

United States Department of Justice



Washington, D.C., June 04, 2019

To whom these presents shall come, Greeting:

That Jason E. Carter whose name is signed
to the accompanying paper, is now, and was at the time of signing the same,
Associate Director, Office of International Affairs, Criminal Division,

United States Department of Justice, Washington, D.C.

duly commissioned and qualified.

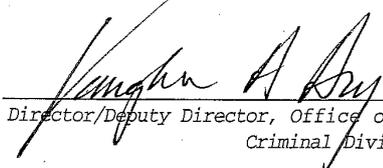
Witness, whereof, I, William P. Barr

Attorney General of the United States,
have hereunto caused the Seal of the
Department of Justice to be affixed and
my name to be attested by the Director/
Deputy Director, Office of International
Affairs, Criminal Division, of the said
Department on the day and year first
above written.



Attorney General

BY



Director/Deputy Director, Office of International Affairs,
Criminal Division

CRM-181
APR 98

CERTIFICATE

I, Jason E. Carter, Associate Director, Office of International Affairs, Criminal Division, United States Department of Justice, United States of America, do hereby certify that attached hereto is the original affidavit, with attachments, of Kellen S. Dwyer, Assistant United States Attorney for the Eastern District of Virginia, which was sworn to before Magistrate Judge Ivan D. Davis, United States District Court for the Eastern District of Virginia, on June 4, 2019, and which is offered in support of the request for extradition of Julian Paul Assange, from the United Kingdom. True copies of these documents are maintained in the official files of the U.S. Department of Justice in Washington, D.C.

4 June 2019
DATE



Jason E. Carter
Associate Director
Office of International Affairs
Criminal Division
Department of Justice
United States of America

**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**

I, Kellen S. Dwyer, being duly sworn, depose and state:

1. I am a citizen of the United States. I make this affidavit in support of the 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.

2. I received a Juris Doctor degree from Yale University in 2009. I am currently a member of the Bar of the District of Columbia, having been admitted in 2012. From 2009 to 2010, I served as a law clerk to Judge Kenneth M. Karas on the United States District Court for the Southern District of New York. From 2010 to 2011, I served as a law clerk for Judge Diarmuid F. O’Scannlain on the United States Court of Appeals for the Ninth Circuit. Since 2014, I have been employed by the U.S. Department of Justice as an Assistant United States Attorney in the Eastern District of Virginia. My duties include the prosecution of persons charged with violations of the criminal laws of the United States, including laws prohibiting computer intrusion and mishandling of national security information. Based on my training and experience, I am an expert in the criminal laws and procedures of the United States.

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 United States 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 the 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 CASE

4. These charges are the result of an FBI investigation into a conspiracy to commit computer hacking, as well as to otherwise unlawfully obtain and disclose classified information – including information that endangered human sources – by the website “WikiLeaks” and ASSANGE, its founder and leader. WikiLeaks is a website that solicits and publishes documents that have been stolen, obtained by illegal computer hacking, disclosed in violation of law, or otherwise obtained illegally. In at least one instance, ASSANGE agreed to assist a member of the U.S. Army in committing an unlawful computer intrusion in order to further their scheme to steal classified documents from the United States and publish them via WikiLeaks. In addition, ASSANGE did in fact publish classified documents that were stolen from the United States via WikiLeaks, knowing that the documents were unlawfully obtained classified documents relating to security, intelligence, defense and international relations of the United States of America, including documents containing the unredacted names of people who provided intelligence to the United States and its allies. By outing these human sources, many of whom lived in warzones or under repressive regimes, ASSANGE created a grave and imminent risk that the innocent people he named would suffer serious physical harm and/or arbitrary detention. The disclosure of these classified documents was damaging to the work of the security and intelligence services of the

United States of America; it damaged the capability of the armed forces of the United States of America to carry out their tasks; and endangered the interests of the United States of America abroad; and ASSANGE knew publishing them on the Internet would be so damaging.

SUMMARY OF THE FACTS OF THE CASE

INTRODUCTION

5. These charges relate to one of the largest compromises of classified information in the history of the United States. Between in or around January 2010 and May 2010, Chelsea Manning, then known as Bradley Manning, an intelligence analyst serving in the U.S. Army, downloaded a vast amount of classified documents. These documents included four, nearly complete and largely classified databases with 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. State Department cables. They also included Iraq war rules of engagement files. Manning provided these records to WikiLeaks, a website founded and led by ASSANGE. On its website, WikiLeaks expressly solicited classified information for public release. WikiLeaks publicly released many of these classified documents in 2010 and 2011. Many remain on the WikiLeaks website.

6. The evidence shows that ASSANGE agreed with Manning to obtain, receive, and communicate some of the classified materials discussed above—namely, Guantanamo Bay detainee assessment briefs, U.S. State Department cables, and Iraq war rules of engagement files. With regard to these sets of classified documents, ASSANGE also (1) encouraged and caused Manning to illegally obtain the documents so that Manning could provide them to ASSANGE; (2) illegally obtained and received the documents knowing that they had been and would be obtained and handled contrary to law; and (3) encouraged and caused Manning to illegally communicate, deliver, and transmit the documents to ASSANGE.

7. The evidence also shows that, in the course of the above activities, ASSANGE agreed with Manning in March 2010 to crack a password hash stored on United States Department of Defense computers connected to the Secret Internet Protocol Network, a United States government network used for classified documents and communications. At the time ASSANGE agreed with Manning to crack the password hash, Manning had already provided WikiLeaks with hundreds of thousands of downloaded classified documents, including the Afghanistan war-related significant activity reports and Iraq war-related significant activity reports. Had ASSANGE and Manning been able to crack the password hash, Manning may have been able to log onto classified computers under a username that did not belong to her, making it more difficult for investigators to identify Manning as the source of disclosures of classified information to ASSANGE and WikiLeaks. By taking steps to crack the password hash, ASSANGE was also attempting to illegally obtain and receive classified information.

8. Separate from the conduct described in the previous two paragraphs, ASSANGE also illegally communicated to the public Afghanistan war-related significant activity reports, Iraq war-related significant activity reports, and U.S. State Department cables containing names of human sources who provided information to U.S. and coalition forces and to U.S. diplomats. ASSANGE communicated these documents to the public by publishing them on the Internet via WikiLeaks, thereby creating a grave and imminent risk that the human sources he named would suffer serious physical harm and/or arbitrary detention. ASSANGE knew the disclosure of these classified documents would be damaging to the work of the security and intelligence services of the United States of America. These disclosures damaged the capability of the armed forces of the United States of America to carry out their tasks; and endangered the interests of the United States of America abroad. Manning, a U.S. citizen and member of the U.S. Army, as part of the conspiracy, attempted to gain unauthorized access to Department of Defense computers located in

the United States of America, and did transfer classified documents from those computers to persons not authorized to receive them. Further, the classified information published by ASSANGE was published in the United States of America and elsewhere through the internet and downloaded in the United States of America and elsewhere.

A. United States Law Regarding the Protection of Classified Information

9. United States 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.

10. 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.

B. ASSANGE and WikiLeaks Repeatedly Encouraged Sources with Access to Classified Information to Steal and Provide it to WikiLeaks so that WikiLeaks Could Disclose It.

11. ASSANGE is the public 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 encouraged sources to (i) circumvent legal safeguards on information; (ii) provide that protected information to WikiLeaks for public dissemination; and (iii) continue the pattern of illegally procuring and providing protected information to WikiLeaks for distribution to the public.

12. WikiLeaks's website explicitly solicited restricted materials, and until September 2010, "classified" materials. As the website then-stated, "WikiLeaks accepts *classified, censored, or otherwise restricted* material of *political, diplomatic, or ethical significance*."¹

13. ASSANGE personally and publicly promoted WikiLeaks to encourage those with access to protected information, including classified information, to provide it to WikiLeaks for public disclosure. For example, in December 2009, ASSANGE and a WikiLeaks affiliate gave a presentation at the 26th Chaos Communication Congress (26C3), described by its website as an annual conference attended by the hacker community and others that is hosted by the Chaos Computer Club (CCC), which was video recorded and posted online. In the presentation, WikiLeaks described itself as the "leading disclosure portal for classified, restricted, or legally threatened publications."

14. To further encourage the disclosure of protected information, including classified information, the WikiLeaks website posted a detailed list of "The Most Wanted Leaks of 2009," organized by country, and 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."

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

¹ All dates in this affidavit are approximate. Statements in this affidavit about information or statements that are now or once were on the WikiLeaks website are based on personal observation of that website by FBI agents investigating this matter and/or records obtained from the Internet Archive company's "Wayback Machine." The Internet Archive is a website that provides free access to a digital library of internet sites. It has partnered with and received support from various institutions, including the U.S. Library of Congress. The "Wayback Machine" is a service maintained by the Internet Archive Company, which allows users to see the content of a URL (i.e., a website address) at a time in the past, even if that content is no longer currently on the website. Evidence obtained from the Wayback machine has been deemed reliable by U.S. courts and has been admitted as evidence in U.S. criminal trials.

- a. “Bulk Databases,” including an encyclopedia used by the United States intelligence community, called “Intellipedia;” the unclassified, but non-public, Central Intelligence Agency (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.

16. The evidence gathered in the course of the investigation shows that ASSANGE intended the “Most Wanted Leaks” list to encourage and cause individuals to illegally obtain and disclose protected information, including classified information, to WikiLeaks contrary to law. For example, in 2009, ASSANGE spoke at the “Hack in the Box Security Conference” in Malaysia. In a video recording of that speech, 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. ASSANGE encouraged people to search for the list and for those with access to obtain and give to WikiLeaks information responsive to that list.

C. Chelsea Manning Responded to ASSANGE’s Solicitation and Stole Classified Documents from the United States.

17. Chelsea Manning was an intelligence analyst in the United States Army who was deployed to Forward Operating Base Hammer (FOB Hammer) in Iraq.

18. According to records from the U.S. Department of Defense (“U.S. DoD”), 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.

19. According to forensic evidence obtained from U.S. DoD computers, beginning in 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, according to forensic evidence obtained from U.S. DoD computers, Manning searched "Intelink," a classified U.S. DoD network search engine, 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.

20. On November 30, 2009, according to forensic evidence obtained from Manning's personal computer and external hard drive that was seized from her living quarters at the time of her arrest (hereinafter "Manning's personal computer"), Manning saved a text file entitled "WL-press.txt" to her external hard drive and to an encrypted container on her 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, 2009, according to forensic evidence obtained from U.S. DoD computers, 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.

21. Between in or around January 2010 and May 2010, according to forensic evidence obtained from U.S. DoD computers and Manning's own admission at her court martial, 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 activities reports, 800 Guantanamo Bay detainee assessment briefs, and 250,000 U.S. Department of State cables. According to U.S. DoD records and the markings on the documents themselves, 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.

22. On or about May 27, 2010, Manning was taken into military custody at FOB Hammer in Iraq. Manning was charged in a military court with 22 violations of the Uniform Code of Military Justice (UCMJ). These charges included aiding the enemy, in violation of UCMJ Art. 104, and sixteen violations of Title 18 of the United States Code, which is incorporated by UCMJ Art. 134, including violations of Sections 641 (theft or conversion of government property), 793 (unlawful gathering or transmission of national defense information) and 1030 (computer intrusion). On July 30, 2013, Manning was convicted of the bulk of these charges, including unlawful gathering or transmission of national defense information, computer intrusion, and theft of government property. Manning was acquitted of aiding the enemy.

23. Also on or about May 27, 2010, the U.S. Army seized Manning's personal computer from her living quarters at FOB Hammer and conducted a forensic examination pursuant to a search and seizure authorization issued by a military magistrate judge. The forensic examination of that computer revealed that Manning had been exchanging instant message

communications for months using the instant message service Jabber with a person using the Jabber account pressassociation@jabber.ccc.de. In this affidavit, I will refer to these communications as “the Jabber Communications.” For the reasons stated in Section H below, the evidence demonstrates that the person using pressassociation@jabber.ccc.de was ASSANGE. Therefore, in this affidavit, I refer to the person using pressassociation@jabber.ccc.de account as “ASSANGE.”

D. ASSANGE Encouraged Manning To Continue Her Theft of Classified Documents and Agreed To Help Her Crack a Password Hash to a Military Computer.

24. During large portions of the same time period (between November 2009, when Manning first became interested in WikiLeaks, through her arrest on or about May 27, 2010), according to the Jabber Communications and other forensic evidence obtained from Manning’s personal computer, Manning was in direct contact with ASSANGE, who encouraged Manning to steal classified documents from the United States and unlawfully disclose that information to WikiLeaks.

