegations of this Superseding Indictment are re-alleged and incorporated into this Count as though fully set forth herein.

B. From in or about July 2010 and continuing until April 2019, in an offense begun and committed outside of the jurisdiction of any particular state or district of the United States, the defendant, JULIAN PAUL ASSANGE, who will be first brought to the Eastern District of Virginia, having unauthorized possession of, access to, and control over documents relating to the national defense, willfully and unlawfully caused and attempted to cause such materials to be communicated, delivered, and transmitted to persons not entitled to receive them.

C. Specifically, as alleged above, ASSANGE, having unauthorized possession of State Department cables, classified up to the **SECRET** level, containing the names of individuals, who risked their safety and freedom by providing information to the United States and our allies, communicated the documents containing names of those sources to persons not authorized to receive them by distributing them and then by publishing them and causing them to be published on the Internet.

(All in violation of Title 18, United States Code, Section 793(e))

## COUNT 18

(Unauthorized Obtaining of National Defense Information)
(Detainee Assessment Briefs)

A. The general allegations of this Superseding Indictment are re-alleged and incorporated into this Count as though fully set forth herein.

B. Between in or about November 2009 and in or about May 2010, in an offense begun and committed outside of the jurisdiction of any particular state or district of the United States, the defendant, JULIAN PAUL ASSANGE, who will be first brought to the Eastern District of Virginia, and others unknown to the Grand Jury, knowingly and unlawfully obtained and aided, abetted, counseled, induced, procured and willfully caused Manning to obtain documents, writings, and notes connected with the national defense, for the purpose of obtaining information respecting the national defense—namely, detainee assessment briefs classified up to the **SECRET** level related to detainees who were held at Guantanamo Bay—and with reason to believe that the information was to be used to the injury of the United States or the advantage of any foreign nation.

(All in violation of Title 18, United States Code, Sections 793(b) and 2)

Notice of Forfeiture

Pursuant to Federal Rule of Criminal Procedure 32.2(a), the United States of America gives notice to the defendant, JULIAN PAUL ASSANGE, that, if convicted of any of the counts of this Second Superseding Indictment, he shall forfeit to the United States, pursuant to 18 U.S.C. §§ 793(h) and 981(a)(1)(C), 28 U.S.C. § 2461, and 21 U.S.C. § 853, any property, real or personal, which constitutes or is derived from proceeds traceable to such violation(s).

A TRUE BILL

24 JUN 2020
DATE

FOREPERSON

G. Zachary Terwilliger
United States Attorney

By:
Tracy Doherty-McCormick
First Assistant United States Attorney
Kellen S. Dwyer
Thomas W. Traxler
Gordon D. Kromberg
Alexander P. Berrang
Assistant United States Attorneys

Adam Small
Nicholas Hunter
Trial Attorneys, National Security Division
U.S. Department of Justice

No. 1:18CR111

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

**THE UNITED STATES OF AMERICA**

*vs.*

**JULIAN PAUL ASSANGE**

## SECOND SUPERSEDING INDICTMENT

**Count 1: 18 U.S.C. § 793(g) - Conspiracy To Obtain and Disclose National Defense Information**
**Count 2: 18 U.S.C. § 371- Conspiracy to Commit Computer Intrusions**
**Counts 3-4: 18 U.S.C. §§ 793(b) and 2 - Obtaining National Defense Information**
**Counts 5-8: 18 U.S.C. §§ 793(c) and 2 - Obtaining National Defense Information**
**Counts 9-11: 18 U.S.C. §§ 793(d) and 2 - Disclosure of National Defense Information**
**Counts 12-14: 18 U.S.C. §§ 793(e) and 2 - Disclosure of National Defense Information**
**Count 15-17: 18 U.S.C. § 793(e) - Disclosure of National Defense Information**

*A true bill.*

_____

_____

*Filed in open court this* 24TH ~~23rd~~ *day, of June A. D. 2020*

_____

*Clerk*

Bail, $ _____