25. In furtherance of this scheme, according to the Jabber Communications, 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 (“SIPRNet”), a United States government network used for classified documents and communications, as designated according to Executive Order No. 13526 or its predecessor orders.

26. As background, a U.S. Army forensic expert provided the following information about how a Microsoft Windows operating system circa 2010 stored passwords. Windows did not store users’ passwords in plain text for security reasons. Instead, the computer stores passwords as “hash values.” When a user creates a password for the relevant username, the password passes through a mathematical algorithm, which creates a “hash value” for the password. Essentially, the

creation of the hash value is a form of encryption for storing the password. The hash value—not the plain text of the password—is then stored on the computer. As additional security, the computer does not store the full hash value in one location. Instead, the hash value for that username is broken into two parts. One part is stored in the Security Accounts Manager (“SAM”) database as the SAM registry file. The SAM file in a Windows operating system keeps usernames and parts of the password hash associated with the username. The other part of the password hash is stored in the “system file.” To obtain the full hash value associated with the password, one needs the parts from the SAM file and the system file. Finally, as further security, Windows locks the SAM file and system file. Only users with administrative level privileges can access the SAM and system files.

27. Manning, who had access to U.S. DoD computers in connection with her duties as an intelligence analyst, was also using the computers to download classified records to transmit to WikiLeaks, according to forensic records from U.S. DoD computers and from Manning’s admissions at her court martial. 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.

28. The Jabber Communications show that on or about March 8, 2010, after ASSANGE indicated he was “good” at “hash-cracking” and that he had a type of tool used to crack Microsoft password hashes, Manning provided ASSANGE with an alphanumeric string. A U.S. Army forensic expert subsequently examined the SIPRNet computers used by Manning and determined that the alphanumeric string that Manning sent to ASSANGE to crack was identical to a password hash stored on the SAM registry file of a SIPRNet computer used by Manning that was associated with an account that was not assigned to any specific user.

29. According to a U.S. Army forensic expert, had Manning retrieved the full password hash for that account (that is, the hash from the SAM file and the system file) and had ASSANGE and Manning successfully cracked it, Manning may have been able to log onto SIPRNet computers under a username that did not belong to her. Such a measure would have made it more difficult for investigators to identify Manning as the source of disclosures of classified information.

30. Based on forensic evidence from U.S. DoD computers and Manning's personal computer, as well as Manning's admissions at her court martial, prior to the formation of the password-cracking agreement, Manning had already provided WikiLeaks with hundreds of thousands of documents classified up to the **SECRET** level that she downloaded from departments and agencies of the United States, including the Afghanistan war-related significant activity reports and Iraq war-related significant activity reports.

31. Based on the Jabber Communications, it is clear that ASSANGE knew, understood, and fully anticipated that Manning was taking and illegally providing WikiLeaks with classified records containing national defense information of the United States that she was obtaining from classified databases, and was knowingly receiving such classified records from Manning for the purpose of publicly disclosing them on the WikiLeaks website. Such knowledge and intent is clear from the following Jabber Communications:

- a. 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 she was "throwing everything [she had] on JTF GTMO [Joint Task Force, Guantanamo] at [Assange] now." ASSANGE responded, "ok, great!"
- b. Also 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,” described above, that solicited “the complete CIA Open Source Center analytical database,” an unclassified (but non-public) database.

- c. Also on March 10, 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.” 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.” On March 10, 2010, ASSANGE told Manning that there was “a username in the GITMO docs.” Manning told ASSANGE, “any usernames should probably be filtered, period.” Manning asked ASSANGE whether there was “anything useful in there.” ASSANGE responded, in part, that “these sorts of things are always motivating to other sources too.” ASSANGE stated, “GITMO=bad, leakers=enemy of GITMO, leakers=good . . . 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.” Manning replied, “true. I’ve crossed a lot of those ‘danger’ zones, so I’m comfortable.”
- d. In addition, based on Manning’s Jabber Communications with ASSANGE and admissions Manning made at her court material, prior to her password-cracking agreement with ASSANGE, Manning used a Secure File Transfer Protocol (“SFTP”) connection to transmit the Detainee Assessment briefs to a cloud drop box operated by WikiLeaks, into a specific directory that WikiLeaks had designated for her use.

32. Accordingly, it is clear that ASSANGE entered into the password-cracking agreement with Manning for the purpose of assisting and joining Manning’s ongoing efforts to steal classified documents from U.S. government computers.

E. At ASSANGE's Direction and Agreement, Manning Continued to Steal Classified Documents and Provide Them to ASSANGE.

33. According to forensic evidence obtained from U.S. DoD computer and Manning's personal computer, as well as Manning's admissions made at her court martial, following ASSANGE's "curious eyes never run dry" comment, on or about March 22, 2010, consistent with WikiLeaks's "Most Wanted Leaks" solicitation of "Iraq and Afghanistan U.S. Army Rules of Engagement 2007-2009 (**SECRET**)," as described above, Manning downloaded multiple Iraq rules of engagement files from her SIPRNet computer and burned these files to a CD, and provided them to ASSANGE and WikiLeaks.

34. 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 "U.S. Rules of Engagement for Iraq; Refcard 2007," which was unclassified but for official use only.

35. 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 to anticipate certain actions or responses by U.S. armed forces and to carry out more effective attacks.

36. Further, according to forensic evidence obtained from U.S. DoD computer and Manning's personal computer, as well as Manning's admissions made at her court martial, following ASSANGE'S "curious eyes never run dry" comment, and consistent with WikiLeaks's solicitation of bulk databases and classified materials of diplomatic significance, as described above, between on or about March 28, 2010, and April 9, 2010, Manning used a United States

Department of Defense computer to download over 250,000 U.S. Department of State cables, which were classified up to the **SECRET** level. Manning subsequently uploaded these cables to ASSANGE and WikiLeaks through an SFTP connection to a cloud drop box operated by WikiLeaks, into a directory that WikiLeaks had designated for Manning's use. ASSANGE and WikiLeaks later disclosed those over 250,000 State Department cables to the public in unredacted form.

37. At the time that ASSANGE agreed to receive and received from Manning 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 had unlawfully obtained and disclosed or would unlawfully disclose such documents. This conclusion is based, among other evidence, not only on the fact that ASSANGE already received thousands of military-related documents classified up to the **SECRET** level from Manning, but also on the Jabber Communications which show that Manning and ASSANGE chatted about military jargon, made references suggesting that Manning was a government or military source, discussed the "releasability" of certain information by ASSANGE, discussed measures to prevent the discovery of Manning as ASSANGE's source, such as clearing logs and use of a "cryptophone;" and discussed a code phrase to use if something went wrong.

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

38. Also following Manning's arrest, during 2010 and 2011, ASSANGE published via the WikiLeaks website the documents classified up to the **SECRET** level that he had obtained from Manning, 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.

39. The significant activity reports from the Afghanistan and Iraq wars that ASSANGE published included names of local Afghans and Iraqis who had provided information to U.S. and coalition forces. The State Department cables that WikiLeaks 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. According to information provided by people with expertise in military, intelligence, and diplomatic matters, as well as individuals with expert knowledge of the political conditions and governing regimes of the countries in which some of these sources were located, by 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.

40. 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 DoD 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. The information published by ASSANGE was useful to an enemy of the United States of America.

41. The following are examples of significant activity reports related to the Afghanistan and Iraq wars that ASSANGE 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.

42. The following are examples of State Department cables that ASSANGE 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.

43. Although the charged crimes do not require the United States to prove that WikiLeaks disclosures caused actual harm to named sources, it is worth noting the following. Upon learning that WikiLeaks had possession of classified documents stolen from the United States, the United States government devoted enormous resources to identifying people who would be put at risk if and when WikiLeaks outed them as being sources for the United States. **The United States identified hundreds of at-risk and potentially at-risk people and made efforts to warn these**

people. Upon being warned, a number of these people expressed fear of retribution and were relocated from their countries with the assistance of the United States. Some people deemed at risk could not be located. Other at-risk people were not warned because the United States assessed that the act of warning might draw further attention to their relationship with the United States and thus put them in more danger. The United States is aware of sources whose unredacted names and/or other identifying information was contained in classified documents published by WikiLeaks who subsequently disappeared, although the United States cannot prove at this point that their disappearance was the result of being outed by WikiLeaks.

G. ASSANGE Knew that the Dissemination of the Names of Sources Endangered Those Individuals.

44. In a recorded interview given at the Frontline Club in London 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.” ASSANGE also knew that his publication of the State Department cables endangered sources whom he named as having provided information to the State Department. In a letter dated November 27, 2010 from the State Department’s legal adviser to ASSANGE and his counsel, 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 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 “reading through every single cable and redacting identities accordingly.” Nonetheless, while ASSANGE and WikiLeaks published some of the cables in redacted form beginning in November 2010, they published over 250,000 cables in September 2011, in unredacted form, that is, without redacting the names of the human sources.

45. 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 will know how to punish them.” When confronted about such reports in a recorded interview with *60 Minutes*, 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.”

H. Evidence that ASSANGE Used pressassociation@jabber.ccc.de To Communicate With Manning.

46. A forensic examination of Manning’s computer showed that Manning herself assigned the name “Julian Assange” to the pressassociation@jabber.ccc.de account on Manning’s “buddy list” on Adium, an instant messaging platform that can be used to communicate via Jabber. Manning told the court martial that Manning exchanged text messages with the person using this jabber account often for an hour or more, for months, on nearly a daily basis. As summarized below, Manning’s belief that Julian Assange used pressassociation@jabber.ccc.de is corroborated.

47. First, in June 2011, the FBI interviewed U.S. Person No. 1 (“US1”), a woman who met ASSANGE in December 2009 in Berlin, Germany. According to US1, ASSANGE and US1 exchanged email addresses at this time and began communicating via email and became

romantically involved. Eventually, ASSANGE and US1 began using the Jabber instant messaging service to communicate. According to US1, ASSANGE used the Jabber account pressassociation@jabber.ccc.de to communicate with US1 via Jabber. US1 said that ASSANGE used pressassociation@jabber.ccc.de until the summer of 2010 to communicate with US1.

48. Second, in August and September 2011, the FBI interviewed an Iceland person (“Iceland1”). Although Iceland1 has been convicted of criminal activity and therefore should be viewed cautiously, Iceland1 did, in fact, work extensively with ASSANGE and Wikileaks in Iceland. Iceland1 told the FBI that ASSANGE used “pressassociation” as one of his online nicknames. Iceland1 further provided the FBI with what purported to be text messages that Iceland1 exchanged with the pressassociation@jabber.ccc.de account in June 2010; those messages identify the user of pressassociation@jabber.ccc.de account as Julian Assange.

PROCEDURAL HISTORY OF THE CASE

The Charging Process

49. Under the laws of the United States, a criminal prosecution may be commenced by the filing of a criminal complaint in a United States District Court. A criminal complaint is a written statement of essential facts constituting an offense charged and is made under oath before a United States Magistrate Judge. A criminal complaint must establish that probable cause exists to believe that an offense has been committed and that the defendant named in the complaint committed it. If satisfied that the complaint sets forth a sufficient factual basis to establish probable cause, the United States Magistrate Judge orders the issuance of a warrant for the arrest of the defendant named in the complaint.

50. Under U.S. law, a criminal case may also be initiated against an individual by the filing of an Indictment. An Indictment is a formal accusation or charging document issued by a grand jury, which is a part of the judicial branch of the U.S. government. A grand jury consists of

16 to 23 citizens impaneled to review evidence of crimes presented to it by U.S. law enforcement authorities. Each member of the grand jury must review the evidence presented and determine whether there is sufficient evidence, referred to as “probable cause,” to believe that a crime has been committed and that the defendant committed the crime. If at least 12 jurors find that the evidence they have reviewed provides probable cause to believe that a particular person committed the crime, the grand jury may return an indictment. An indictment is a formal written accusation that charges the particular person, now a defendant, with a crime, identifies the specific laws that the defendant is accused of violating, and specifies the date and place where the charged crime occurred.

51. The grand jury initiates the criminal prosecution when it files the indictment with the United States District Court. Thereafter, the clerk of the court, at the direction of a United States District Judge or Magistrate Judge, normally issues a warrant for the defendant’s arrest.

52. If additional evidence is presented to a grand jury as to a defendant against whom an indictment has already been returned, the grand jury may return a superseding indictment using the same procedure as is used with an original indictment. In such instance, the superseding indictment may take the place of the previous indictment. If still more evidence is presented to a grand jury after a superseding indictment has been returned, the grand jury may return a second superseding indictment that takes the place of the earlier superseding indictment. A warrant for the defendant’s arrest may issue, but need not issue, from a superseding indictment, or second superseding indictment, by using the same procedure as is used to issue an arrest warrant on an original indictment. It is common in the United States to start a criminal case by filing a criminal complaint, then subsequently charge the same crime by way of indictment, and then later charge the same defendant with additional crimes in a superseding indictment, as occurred in this case.

The Charges and Pertinent U.S. Law

53. On December 21, 2017, a federal magistrate judge in Alexandria, Virginia, issued a criminal complaint, bearing case number 1:17-mj-611, charging ASSANGE with conspiracy, in violation of Title 18, United States Code, Section 371, which is punishable by a maximum penalty of 5 years' imprisonment. The objects of the charged conspiracy were unlawful computer intrusion, in violation of Title 18, United States Code, Section 1030(a)(1) and (2).

54. On March 6, 2018, a federal grand jury in Alexandria, Virginia returned an Indictment, bearing case number 1:18-CR-111, charging ASSANGE with conspiracy, in violation of Title 18, United States Code, Section 371, which is punishable by a maximum penalty of 5 years' imprisonment. The objects of the charged conspiracy were unlawful computer intrusion, in violation of Title 18, United States Code, Section 1030(a)(1) and (2).

55. On May 23, 2019, a federal grand jury in Alexandria, Virginia returned a Superseding Indictment, also bearing case number 1:18-CR-111, charging ASSANGE with the following crimes:

- a. Count One: Conspiracy To Obtain, Receive, and Disclose National Defense Information, in violation of Title 18, United States Code, Section 793(g), which punishable by a maximum penalty of 10 years' imprisonment;
- b. Counts Two through Four: Unauthorized Obtaining of National Defense Information, in violation of Title 18, United States Code, Section 793(b), which is punishable by a maximum penalty of 10 years' imprisonment;
- c. Counts Five through Eight: Unauthorized Obtaining and Receiving of National Defense Information, in violation of Title 18, United States Code, Section 793(c), which is punishable by a maximum penalty of 10 years' imprisonment;
- d. Counts Nine through Eleven: Unauthorized Disclosure of National Defense

Information, in violation of Title 18, United States Code, Section 793(d), which is punishable by a maximum penalty of 10 years' imprisonment;

e. Counts Twelve through Fourteen: Unauthorized Disclosure of National Defense

Information, in violation of Title 18, United States Code, Section 793(e), which is punishable by a maximum penalty of 10 years' imprisonment;

f. Counts Fifteen through Seventeen: Unauthorized Disclosure of National Defense

Information, in violation of Title 18, United States Code, Section 793(e), which is punishable by a maximum penalty of 10 years' imprisonment;

g. Count Eighteen: Conspiracy to Commit Computer Intrusion, in violation of

Title 18, United States Code, Sections 371 and 1030, which is punishable by a maximum penalty of 5 years' imprisonment.

56. It is the practice in the United States 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 United States 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 Superseding Indictment (Case No. 1:18-CR-111) and attached it to this affidavit as **Exhibit 1**.

57. On May 23, 2019, the United States Court for the Eastern District of Virginia issued an arrest warrant for ASSANGE for the offenses charged in the Superseding Indictment. It is the practice in the United States 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 **Exhibit 2**.

58. The United States requests the extradition of ASSANGE for all the offenses charged in the 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 **Exhibit 3**.

**Count 1: Conspiracy to Obtain, Receive, and Disclose
National Defense Information**

59. Count One of the Superseding Indictment charges ASSANGE with Conspiracy to Obtain, Receive, and Disclose National Defense Information, in violation of Title 18, United States Code, Section 793(g). Under United States law, a conspiracy is simply an agreement to commit one or more “substantive” criminal offenses, referred to as the purpose or objects of the conspiracy. The agreement on which the conspiracy is based need not be expressed in writing or in words, but may be simply a tacit understanding by two or more persons to do something illegal. Conspirators enter into a partnership for a criminal purpose in which each member or participant becomes a partner or agent of every other member. A person may become a member of a conspiracy without full knowledge of all of the details of the unlawful scheme or the identities of all the other members of the conspiracy. If a person has an understanding of the unlawful nature of a plan and knowingly and willfully agrees to it, joining in the plan, he is guilty of conspiracy even though he did not participate before and may play only a minor part. A conspirator can be held criminally responsible for all reasonably foreseeable actions undertaken by other conspirators in furtherance of the criminal partnership.

60. Moreover, because of this partnership, statements made by a conspirator in the course of and while he is a member of the criminal conspiracy are admissible in evidence not only against that conspirator, but also against all other members of the conspiracy. This is so because, as stated earlier, a conspirator acts as an agent or representative of the other conspirators when he is acting in furtherance of their illegal scheme. Therefore, statements of conspirators made in furtherance of the conspiracy may be deemed to be the statements of all conspirators. The crime of conspiracy is an independent offense, separate and distinct from the commission of any specific “substantive crimes.” Consequently, a conspirator can be found guilty of the crime of conspiracy to commit an offense even where the substantive crime that was the purpose of the conspiracy is not committed, or even attempted. The Congress of the United States has deemed it appropriate to make conspiracy, standing alone, a separate crime, even if the conspiracy is not successful, because collective criminal planning poses a greater threat to the public safety and welfare than individual conduct and increases the likelihood of success of a particular criminal venture.

61. In this instance, the objective of the conspiracy charged in Count 1 of the Superseding Indictment was to obtain, receive, and disclose national defense information, in violation of Title 18, United States Code, Section 793(b)-(e). The relevant sections of that statute are included in **Exhibit 3**.

62. In order to convict ASSANGE of Conspiracy To Obtain, Receive, and Disclose National Defense Information, in violation of Title 18, United States Code, Section 793(g), the United States must prove:

- a. ASSANGE entered into an agreement with one or more persons to accomplish at least one of the illegal objectives charged in the superseding indictment; here, to obtain, receive, and disclose national defense information without authorization;
- b. ASSANGE knew the unlawful purposes of this agreement;

- c. ASSANGE knowingly became a member of the conspiracy to commit at least one of the underlying offenses; and
- d. ASSANGE or another co-conspirator committed at least one overt act in furtherance of the conspiracy.

63. An overt act is any action taken to further an objective of the conspiracy. The government is not required to prove that the defendant personally did one of the overt acts. In addition, the overt act itself does not have to be unlawful, but may appear totally innocent and legal. A lawful act may be an element of a conspiracy if it was done for the purpose of carrying out the conspiracy. As detailed in the Superseding Indictment, the United States will establish that, beginning in at least 2009, ASSANGE conspired with Manning in order to unlawfully receive 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 and agreed to assist Manning in cracking a password hash stored on United States Department of Defense computers connected to SIPRNet, a United States government network used for classified documents and communications.

64. At trial, the evidence in support of Count 1 will include, but will not be limited to, the following:

- a. Forensic evidence recovered from Manning's personal and government computers, including classified information that Manning searched for and downloaded from U.S. government computers, as well as electronic messages Manning sent to and received from ASSANGE using her personal computer;

- b. Statements made by Manning under oath during her court martial, as well as electronic messages and other statements that Manning made to others in furtherance of and within the scope of the conspiracy;
- c. Testimony from former members and affiliates of WikiLeaks;
- d. Documents and other materials obtained from the WikiLeaks website, as well as evidence from Internet Archive's "Wayback Machine," which shows information that was once on the WikiLeaks website;
- e. ASSANGE's own public statements and Tweets from the official WikiLeaks account; and
- f. Testimony from individuals with knowledge and expertise in the United States military, diplomatic, and intelligence fields.

Counts 2 – 4: Unauthorized Obtaining of National Defense Information

65. Counts Two through Four of the Superseding Indictment charge ASSANGE with aiding and abetting the Unauthorized Obtaining of National Defense Information, in violation of Title 18, United States Code, Section 793(b) and 2. Title 18, United States Code, section 2, provides that a person who aids and abets or causes the commission of a crime -- in this instance the receipt of national defense information -- is as guilty as the person who actually performs the criminal act.

66. In order to convict ASSANGE of these charges, the United States must prove:

- a. Another person, namely, Manning, copied, took, made, or obtained, or attempted to copy, take, make, or obtain any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the U.S. national defense;

- b. Manning did so for the purpose of obtaining information respecting the national defense; and
- c. Manning did so with intent or reason to believe that the information was to be used to the injury of the United States or to the advantage of any foreign nation.

67. Because Counts Two through Four charge ASSANGE with aiding and abetting or causing Manning's crimes, rather than committing the crimes himself as a principal, the government must prove the following in addition to proving that Manning committed the elements of the crime as stated above:

- a. ASSANGE aided, abetted, counseled, commanded, induced or procured the commission of the offense; or
- b. ASSANGE willfully caused an act to be done which if directly performed by him or another would constitute the commission of the offense.

68. As alleged in the Superseding Indictment, the United States will establish that, between on or about November 2009 and May 27, 2010, ASSANGE 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, 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. As stated in the Superseding Indictment, the specific sets of documents that ASSANGE is charged with aiding and abetting the unlawful obtaining of are detainee assessment briefs related to detainees who were held at Guantanamo Bay classified up to the "Secret" level (Count 2), U.S. Department of State cables classified up to the "Secret" level (Count 3), and Iraq rules of engagement files classified up to the "Secret" level (Count 4).

69. At trial, the evidence in support of Counts Two through Four will include, but will not be limited to, the following:

- a. Forensic evidence recovered from Manning's personal and government computers, including classified information that Manning searched for and downloaded from U.S. government computers, as well as electronic messages Manning sent to and received from ASSANGE using her personal computer;
- b. Statements made by Manning under oath during her court martial, as well as electronic messages and other statements that Manning made to others in furtherance of and within the scope of the conspiracy;
- c. Testimony from former members and affiliates of WikiLeaks;
- d. Documents and other materials obtained from the WikiLeaks website, as well as evidence from Internet Archive's "Wayback Machine," which shows information that was once on the WikiLeaks website;
- e. ASSANGE's own public statements and Tweets from the official WikiLeaks account; and
- f. Testimony from individuals with knowledge and expertise in the United States military, diplomatic, and intelligence fields.

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

70. Counts Six through Eight of the Superseding Indictment charge ASSANGE with Unauthorized Obtaining and Receiving of National Defense Information, in violation of Title 18, United States Code, Section 793(c) and 2. In order to convict ASSANGE of these charges, the United States must prove:

- a. ASSANGE received or obtained, or agreed or attempted to receive or obtain any document, writing, code book, signal book, sketch, photograph, photographic

negative, blueprint, plan, map, model, instrument, appliance, or note, connected to the national defense;

- b. ASSANGE acted with the purpose of obtaining information respecting the national defense; and
- c. ASSANGE, at the time of receipt, knew or had reason to believe that such information was or will be obtained, taken, made, or disposed of by any person contrary to law.

71. Count 5 of the Superseding Indictment charges ASSANGE with Attempted Unauthorized Obtaining and Receiving of National Defense Information, in violation of Title 18, United States Code, Section 793(c). In order to carry its burden of proof for an attempted crime, the United States must prove beyond a reasonable doubt:

- a. ASSANGE intended to commit the crime charged, here, Unauthorized Obtaining and Receiving of National Defense Information, as defined above; and
- b. ASSANGE took a substantial step towards completion of the crime that strongly corroborates the intent.

72. As detailed in the Superseding Indictment, the government's evidence will establish that, between in or about November 2009 and May 27, 2010, ASSANGE knowingly and unlawfully received and obtained, and attempted to receive and obtain, documents, writings, and notes connected with the national defense 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 law. As stated in the Superseding Indictment, the specific sets of documents that ASSANGE is charged with knowingly receiving and obtaining are detainee assessment briefs related to detainees who were held at Guantanamo Bay classified up to the "Secret" level (Count

6); U.S. Department of State cables classified up to the “Secret” level (Count 7), and Iraq rules of engagement files classified up to the “Secret” level (Count 8). ASSANGE is also charged with attempting to obtain classified documents stored on SIPRNet (Count 5), based on his attempt to crack a SIPRNet password hash, as stated in paragraphs 24 through 32 above.

73. At trial, the evidence in support of Counts 5 through 8 will include, but will not be limited to, the following:

- a. Forensic evidence recovered from Manning’s personal and government computers, including classified information that Manning searched for and downloaded from U.S. government computers, as well as electronic messages Manning sent to and received from ASSANGE using her personal computer;
- b. Statements made by Manning under oath during her court martial, as well as electronic messages and other statements that Manning made to others in furtherance of and within the scope of the conspiracy;
- c. Testimony from former members and affiliates of WikiLeaks;
- d. Documents and other materials obtained from the WikiLeaks website, as well as evidence from Internet Archive’s “Wayback Machine,” which shows information that was once on the WikiLeaks website;
- e. ASSANGE’s own public statements and Tweets from the official WikiLeaks account; and
- f. Testimony from individuals with knowledge and expertise in the United States military, diplomatic, and intelligence fields.

**Counts 9-11: Unauthorized Disclosure of
National Defense Information**

74. Counts Nine through Eleven of the Superseding Indictment charge ASSANGE with aiding and abetting the Unauthorized Disclosure of National Defense Information, in violation of Title 18, United States Code, Sections 793(d) and 2. In order to convict ASSANGE of these charges, the United States must prove:

- a. Another person, namely, Manning, had lawful possession of, access to, control over, or was entrusted with any document relating to the national defense;
- b. Manning communicated, delivered, or transmitted (or attempted or caused to be communicated, delivered, or transmitted) the document to any person not entitled to receive it; and
- c. Manning did so willfully.

75. Because Counts Nine through Eleven charge ASSANGE with aiding and abetting or causing Manning's crimes, rather than committing the crimes himself as a principal, the government must prove the following in addition to proving that Manning committed the elements of the crime as stated above:

- a. ASSANGE aided, abetted, counseled, commanded, induced or procured the commission of the offense; or
- b. ASSANGE willfully caused an act to be done which if directly performed by him or another person would constitute the commission of the offense.

76. As detailed in the Superseding Indictment, the United States will establish that between in or about November 2009 and in or about May 2010, ASSANGE 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 (Count 9); U.S. Department of State cables classified up to the **SECRET** level (Count 10); Iraq rules of engagement files classified up to the **SECRET** level (Count 11)—to communicate, deliver, and transmit the documents to ASSANGE, a person not entitled to receive them.

77. At trial, the evidence in support of Counts 9 through 11 will include, but will not be limited to, the following:

- a. Forensic evidence recovered from Manning's personal and government computers, including classified information that Manning searched for and downloaded from U.S. government computers, as well as electronic messages Manning sent to and received from ASSANGE using her personal computer;
- b. Statements made by Manning under oath during her court martial, as well as electronic messages and other statements that Manning made to others in furtherance of and within the scope of the conspiracy;
- c. Testimony from former members and affiliates of WikiLeaks;
- d. Documents and other materials obtained from the WikiLeaks website, as well as evidence from Internet Archive's "Wayback Machine," which shows information that was once on the WikiLeaks website;
- e. ASSANGE's own public statements and Tweets from the official WikiLeaks account; and
- f. Testimony from individuals with knowledge and expertise in the United States military, diplomatic, and intelligence fields.

**Counts 12-14: Unauthorized
Disclosure of National Defense Information**

78. Counts Twelve through Fourteen of the Superseding Indictment charge ASSANGE with aiding and abetting the Unauthorized Disclosure of National Defense Information, in violation of Title 18, United States Code, Sections 793(e) and 2. In order to convict ASSANGE of these charges, the United States must prove:

- a. Another person, namely, Manning, had unauthorized possession of, access to, control over, any document relating to the national defense;
- b. Manning communicated, delivered, or transmitted (or attempted or caused to be communicated, delivered, or transmitted) the document to any person not entitled to receive it; and
- c. Manning did so willfully.
- d. Because Counts Twelve through Fourteen charge ASSANGE with aiding and abetting or causing Manning's crimes, rather than committing the crimes himself as a principal, the government must prove the following in addition to proving that Manning committed the elements of the crime as stated above:
 - e. ASSANGE aided, abetted, counseled, commanded, induced or procured the commission of the offense; or
 - f. ASSANGE willfully caused an act to be done which if directly performed by him or another would constitute the commission of the offense.

79. As detailed in the Superseding Indictment, the United States will establish that between in or about November 2009 and in or about May 2010, ASSANGE 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 (Count 12); U.S. Department of State cables classified up to the **SECRET** level (Count 13); Iraq rules of engagement files classified up to the **SECRET** level (Count 14)—to communicate, deliver, and transmit the documents to ASSANGE, a person not entitled to receive them.

80. At trial, the evidence in support of Counts Twelve through Fourteen will include, but will not be limited to, the following:

- a. Forensic evidence recovered from Manning's personal and government computers, including classified information that Manning searched for and downloaded from U.S. government computers, as well as electronic messages Manning sent to and received from ASSANGE using her personal computer;
- b. Statements made by Manning under oath during her court martial, as well as electronic messages and other statements that Manning made to others in furtherance of and within the scope of the conspiracy;
- c. Testimony from former members and affiliates of WikiLeaks
- d. Documents and other materials obtained from the WikiLeaks website, as well as evidence from Internet Archive's "Wayback Machine," which shows information that was once on the WikiLeaks website;
- e. ASSANGE's own public statements and Tweets from the official WikiLeaks account; and
- f. Testimony from individuals with knowledge and expertise in the United States military, diplomatic, and intelligence fields.

Counts 15- 17: Unauthorized Disclosure of National Defense Information

81. Counts Fifteen through Seventeen of the Superseding Indictment charge ASSANGE with Unauthorized Disclosure of National Defense Information, in violation of Title 18, United States Code, Section 793(e). In order to convict ASSANGE of these charges, the United States must prove

- a. ASSANGE, without authorization, had possession of, access to, or control over any document relating to the national defense;
- b. ASSANGE communicated, delivered, or transmitted (or attempted or caused to be communicated, delivered, or transmitted) the document to any person not entitled to receive it, or retained the above material and failed to deliver it to the officer or employee of the United States entitled to receive it; and
- c. ASSANGE did so willfully.

82. To prove Counts Fifteen and Sixteen of the Superseding Indictment, the United States will establish that in or around July 2010, ASSANGE through WikiLeaks published Afghanistan war-related significant activity reports and Iraq war-related significant activity reports that were stolen from the United States describing 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 source's 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.

83. To prove Count Seventeen of the Superseding Indictment, the United States will establish that in or around September 2011, ASSANGE through WikiLeaks published diplomatic

cables that were stolen from the U.S. Department of State. These cables, which were generally written from State department 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 United States 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 published the unredacted names of the State Department's sources, ASSANGE was aware that doing so would cause serious risk to innocent human life.

84. At trial, the evidence in support of Counts 15 through 17 will include, but will not be limited to, the following:

- a. Forensic evidence recovered from Manning's personal and government computers, including classified information that Manning searched for and downloaded from U.S. government computers, as well as electronic messages Manning sent to and received from ASSANGE using her personal computer;
- b. Statements made by Manning under oath during her court martial, as well as electronic messages and other statements that Manning made to others in furtherance of and within the scope of the conspiracy;
- c. Testimony from former members and affiliates of WikiLeaks;
- d. Documents and other materials obtained from the WikiLeaks website, as well as evidence from Internet Archive's "Wayback Machine," which shows information that was once on the WikiLeaks website;

- e. ASSANGE's own public statements and Tweets from the official WikiLeaks account; and
- f. Testimony from individuals with knowledge and expertise in the United States military, diplomatic, and intelligence fields.

Count 18: Conspiracy to Commit Computer Intrusion

85. Count Eighteen of the Superseding Indictment charges ASSANGE with conspiracy, in violation of Title 18, United States Code, Section 371. The objects of the conspiracy charged in Count Eighteen 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 any person not entitled to receive it, and willfully retain the same and fail to deliver it to the officer or employee entitled to receive it; and
- b. to intentionally access a computer, without authorization and exceeding authorized access, to obtain information from a department and agency of the United States in furtherance of a criminal act in violation of the laws of the United States, that is, a violation of Title 18, United States Code, Sections 641, 793(c), and 793(e). Title 18, United States Code, Section 641 makes it a crime to knowingly receive stolen property of the United States with intent to convert it to one's own use or gain.

86. In order to convict ASSANGE of conspiracy, in violation of Title 18 United States Code, Section 371, the United States must establish that:

- a. ASSANGE entered into an agreement with one or more persons to accomplish an illegal objective as charged in the superseding indictment; here, to commit an unlawful computer intrusion;
- b. ASSANGE knew the unlawful purposes of this agreement;
- c. ASSANGE knowingly became a member of the conspiracy to commit at least one of the underlying offenses; and
- d. ASSANGE or another co-conspirator committed at least one overt act in furtherance of the conspiracy.

87. As detailed in the Superseding Indictment, the United States will establish that in or around March 2010, ASSANGE agreed to assist Manning in cracking a password hash stored on United States Department of Defense computers connected to SIPRNet, a United States government network used for classified documents and communications. Cracking the password hash would have allowed Manning to log onto the computers under a username that did not belong to her. Such a measure would have made it more difficult for investigators to identify Manning as the source of disclosures of classified information. The evidence will show that, at the time he entered into this agreement, ASSANGE knew that Manning was providing WikiLeaks with classified records containing national defense information of the United States and that the purpose of ASSANGE's password hash-cracking agreement with Manning was to enable Manning to continue to steal classified documents from the United States to provide to ASSANGE with less risk of being detected by the United States.

88. At trial, the evidence in support of Count Eighteen will include, but will not be limited to, the following:

- a. Forensic evidence recovered from Manning's personal and government computers, including classified information that Manning searched for and downloaded from U.S. government computers, as well as electronic messages Manning sent to and received from ASSANGE using her personal computer;
- b. Statements made by Manning under oath during her court martial, as well as electronic messages and other statements that Manning made to others in furtherance of and within the scope of the conspiracy;
- c. Testimony from former members and affiliates of WikiLeaks;
- d. Documents and other materials obtained from the WikiLeaks website, as well as evidence from Internet Archive's "Wayback Machine," which shows information that was once on the WikiLeaks website;
- e. ASSANGE's own public statements and Tweets from the official WikiLeaks account;
- f. Testimony from individuals with knowledge and expertise in the United States military, diplomatic, and intelligence fields; and
- g. Testimony from individuals with knowledge and expertise in the field of computer forensics and specifically with knowledge of access controls used to protect and store login credentials for computer systems and with the tools and language used by malicious actors to gain unauthorized access to computer systems.

IDENTIFICATION INFORMATION

89. Julian Paul ASSANGE (Family name at birth, Julian Paul Hawkins) is believed to be a citizen of Australia and Ecuador, born on July 3, 1971, in Townsville, Australia. He is a white male, approximately 189 centimeters (6 feet 2 inches) tall, with white hair and blue eyes. A copy of a photograph of ASSANGE, which has been verified to be accurate by an FBI agent familiar with ASSANGE's appearance, is attached as **Exhibit 4**.

SURRENDER OF PROPERTY

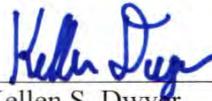
90. Pursuant to Article 16 of the Annex to the U.S.—UK Extradition Instrument, it is requested that any items relevant to the charged offenses and found in ASSANGE's possession at the time of his arrest, such as computers, cell phones, electronic memory devices, and personal papers, be delivered to the United States if he is found to be extraditable.

SUPPLEMENTING THE REQUEST

91. 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

92. This affidavit was sworn to before a United States 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.



Kellen S. Dwyer
Assistant United States Attorney
Office of the United States Attorney

Sworn and subscribed before me
this 4th day of June 2019



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

Handwritten signature in blue ink.

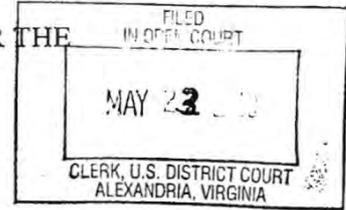


LIST OF EXHIBITS

- EXHIBIT 1:** Copy of Superseding Indictment, Case No: 1:18-CR-111, dated May 23, 2019
- EXHIBIT 2:** Copy of Arrest Warrant for JULIAN PAUL ASSANGE, dated May 23, 2019
- EXHIBIT 3:** Relevant portions of statutes cited in Superseding Indictment
- EXHIBIT 4:** Photograph of JULIAN PAUL ASSANGE

EXHIBIT 1

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 (CMH)

Count 1: 18 U.S.C. § 793(g)
Conspiracy To Receive National Defense
Information

Counts 2-4: 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

Counts 15-17: 18 U.S.C. § 793(e)
Disclosure of National Defense Information

Count 18: 18 U.S.C. §§ 371 and 1030
Conspiracy To Commit Computer Intrusion

SUPERSEDING INDICTMENT

May 2019 Term – at Alexandria, Virginia

THE GRAND JURY CHARGES THAT:

GENERAL ALLEGATIONS

At times material to this Superseding Indictment:

A. ASSANGE and WikiLeaks Repeatedly Encouraged Sources with Access to Classified Information to Steal and Provide It to WikiLeaks to Disclose.

1. JULIAN PAUL ASSANGE (“ASSANGE”) is the public 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 encouraged sources to (i) circumvent legal safeguards on information; (ii) provide that protected information to WikiLeaks for public dissemination; and (iii) continue the pattern of illegally procuring and providing protected information to WikiLeaks for distribution to the public.

2. ASSANGE and WikiLeaks have 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. WikiLeaks’s website explicitly solicited censored, otherwise restricted, and until September 2010,¹ “classified” materials. As the website then-stated, “WikiLeaks accepts *classified, censored, or otherwise restricted material of political, diplomatic, or ethical significance.*”²

3. ASSANGE personally and publicly promoted WikiLeaks to encourage those with access to protected information, including classified information, to provide it to WikiLeaks for public disclosure. For example, in December 2009, ASSANGE and a WikiLeaks affiliate gave a presentation at the 26th Chaos Communication Congress (26C3), described by the website as an annual conference attended by the hacker community and others that is hosted by the Chaos

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 was alleged to occur “on or about” that date.

² One month later, the WikiLeaks website not only deleted the term “classified” from the list of materials it would accept, but also included the following disclaimer: “WikiLeaks accepts a range of material, but we do not solicit it.”

Computer Club (CCC), which its website purports is “Europe’s largest association of hackers.” During that presentation, WikiLeaks described itself as the “leading disclosure portal for classified, restricted or legally threatened publications.”

4. To further encourage the disclosure of protected information, including classified information, the WikiLeaks website posted a detailed list of “The Most Wanted Leaks of 2009,” organized by country, and 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.”

5. 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;” 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.

6. ASSANGE intended the “Most Wanted Leaks” list to encourage and cause individuals to illegally obtain and disclose protected information, including classified information, to WikiLeaks contrary to law. For example, in 2009, ASSANGE spoke at the “Hack in the Box Security Conference” in Malaysia. 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. He encouraged people to search for the list and for those with access to obtain and give to WikiLeaks information responsive to that list.

7. ASSANGE designed WikiLeaks to focus on information, restricted from public disclosure by law, precisely because of the value of that information. Therefore, he predicated his and WikiLeaks’s success in part upon encouraging sources with access to such information to violate legal obligations and provide that information for WikiLeaks to disclose.

B. Chelsea Manning Responded to ASSANGE’S Solicitation and Stole Classified Documents from the United States.

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

9. 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.

10. 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 in paragraphs 4-5, 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.

11. On November 30, 2009, Manning saved a text file entitled “wl-press.txt” to her external hard drive and to an encrypted container on her 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, 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.

12. Between in or around 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 activities 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.

13. Manning was arrested on or about May 27, 2010. The “Most Wanted Leaks” posted on the WikiLeaks website in May 2010 no longer contained the “Military and Intelligence” category.

C. ASSANGE Encouraged Manning to Continue Her Theft of Classified Documents and Agreed to Help Her Crack a Password Hash to a Military Computer.

14. During large portions of the same time period (between November 2009, when Manning first became interested in WikiLeaks, through her arrest on or about May 27, 2010), Manning was in direct contact with ASSANGE, who encouraged Manning to steal classified documents from the United States and unlawfully disclose that information to WikiLeaks.

15. In furtherance of this scheme, 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, a United States government network used for classified documents and communications, as designated according to Executive Order No. 13526 or its predecessor orders.

16. Manning, who had access to the computers in connection with her duties as an intelligence analyst, was also 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.

17. The portion of the password hash Manning gave to ASSANGE to crack 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 portion of the password provided to ASSANGE.

18. Had Manning retrieved the full password hash and had ASSANGE and Manning successfully cracked it, Manning may have been able to log onto computers under a username that did not belong to her. Such a measure would have made it more difficult for investigators to identify Manning as the source of disclosures of classified information.

19. Prior to the formation of the password-cracking agreement, Manning had already provided WikiLeaks with hundreds of thousands of documents classified up to the **SECRET** level that she downloaded from departments and agencies of the United States, including the Afghanistan war-related significant activity reports and Iraq war-related significant activity reports.

20. At the time he entered into this agreement, ASSANGE knew, understood, and fully anticipated that Manning was taking and illegally providing WikiLeaks with classified records containing national defense information of the United States that she was obtaining from classified databases. ASSANGE was knowingly receiving such classified records from Manning for the purpose of publicly disclosing them on the WikiLeaks website.

21. For example, 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 she was “throwing everything [she had] on JTF GTMO [Joint Task Force, Guantanamo] at [Assange] now.” ASSANGE responded, “ok, great!” 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,” described in paragraphs 4-5, that solicited “the complete CIA Open Source Center analytical database,” an unclassified (but non-public) database. Manning later told ASSANGE in reference to the Guantanamo Bay detainee assessment briefs that “after this upload, thats all i really have got left.” 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.” ASSANGE intended his

statement to encourage Manning to continue her theft of classified documents from the United States and to continue the unlawful disclosure of those documents to ASSANGE and WikiLeaks.

22. Manning used a Secure File Transfer Protocol (“SFTP”) connection to transmit the Detainee Assessment briefs to a cloud drop box operated by WikiLeaks, with an X directory that WikiLeaks had designated for her use.

23. Two days later, ASSANGE told Manning that there was “a username in the gitmo docs.” Manning told ASSANGE, “any usernames should probably be filtered, period.” Manning asked ASSANGE whether there was “anything useful in there.” ASSANGE responded, in part, that “these sorts of things are always motivating to other sources too.” ASSANGE stated, “gitmo=bad, leakers=enemy of gitmo, leakers=good . . . 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.” Manning replied, “true. ive crossed a lot of those ‘danger’ zones, so im comfortable.”

D. At ASSANGE’s Direction and Agreement, Manning Continued to Steal Classified Documents and Provide Them to ASSANGE.

24. Following ASSANGE’s “curious eyes never run dry” comment, on or about March 22, 2010, consistent with WikiLeaks’s “Most Wanted Leaks” solicitation of “Iraq and Afghanistan US Army Rules of Engagement 2007-2009 (SECRET),” as described in paragraphs 4-5, Manning downloaded multiple Iraq rules of engagement files from her Secret Internet Protocol Network computer and burned these files to a CD, and provided them to ASSANGE and WikiLeaks.

25. 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.

26. 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.

27. Further, following ASSANGE’s “curious eyes never run dry” comment, and consistent with WikiLeaks’s solicitation of bulk databases and classified materials of diplomatic significance, as described in paragraphs 2, 4-5, between on or about March 28, 2010, and April 9, 2010, Manning used a United States Department of Defense computer to download over 250,000 U.S. Department of State cables, which were classified up to the **SECRET** level. Manning subsequently 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. ASSANGE and WikiLeaks later disclosed them to the public.

28. At the time ASSANGE agreed to receive and received from Manning 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 had unlawfully obtained and disclosed or would unlawfully disclose such documents. For example, not only had ASSANGE already received thousands of military-related documents classified up to the **SECRET** level from Manning, but Manning and ASSANGE also chatted about military jargon and references to current events in Iraq, which showed that Manning was a government or military source; the “releasability” of certain information by ASSANGE; measures to prevent the discovery of

Manning as ASSANGE's source, such as clearing logs and use of a "cryptophone;" and a code phrase to use if something went wrong.

E. ASSANGE, WikiLeaks Affiliates, and Manning Shared the Common Objective to Subvert Lawful Restrictions on Classified Information and to Publicly Disseminate it.

29. ASSANGE, Manning, and others shared the objective to further the mission of WikiLeaks, as an "intelligence agency of the people," to subvert lawful measures imposed by the United States government to safeguard and secure classified information, in order to disclose that information to the public and inspire others with access to do the same.

30. Manning and ASSANGE discussed this shared philosophy. For example, when Manning said, "i told you before, government/organizations cant control information ... the harder they try, the more violently the information wants to get out," ASSANGE replied, "restrict supply = value increases, yes." Further, when Manning said, "its like you're the first 'Intelligence Agency' for the general public," ASSANGE replied, that is how the original WikiLeaks had described itself.

31. Even after Manning's arrest on or about May 27, 2010, ASSANGE and others endeavored to fulfill this mission of WikiLeaks to publish the classified documents that Manning had disclosed by threatening to disclose additional information that would be even more damaging to the United States and its allies if anything should happen to WikiLeaks or ASSANGE to prevent dissemination.

32. On August 20, 2010, for instance, WikiLeaks tweeted that it had distributed an encrypted "'insurance' file" to over 100,000 people and referred to the file and the people who downloaded it as "our big guns in defeating prior restraint."

33. ASSANGE spoke about the purpose of this “insurance file,” stating that it contained information that WikiLeaks intended to publish in the future but without “harm minimization,” that is to say, without redactions of things, like names of confidential informants, that could put lives at risk. When asked how these insurance files could be used to prevent “prior restraint and other legal threats,” ASSANGE responded that WikiLeaks routinely “distributed encrypted backups of material we have yet to release. And that means all we have to do is release the password to that material and it’s instantly available. Now of course, we don’t like to do that, because there is various harm minimization procedures to go through.” But, ASSANGE continued, the insurance file is a “precaution[] to make sure that sort of material [the data in WikiLeaks’s possession] is not going to disappear from history, regardless of the sort of threats to this organization.”

34. Similarly, on August 17, 2013, WikiLeaks posted on its Facebook account: “WikiLeaks releases encrypted versions of upcoming publication data (‘insurance’) from time to time to nullify attempts at prior restraint.” The post also provided links to previous insurance files and asked readers to “please mirror” the links, meaning to post the links on other websites to help increase the number of times the files are downloaded.

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

35. Also following Manning’s arrest, during 2010 and 2011, ASSANGE published via the WikiLeaks website the documents classified up to the **SECRET** level that he had obtained from Manning, as described in paragraphs 12, 21, and 27, including approximately 75,000 Afghanistan war-related significant activity reports, 400,000 Iraq war-related significant activities reports, 800 Guantanamo Bay detainee assessment briefs, and 250,000 U.S. Department of State cables.

36. The significant activity reports from the Afghanistan and Iraq wars that ASSANGE published included names of local Afghans and Iraqis who had provided information to U.S. and coalition forces. The State Department cables that WikiLeaks 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 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.

37. 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 DoD 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.

38. Paragraphs 39 and 40 contain examples of a few of the documents ASSANGE published that contained the unredacted names of human sources. These are not the only documents that WikiLeaks published containing the names of sources, nor the only documents that put innocent people in grave danger simply because they provided information to the United States.

39. The following are examples of significant activity reports related to the Afghanistan and Iraq wars that ASSANGE 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.

40. The following are examples of State Department cables that ASSANGE 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.

G. ASSANGE Knew that the Dissemination of the Names of Individual Sources Endangered Those Individuals.

41. ASSANGE knew that his 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.

42. 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.”

43. ASSANGE also knew that his publication of the State Department cables endangered sources whom he named as having provided information to the State Department. In a letter dated November 27, 2010 from the State Department’s legal adviser to ASSANGE and his counsel, 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 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 “reading through every single cable and redacting identities accordingly.” Nonetheless, while ASSANGE and WikiLeaks published some of the cables in redacted form beginning in November 2010, they published over 250,000 cables in September 2011, in unredacted form, that is, without redacting the names of the human sources.

44. 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.”

H. United States Law to Protect Classified Information

45. 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.

46. 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, Receive, 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.

B. Between in or about November 2009 and continuing until at least September 2011, 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—namely, 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 or 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—namely, detainee assessment briefs related to detainees who were held at Guantanamo Bay, U.S. State Department cables, Iraq rules of engagement files, and information stored on the Secret Internet Protocol Network 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 are 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 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, the defendant and his conspirators committed 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, Section 793(g))

COUNT 2

(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)

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 at least the time of this Superseding Indictment, 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 all the world by publishing them 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 at least the time of this Superseding Indictment, 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 all the world by publishing them 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 at least the time of this Superseding Indictment, 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 all the world by publishing them on the Internet.

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

COUNT 18

(Conspiracy to Commit Computer Intrusion)

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

2. Beginning on or about March 2, 2010, and continuing thereafter until on or about March 10, 2010, the exact date being unknown to the Grand Jury, 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, did knowingly and unlawfully conspire with others known and unknown to the Grand Jury to commit offenses against the United States, to wit:

(A) 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 any person not entitled to receive it, and willfully retain the same and fail to deliver it to the officer or employee entitled to receive it; and

(B) to intentionally access a computer, without authorization and exceeding authorized access, to obtain information from a department and agency of the United States

in furtherance of a criminal act in violation of the laws of the United States, that is, a violation of Title 18, United States Code, Sections 641, 793(c), and 793(e).

PURPOSE AND OBJECT OF THE CONSPIRACY

The primary purpose of the conspiracy was to facilitate Manning's acquisition and transmission of classified information related to the national defense of the United States so that WikiLeaks could publicly disseminate the information on its website.

MANNERS AND MEANS OF THE CONSPIRACY

ASSANGE and his conspirators used the following ways, manners and means, among others, to carry out this purpose:

1. It was part of the conspiracy that ASSANGE and Manning used the "Jabber" online chat service to collaborate on the acquisition and dissemination of the classified records, and to enter into the agreement to crack the password hash stored on United States Department of Defense computers connected to the Secret Internet Protocol Network.
2. It was part of the conspiracy that ASSANGE and Manning took measures to conceal Manning as the source of the disclosure of classified records to WikiLeaks, including by removing usernames from the disclosed information and deleting chat logs between ASSANGE and Manning.
3. It was part of the conspiracy that ASSANGE encouraged Manning to provide information and records from departments and agencies of the United States.
4. It was part of the conspiracy that ASSANGE and Manning used a special folder on a cloud drop box of WikiLeaks to transmit classified records containing information related to the national defense of the United States.

ACTS IN FURTHERANCE OF THE CONSPIRACY

In order to further the goals and purposes of the conspiracy, ASSANGE and his conspirators committed overt acts, including, but not limited to, the following:

1. On or about March 2, 2010, Manning copied a Linux operating system to a CD, to allow Manning to access a United States Department of Defense computer file that was accessible only to users with administrative-level privileges.
2. On or about March 8, 2010, Manning provided ASSANGE with part of a password hash stored on United States Department of Defense computers connected to the Secret Internet Protocol Network.
3. On or about March 10, 2010, ASSANGE requested more information from Manning related to the password hash. ASSANGE indicated that he had been trying to crack the password hash by stating that he had "no luck so far."

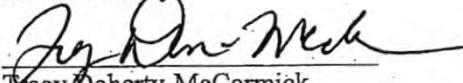
(All in violation of Title 18, United States Code, Sections 371, 1030(a)(1), 1030(a)(2), 1030(c)(2)(B)(ii).)

5/23/19
DATE

Presented to the Government Act,
A TRUE BILL
the original of this page has been filed
with the Clerk's Office.

FOREPERSON

G. Zachary Terwilliger
United States Attorney

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

Matthew Walczewski
Nicholas Hunter
Trial Attorneys, National Security Division
U.S. Department of Justice

EXHIBIT 2

UNITED STATES DISTRICT COURT

for the Eastern District of Virginia

UNDER SEAL

United States of America v. Julian Paul Assange a/k/a Julian Paul Hawkins

Case No. 1:18cr111

Defendant

RECEIVED UNITED STATES MARSHAL 2019 MAY 24 AM 10:58 EASTERN DISTRICT OF VIRGINIA ALEXANDRIA DIVISION

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay (name of person to be arrested) Julian Paul Assange a/k/a Julian Paul Hawkins who is accused of an offense or violation based on the following document filed with the court:

- Indictment, Superseding Indictment, Information, Superseding Information, Complaint, Probation Violation Petition, Supervised Release Violation Petition, Violation Notice, Order of the Court

This offense is briefly described as follows:

Obtaining and disclosing national defense information, and conspiring to do so, in violation of 18 U.S.C. §§ 793 and 2; Violating 18 U.S.C. § 371 by conspiring to (1) access a computer, without authorization and exceeding authorized access, to obtain classified national defense information in violation of 18 U.S.C. 1030(a)(1); and (2) access a computer, without authorization and exceeding authorized access, to obtain information from a department or agency of the United States in furtherance of a criminal act in violation of 18 U.S.C. § 1030(a)(2), (c)(2)(B)(ii).

Date: 5/23/19

Issuing officer's signature

City and state: Alexandria, Virginia

J. Lonham, Deputy Clerk Printed name and title

Return This warrant was received on (date) at (city and state) Date: NOTICE: BEFORE ARREST, VALIDATE THROUGH NCIC. ORIGINAL HELD BY U.S. MARSHAL. COPY ONLY COPY Arresting officer's signature Printed name and title

EXHIBIT 3

Presidential Executive Order 13,526

Sec. 1.2. Classification Levels.

(a) Information may be classified at one of the following three levels:

(1) “Top Secret” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) “Secret” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) “Confidential” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

(c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

Title 18, U.S. Code, Section 2 – Aiding and Abetting

(a) Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal.

(b) Whoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal.

Title 18, U.S. Code, Section 371 — Conspiracy against the United States

If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both.

If, however, the offense, the commission of which is the object of the conspiracy, is a misdemeanor only, the punishment for such conspiracy shall not exceed the maximum punishment provided for such misdemeanor.

Title 18, U.S. Code, Section 641 — Unlawful Receipt of Stolen Government Property

Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or

Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted—

Shall be fined under this title or imprisoned not more than ten years, or both; but if the value of such property in the aggregate, combining amounts from all the counts for which the defendant is convicted in a single case, does not exceed the sum of \$1,000, he shall be fined under this title or imprisoned not more than one year, or both.

Title 18, U.S. Code, Section 793 — Unauthorized Receipt, Retention, and Disclosure of National Defense Information

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer—

Shall be fined under this title or imprisoned not more than ten years, or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

* * *

Title 18, U.S. Code, Section 1030 — Computer Intrusion

- (a) Whoever (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; [or] (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) [1] of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); (B) information from any department or agency of the United States; or (C) information from any protected computer

* * *

shall be punished as provided in subsection (c) of this section.

* * *

- (b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.
- (c) The punishment for an offense under subsection (a) or (b) of this section is . . . (2)(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if . . . (ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

EXHIBIT 4



IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA)	
)	
v.)	Criminal No. 1:18cr111
)	
JULIAN PAUL ASSANGE,)	
)	
Defendant.)	

DECLARATION IN SUPPORT OF REQUEST
FOR EXTRADITION OF JULIAN PAUL ASSANGE

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

1. I am a citizen of the United States.
2. I am an Assistant United States Attorney in the Eastern District of Virginia, and have been so employed since 1991. I received my Bachelor's degree from Princeton University in 1979, and a Juris Doctor degree from New York University School of Law in 1982. Before joining the United States Attorney's Office, I served as a trial attorney in the United States Department of Justice, and as a defense attorney in the United States Army's Judge Advocate General's Corps.
3. My duties as an Assistant United States Attorney include the prosecution of persons charged with violations of the criminal laws of the United States, including laws prohibiting computer intrusion and mishandling of national security information. For my work as an Assistant United States Attorney, I have received various awards, including the Attorney General's Award for Excellence in Furthering the Interests of U.S. National Security, and, on three separate occasions, the FBI Director's Award for Outstanding Counterterrorism

Investigation. Based on my training and experience, I am an expert in the criminal laws and procedures of the United States.

4. 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 Paul Assange*, Case Number 1:18-CR-111, pending in the United States District Court for the Eastern District of Virginia. I make this declaration for the limited purpose of providing additional information relevant to several objections that Assange has made to the request of the United States for his extradition. The statements in this declaration are based on my experience, training, and research, as well as information provided to me by other members of the U.S. government, including members of the United States Department of Justice, the FBI, and other federal agencies.

5. This declaration does not respond to every assertion or allegation made in the defense case. I understand that a number of these can be answered by reference to matters which have already been decided as a matter of English extradition law. If I have not addressed a matter in this declaration, my failure to do so should not be regarded as an acceptance of the accuracy of such matter.

I. Assange's Challenges to the Superseding Indictment Lack Merit

A. The Charges in the Superseding Indictment
Are Based on the Evidence and Rule of Law

6. Based on the evidence and applicable law, a grand jury found probable cause to charge Julian Paul Assange for violating United States law. An independent grand jury issued these charges based on evidence of the following actions that Assange knowingly took, in committing the charged criminal offenses:

- His *complicity in illegal acts* to obtain or receive voluminous databases of classified information;
- His agreement and attempt to obtain classified information through *computer hacking*; and
- His publishing certain classified documents that 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.

7. Contrary to the claims of Cary Shenkman and others, such acts are illegal and not protected by the U.S. Constitution. There is a “well-established line of decisions holding that generally applicable laws do not offend the First Amendment simply because their enforcement against the press has incidental effects on its ability to gather and report the news.” *Cohen v. Cowles Media Co.*, 501 U.S. 663, 669 (1991). Regardless of whether one considers Assange to be a journalist, it is well-settled that journalists do not have a First Amendment right to steal or otherwise unlawfully obtain information. *See Bartnicki v. Vopper*, 532 U.S. 514, 532 n.19 (2001) (noting that the First Amendment does not protect those who “obtain[] ... information unlawfully”); *Cohen*, 501 U.S. at 669 (“The press may not with impunity break and enter an office or dwelling to gather news.”); *Branzburg v. Hayes*, 408 U.S. 665, 691 (1972) (“It would be frivolous to assert—and no one does in these cases—that the First Amendment, in the interest of securing news or otherwise, confers a license on either the reporter or his news sources to violate valid criminal laws. Although stealing documents or private wiretapping could provide newsworthy information, neither reporter nor source is immune from conviction for such conduct, whatever the impact on the flow of news.”); *Zemel v. Rusk*, 381 U.S. 1, 17 (1965) (observing that the First Amendment “right to speak and publish does not carry with it the unrestrained right to gather information,” for example, “the prohibition of unauthorized entry

into the White House diminishes the citizen's opportunities to gather information he might find relevant to his opinion of the way the country is being run, but that does not make entry into the White House a First Amendment right"). Like Assange, numerous people have been charged in the United States for conspiracy to commit computer hacking even though they engaged in that hacking purportedly to obtain newsworthy information or for political purposes. *See, e.g., United States v. Liverman*, 16-cr-313 (E.D. Va. 2016) (defendant sentenced to five years' imprisonment for conspiring to hack the email account of a former CIA director and causing the hacked materials to be distributed online, among other crimes); *United States v. Hammond*, 12-cr-185 (S.D.N.Y. 2012) (defendant sentenced to ten years' imprisonment for conspiring to hack websites related to U.S. law enforcement and U.S. cybersecurity and intelligence contractors for the stated purpose of exposing alleged corruption, among other crimes).

8. Distributing the names of individuals who provide intelligence to the United States also is not protected speech under the First Amendment. In *Haig v. Agee*, 453 U.S. 280 (1981), the United States Supreme Court considered the validity of the U.S. State Department's revocation of the passport of Phillip Agee, a former intelligence officer who engaged in a campaign to identify and disclose the identities of CIA agents operating abroad. *Id.* at 283. The U.S. Supreme Court acknowledged that the "revocation of Agee's passport rests in part on the content of his speech: specifically, his repeated disclosures of intelligence operations and names of intelligence personnel." *Id.* at 308. Still, the Supreme Court found that his speech was "clearly not protected by the Constitution." *Id.* For support, the Supreme Court quoted the well-settled principle that "[n]o one would question but that a government might prevent actual obstruction to its recruiting service or the publication of the sailing dates of transports or the number and location of troops.'" *Id.* (quoting *Near v. Minnesota*, 283 U.S. 697 (1931)). The

Supreme Court added that “[t]he mere fact that Agee is also engaged in criticism of the Government does not render his conduct beyond the reach of the law.” *Id.* at 309.

9. More recently, the U.S. Court of Appeals for the Fourth Circuit upheld the conviction of a former intelligence officer who willfully caused a reporter to publish information about an intelligence source. *See United States v. Sterling*, 860 F.3d 233 (4th Cir. 2017). Similarly, the U.S. Department of Justice’s Office of Legal Counsel, which issues authoritative opinions on constitutional questions, has twice determined to be consistent with the First Amendment proposed legislation (ultimately signed into law as the Intelligence Identities Protection Act, Title 50, United States Code, Section 3121) criminalizing, in certain circumstances, the intentional public disclosure of the names of intelligence agents and sources. These opinions were issued in 1980 and 1981 during two different Presidential administrations, from rival political parties. Although the Superseding Indictment does not charge Assange under the Intelligence Identities Protection Act, the Office of Legal Counsel opinions on that act are relevant here, because they show that the U.S. Department of Justice (along with the U.S. Congress, and Presidents of the United States of both political parties) has long viewed the intentional outing of intelligence sources as generally outside the protection of the First Amendment.

10. Assange also has alleged that the charges against him are politically motivated. Defense Summary of Issues ¶¶ 7-9. Prosecutors from the U.S. Department of Justice (i.e., federal prosecutors), however, are required to act in a manner free from political bias or motivation. This is true irrespective of any sentiments or statements made by politicians from any political party.

11. The superseding indictment here reflects no such political bias or motivation. Similar to what I understand to be *The Code for Crown Prosecutors*, the United States has publicly promulgated policies and practices to guide prosecution decisions by federal prosecutors, including whether to seek charges and what charges to seek. These so-called “Principles of Federal Prosecution” serve two important purposes. See Justice Manual, Principles of Federal Prosecution, available at <https://www.justice.gov/jm/jm-9-27000-principles-federal-prosecution> (last visited Jan. 8, 2020). The first important purpose is to ensure “the fair and effective exercise of prosecutorial discretion and responsibility.” *Id.* § 9-27.001. The second important purpose is to promote “confidence on the part of the public and individual defendants that important prosecutorial decisions will be made rationally and objectively on the merits of each case.” *Id.* § 9-27.110.

12. The Principles of Federal Prosecution set forth specific factors that federal prosecutors may *not* consider “[i]n determining whether to commence or recommend prosecution or take other action against a person.” *Id.* § 9-27.260. Among other impermissible factors, federal prosecutors are forbidden from considering a person’s “*political association, activities or beliefs*,” the prosecutor’s own personal feelings, or the possible effect on the prosecutor’s own personal or professional circumstances. *Id.*

13. My colleagues and I take these responsibilities seriously, and the superseding indictment reflects these principles. As publicly stated by a U.S. Department of Justice official in announcing the superseding indictment against Assange, “in making any prosecutorial decision, the United States looks to the principles of federal prosecution, which provide that . . . [a] determination to prosecute represents a policy judgment that the fundamental interests of society require the application of federal criminal law to a particular set of circumstances.” See

U.S. Dep't of Justice, Remarks from the Briefing Announcing the Superseding Indictment of Julian Assange, available at <https://www.justice.gov/opa/press-release/file/1165636/download> (last visited Jan. 16, 2020) (discussing that the superseding indictment is consistent with the Justice Manual, Principles of Federal Prosecution, § 9-27.001).

14. My colleagues and I presented these charges and the evidence that supports them to a federal grand jury, which found probable cause to proceed: at least 16 grand jurors must have been present for the vote and at least 12 must have voted in favor.

15. In the United States, the grand jury, composed of independent citizens, is an essential component required in the enforcement of its federal criminal laws. The federal version, enshrined in the Fifth Amendment to the U.S. Constitution, has its origins in English common law and statutes. “There is every reason to believe that our constitutional grand jury was intended to operate substantially like its English progenitor. The basic purpose of the English grand jury was to provide a fair method for instituting criminal proceedings against persons believed to have committed crimes.” *Costello v. United States*, 350 U.S. 359, 362 (1956).

16. The grand jury serves ““as a means, not only of bringing to trial persons accused of public offences upon just grounds, but also as a means of protecting the citizen against unfounded accusation, whether it comes from government, or be prompted by partisan passion or private enmity.”” *United States v. Dionisio*, 410 U.S. 1, 17 n.15 (1973) (quoting *Ex Parte Bain*, 121 U.S. 1, 11 (1887), *overruled on other grounds by United States v. Cotton*, 535 U.S. 625 (2002)). Like federal prosecutors, grand jurors are bound to examine evidence objectively, and they take an oath to that effect, one that “binds them to inquire diligently and objectively into all federal crimes committed within the district about which they have or may obtain evidence, and

to conduct such inquiry without malice, fear, ill will, or other emotion.” Administrative Office of the United States Courts, Handbook for Federal Grand Jurors 7 (2012), <https://www.uscourts.gov/sites/default/files/grand-handbook.pdf>.

17. In short, the superseding indictment is based on the evidence and the rule of law, not Assange’s political opinions. If Assange wishes to challenge this, he may do so in the United States, as further discussed below, by asking an independent court to dismiss the superseding indictment because of selective prosecution.¹

18. Assange also has alleged that the superseding indictment is part of some “escalating public ‘war’” against journalists or publishers. Defense Summary of Issues ¶ 8. Indeed, Assange asserts that “[a]ll charges seek to criminalise the act of publishing leaked information.” Defense Summary of Issues ¶ 6. He further asserts that “criminalisation of journalistic activities,” such as “the public interest in publication” of the “collateral murder video,” and “conditions in Guantanamo Bay,” “strikes at the very essence of Article 10” of the European Convention on Human Rights. Defense Summary of Issues ¶ 13. The grand jury, however, did not charge Assange for passively obtaining or receiving classified information; neither did it charge him for publishing in bulk hundreds of thousands of these stolen classified documents.

19. Rather, the charges against Assange focus on his complicity in Manning’s theft and unlawful disclosure of national defense information (Counts 1-4, 9-14), his knowing and

¹ Assange would need to proceed with any such motion under the U.S. Constitution instead of the Principles of Federal Prosecution because those principles, and internal office procedures adopted pursuant to them, are intended solely for the guidance of attorneys for the government. They are not intended to create a substantive or procedural right or benefit, enforceable at law, and may not be relied upon by a party to litigation with the United States. *See* Principles of Federal Prosecution, *supra*, § 9-27.150.

intentional receipt of national defense information from Manning (Counts 6-8), his agreement with Manning to engage in a conspiracy to commit computer hacking, and his attempt to crack a password hash to a classified U.S. Department of Defendant account (Counts 5 and 18).

20. The only instances in which the superseding indictment charges Assange with the distribution of national security information to the public are explicitly limited to his distribution of “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 the public.” Superseding Indictment, Count 1, ¶B(4); *see also id.*, Count 15 ¶C (“Specifically, . . . 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 all the world by publishing them on the Internet.”); *id.*, Count 16 ¶C (“Specifically, . . . 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 all the world by publishing them on the Internet.”); *id.* Count 17 ¶C (“Specifically, . . . 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 all the world by publishing them on the Internet.”).

21. In short, Assange was charged for publishing specified classified documents that contained the *un-redacted names of innocent people* who risked their safety and freedom to provide information to the United States and its allies. He was not, for example, charged for publishing the so-called “Collateral Murder” video that WikiLeaks disclosed in April 2010; in addition, none of the charges alleges that Assange violated the law by obtaining and releasing that video, and the superseding indictment does not even mention it.

22. As publicly stated by another Department of Justice official in announcing the superseding indictment, “[t]he Department takes seriously the role of journalists in our democracy . . . and it is not and has never been the Department’s policy to target them for their reporting. Julian Assange is no journalist. This [is] made plain by the totality of his conduct as alleged in the indictment – i.e., his conspiring with and assisting a security clearance holder to acquire classified information, and his publishing the names of human sources. Indeed, no responsible actor – journalist or otherwise – would purposely publish the names of individuals he or she knew to be confidential human sources in war zones, exposing them to the gravest of danger.” See U.S. Dep’t of Justice, Remarks from the Briefing Announcing the Superseding Indictment of Julian Assange, *available at* <https://www.justice.gov/opa/press-release/file/1165636/download> (last visited Jan. 16, 2020). As summarized in the next section, Assange placed these individuals in grave danger.

23. Assange also has suggested that the addition of a number of new charges against him in the Superseding Indictment somehow reflects an increased bias against him. That suggestion is based on a misunderstanding of both the practice and policy of federal prosecutions in the United States. First, it is quite common for a case to be initially charged with a single crime, and then followed by one or more superseding indictments that add charges or defendants.

This regular practice permits a case to be initiated with limited evidence, while the investigation of more complex charges can be more fully investigated. In some cases involving national security issues, declassification of necessary evidence can be a time-consuming and complex process which prohibits all charges from being brought at the very outset of the case. Likewise, once a defendant is charged, additional witnesses may be located or come forward, which permits additional charges to be brought.

24. Moreover, the Principles of Federal Prosecution also call for prosecutors to “charge and pursue the most serious, readily provable offenses.” Justice Manual at 9-27.300. As additional evidence is gathered and declassified, the Principles counsel the addition of “readily provable offenses.” While the United States will not waive its deliberative process privilege to discuss the specific decision-making process in this case, I note that there are many reasons for adding charges in a superseding indictment which are consistent with the exercise of independent prosecutorial decision-making in line with the Principles of Federal Prosecution.

B. Many Individuals Outed By Assange Were Placed
Placed at Grave Risk and Suffered Grave Harm

25. The significant activity reports from the Afghanistan and Iraq wars that WikiLeaks published included the names of local Afghans and Iraqis who had provided information to U.S. and coalition forces. The State Department cables that WikiLeaks published included the 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 living in repressive regimes, who, at great risk to their own safety, reported to the United States the political conditions within their own countries and abuses of their own governments.

26. Based on information provided by people with expertise in military, intelligence, and diplomatic matters, as well as individuals with expert knowledge of the political conditions and governing regimes of the countries in which some of these sources were located, I know that, by 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.

1. The United States Identified And Attempted to Notify
Hundreds of People Whom Assange Endangered

27. After WikiLeaks published the Afghanistan significant activity reports on or about July 25, 2010, the U.S. Department of Defense ("DoD") established an "Information Review Task Force," commonly known as the "IRTF." The purpose of the IRTF was to conduct a DoD review of the classified records published by WikiLeaks, as well as classified records obtained but not yet published by WikiLeaks. Among other things, the IRTF was tasked with reviewing the records to understand the risks that the disclosure of the records posed to sources named within them. Over the course of its review, the IRTF identified hundreds of Afghans and Iraqis whom it assessed were potentially endangered by the publication of the significant activity reports in unredacted form.

28. Similarly, upon learning of the compromise of the diplomatic cables described in paragraph 25, the U.S. Department of State established a "WikiLeaks Persons at Risk Task Force," which identified hundreds more individuals who could be endangered if the cables were published or otherwise disclosed to the governments and/or nonstate actors in the countries where the individuals resided. The State Department defined "Persons at Risk" as those facing "death, violence, or incarceration."

29. Both the U.S. Department of Defense and the U.S. Department of State engaged in extensive efforts to notify sources who were put at risk by the WikiLeaks disclosures. Not all sources, however, could be notified. Some people deemed at risk could not be located. Other at-risk people were not warned because the United States assessed that the act of warning might draw further attention to their relationship with the United States and, thus, put them in more danger. Still other at-risk people were not notified because military officials determined that an attempt to notify them could present an unacceptable risk of harm to U.S. forces in carrying out the notification.

2. Individuals Named in Wikileaks Cables Have Been Harassed, Investigated, Surveilled, Arrested, Disappeared, and/or Forced to Flee Their Homelands

30. The State Department determined that well over 100 people were placed at risk from the disclosures. In turn, approximately 50 people sought and received assistance from the United States. For some of these individuals, the United States assessed that it was necessary and advisable for them to flee their home countries. The United States assisted in moving some of these individuals to the United States or to safe third countries. In some instances, the United States also assisted in moving the spouses and/or families of these individuals to the United States or to third countries.

31. All of the individuals who had to flee their homelands because they were identified by WikiLeaks in State Department cables suffered actual harm attributable to Assange. Some of these harms are quantifiable, such as losing employment or having assets frozen by the autocratic regimes from which they fled. Other harms suffered by sources forced to flee are not easily quantifiable, but are, nonetheless, very real.

32. The United States also is aware of individuals whose unredacted names and/or other identifying information were contained in classified documents published by WikiLeaks,

and who subsequently disappeared, although the United States cannot prove at this point that their disappearance was the result of being outed by WikiLeaks.

33. The United States also is aware of individuals who were investigated and/or arrested because they were named in the State Department cables published by WikiLeaks. For example, according to the Committee To Protect Journalists and media reports, an Ethiopian journalist was forced to flee Ethiopia after he was interrogated and threatened by Ethiopian authorities regarding the contents of a cable published by WikiLeaks. According to the WikiLeaks cable, the Ethiopian journalist had told U.S. diplomats in 2009 that an Ethiopian government source had told him of a plot to arrest the editors of an Ethiopian publication that had been critical of the government. According to information the journalist reportedly told the Committee to Protect Journalists and the BBC, Ethiopian police interrogated him after WikiLeaks published this cable, and threatened to jail him if he did not reveal his government source; rather than reveal his source or risk prison, the journalist reportedly fled his country.

34. The United States also is aware of at least one instance where an individual named in the State Department cables released by WikiLeaks was subsequently arrested and detained. In that case, a news organization close to the arresting regime openly stated that the arrest was based, at least in part, on information revealed by WikiLeaks showing the arrested individual's relationship with the State Department.

35. People named by WikiLeaks as having provided information to the State Department also reportedly faced threats and harassment by non-state actors. According to Canada's *Globe and Mail*, "[s]ome of China's top academics and human rights activists are being attacked as 'rats' and 'spies' after their names were revealed as U.S. Embassy sources in the unredacted WikiLeaks cables that have now been posted online." Mark MacKinnon, *Leaked*

Cables Spark Witch-Hunt for Chinese 'Rats,' *Globe and Mail* (Sept. 14, 2011),

[https://www.theglobeandmail.com/news/world/leaked-cables-spark-witch-hunt-for-chinese-](https://www.theglobeandmail.com/news/world/leaked-cables-spark-witch-hunt-for-chinese-rats/article594194/)

[rats/article594194/](https://www.theglobeandmail.com/news/world/leaked-cables-spark-witch-hunt-for-chinese-rats/article594194/). The *Globe and Mail* further reported that WikiLeaks' "release of the

previously protected names has sparked an online witch-hunt by Chinese nationalist groups, with

some advocating violence against those now known to have met with U.S. Embassy staff. "When

the time comes, they should be arrested and killed," reads one typical posting on a prominent

neo-Maoist website." *Id.* One Chinese national who was named in the WikiLeaks cables and

consequently fled to the United States reported experiencing harassment from non-state actors.

3. Hostile Foreign Governments, Terrorist Groups, and Criminal Organizations Have Exploited Wikileaks Disclosures in Order to Gain Actionable Intelligence

36. Hostile foreign governments, terrorist groups, and criminal organizations have exploited WikiLeaks disclosures in order to gain intelligence to be used against the United States and to be used against foreign nationals who provided assistance to the United States. For example, 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 (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 DoD material posted to WikiLeaks, (2) a letter from that same member of al-Qaeda to Bin Laden with information from the Afghanistan War Documents released by WikiLeaks, and (3) Department of State information released by WikiLeaks.

37. 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 will know how to punish them.”

38. In addition, the Department of Justice and the FBI have conducted interviews with several experts on Syria, Iran, and China. These experts uniformly reported that foreign intelligence services would have read the WikiLeaks cables to gain actionable intelligence.

4. Assange Endangered Afghans and Iraqis Who Provided Information to U.S. and Coalition Forces

39. The U.S. Department of Defense identified hundreds of Iraqis and Afghans whose lives and freedom were endangered by Assange’s publication of the unredacted significant activity reports discussed above. The Superseding Indictment describes a sample of these significant activity reports as follows:

- 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 DI was a 2009 report discussing an improvised explosive device (IED) attack in Iraq. Classified Document DI named local human sources who provided information on the attack. Classified Document DI was classified at the SECRET level; and
- 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.

40. Assange placed in extreme danger the above-referenced individuals, along with many other Iraqis and Afghans whom Assange named as having provided information to U.S. and coalition forces. According to experts with the U.S. Department of Defense, in and around 2010, the Taliban in Afghanistan and the insurgency in Iraq were known to take brutal measures against Iraqis and Afghans whom they believed (rightly or wrongly) to have collaborated with U.S. and coalition forces.

41. According to the State Department's 2010 Human Rights Report on Afghanistan, the Taliban continued its "politically-targeted killings" in 2010 and killed numerous Afghan civilians. On July 18, 2010, "Taliban leader Mullah Omar issued new rules of engagement, calling on Taliban commanders to capture or kill civilians working for foreign forces or the government." In addition, "[t]he media reported that the Taliban issued 'night letters' threatening anyone who made peace with the government, a charge Taliban spokesmen denied," and "[t]here were numerous reports of summary justice by the Taliban resulting in extrajudicial executions." Moreover, "Media reports and firsthand accounts accused the Taliban of employing torture in interrogations of persons they accused of supporting coalition forces and the central government. The Taliban contacted newspapers and television stations in several such cases to claim responsibility." And "[i]n areas not under government control, the Taliban enforced a parallel judicial system. The Taliban issued punishments including beatings, cutting off fingers, beheadings, hangings, and stonings. On March 9 [2010], the Taliban killed a man for allegedly spying." <https://2009-2017.state.gov/documents/organization/160445.pdf>.

42. Moreover, as noted above, the Taliban openly stated in July 2010 that it was reviewing the WikiLeaks publications in order to identify "spies" whom they could "punish."

43. According to the State Department's 2010 Human Rights Report on Iraq, "[v]iolence against the civilian population perpetrated by terrorist groups remained a problem during [2010], and bombings, executions, and killings were regular occurrences throughout all regions and sectors of society." In particular, in 2010 Iraq saw "an increase in AQI [al-Qaida in Iraq] attacks against Sunnis cooperating with the government." For example, "[o]n April 20, [2010], gunmen killed five family members, beheading three, of the local anti-AQI militia in Tarmiyah." Similarly, "[o]n July 18, [2010], a suicide bomber killed at least 45 anti-al Qaida Sunni fighters waiting for their paychecks."

5. Assange Endangered Many Iranians By Outing Them As Having Provided Information to the United States

44. The State Department's persons-at-risk task force identified many individuals in Iran whose lives and freedom were endangered by Assange's publication of the unredacted State Department cables described above. The Superseding Indictment describes two such cables as follows:

- 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; and
- 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.

45. Assange placed in extreme danger the above-referenced individuals, along with many other people located in Iran or who regularly travel to Iran, whom Assange named as having provided information to U.S. diplomats. According to State Department personnel with expertise in Iran, the Iranian regime in 2011 and continuing to the present, is repressive. Iranians who spoke to the United States without authorization faced reprisal.

46. According to the State Department's 2011 Human Rights Report on Iran, "the government increased its oppression of media and the arts, arresting and imprisoning dozens of journalists, bloggers, poets, actors, filmmakers, and artists throughout [2011]." This "suppression and intimidation of voices of opposition continued at a rapid pace at year's end. The most egregious human rights problems were the government's severe limitations on citizens' right to peacefully change their government through free and fair elections, restrictions on civil liberties, and disregard for the sanctity of life through the government's use of arbitrary detention, torture, and deprivation of life without due process." In particular, "[s]ecurity forces under the government's control committed acts of politically motivated violence and repression, including torture, beatings, and rape. The government administered severe officially sanctioned punishments, including amputation and flogging. Security forces arbitrarily arrested and detained individuals, often holding them incommunicado."

47. The State Department further noted that "[t]he UN special rapporteur for human rights in Iran noted in his October [2011] report that at least 83 persons, including three political prisoners, were known to have been executed in January alone." In addition, "[h]uman rights activists reported that the government executed an average of two persons a day during the first six months of [2011]" and "exiles and human rights monitors alleged that many persons supposedly executed for criminal offenses such as narcotics trafficking were actually political dissidents." Iranian "law criminalizes dissent and also applies the death penalty to offenses such as 'attempts against the security of the state,' 'outrage against high-ranking officials,' 'enmity towards god,' and 'insults against the memory of Imam Khomeini and against the supreme leader of the Islamic Republic.'"

48. The State Department further reported that in 2011 “[a]rbitrary arrest was a common practice [in Iran] and was used by authorities to spread fear and deter activities deemed against the regime.” The State Department relied on a study from International Campaign for Human Rights in Iran (ICHR), which concluded that “an estimated 500 persons were arbitrarily detained [in Iran in 2011] for peaceful activities or the exercise of free expression, and another 500 prisoners of conscience had been sentenced to lengthy prison terms following unfair trials.” The State Department Human rights report further noted that detainees in Iran face a high risk of physical violence and abuse while incarcerated.

6. Assange Endangered Many Chinese Nationals by Outing Them as Having Provided Information to the United States

49. The State Department’s persons-at-risk task force identified many individuals in China whose lives and freedom were endangered by Assange’s publication of the unredacted State Department cables. The Superseding Indictment describes one of those cables as follows:

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.

50. Assange placed in extreme danger the above-referenced individual, along with many other people in China whom Assange named as having provided information to U.S. diplomats. According to State Department personnel with expertise in China, the Chinese regime in 2011 and continuing to the present, is repressive. In addition, the Chinese intelligence services are vast, well-resourced, and focused on internal dissent, especially dissent from ethnic and religious minorities in the western provinces. Chinese nationals who spoke to the United States without authorization faced reprisal.

51. According to the State Department's 2011 Human Rights report on China, 2011 saw confirmed “[d]eterioration in key aspects of the country’s human rights situation” where “[r]epression and coercion, particularly against organizations and individuals involved in rights advocacy and public interest issues, were routine.” “Efforts to silence political activists and public interest lawyers were stepped up, and, increasingly, authorities resorted to extralegal measures including enforced disappearance, ‘soft detention,’ and strict house arrest, including house arrest of family members, to prevent the public voicing of independent opinions.” Moreover, “[t]he authorities continued severe cultural and religious repression of ethnic minorities in Xinjiang Uighur Autonomous Region (XUAR) and Tibetan areas.” The country also saw “extrajudicial killings, including executions without due process; enforced disappearance and incommunicado detention, including prolonged illegal detentions at unofficial holding facilities known as ‘black jails’; torture and coerced confessions of prisoners; detention and harassment of lawyers, journalists, writers, [and] dissidents.” In particular, the 2011 State Department Human Rights Report on China specified that “[d]uring the year security forces reportedly committed arbitrary or unlawful killings.”

52. The State Department further reported that as of 2011, “[t]ens of thousands of political prisoners remained incarcerated [in China], some in prisons and others in RTL [Reeducation Through Labor] camps or administrative detention” and that in 2011 “[a]uthorities arrested persons on allegations of revealing state secrets, subversion, and other crimes as a means to suppress political dissent and public advocacy.” NGOs estimated that in China in 2011 alone “approximately 50 human rights activists and lawyers were formally arrested or placed under extralegal detention, up to 200 people were placed under house arrest, and 15 were charged with ‘inciting subversion of state power.’” The Committee to Protect Journalists reported in 2011 that

there were at least “27 known journalists imprisoned in [China], 10 were Tibetan and six were Uighur.” Moreover, “[t]here were widespread reports of activists and petitioners being committed to mental health facilities and involuntarily subjected to psychiatric treatment for political reasons.”

53. The State Department reported that religious and ethnic minority were particularly vulnerable in China. In 2011, “[t]he government continued to repress Uighurs expressing peaceful political dissent and independent Muslim religious leaders” and “Uighurs continued to be sentenced to long prison terms, and in some cases executed without due process, on charges of separatism and endangering state security.”

54. The 2011 State Department Human Rights Report on China further noted that detained political prisoners were at increased risk of violence: “Although ordinary prisoners were subjects of abuse, political and religious dissidents were singled out for particularly harsh treatment. In some instances close relatives of dissidents were singled out for abuse” and “[c]onditions in penal institutions for both political prisoners and criminal offenders were generally harsh and often degrading.” Indeed, “[b]eating deaths occurred in administrative detention and RTL facilities” and “[d]etainees reported beatings, sexual assaults, lack of proper food, and no access to medical care.”

7. Assange Endangered Many Syrians by Outing Them as Having Provided Information to the United States

55. The State Department’s persons-at-risk task force identified many individuals in Syria whose lives and freedom were endangered by Assange’s publication of the unredacted State Department cables described above. The Superseding Indictment describes two such cables as follows:

- a. 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; and
- b. 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.

56. Assange placed in extreme danger the above-referenced individuals, along with the other Syrians whom Assange named as having provided information to U.S. diplomats. According to State Department diplomats with expertise in Syria, the Syrian regime in 2011 and continuing to the present, is repressive. Syrians who spoke to the United States without authorization faced reprisal.

57. According to the State Department's 2011 human rights report on Syria, the regime used "massive attacks and strategic use of citizen killings as a means of intimidation and control" over the population. Indeed, in 2011 alone, "there were thousands of reports of arbitrary or unlawful deprivation of life, many as a result of government actions against peaceful prodemocracy protesters." "The vast majority of disappearances reported by activists, human rights observers, and international NGOs appeared to be politically motivated" as "[t]he regime targeted critics and antigovernment protesters."

58. Those detained in Syria remained in serious physical risk as "[t]he government also reportedly tortured detainees to death." In particular, "[a]n August 31 [2011] Amnesty International (AI) report detailed extrajudicial killings in detention facilities," and "not[ed] at least 88 deaths were reported to AI between April 1 and 15 and that there was evidence that torture caused or contributed to death in at least 52 cases." In sum, the State Department's 2011 Human Rights Report for Syria concluded that "[h]arsh and life-threatening prison conditions

were common, especially after arrests stemming from the protests caused a substantial increase in the prison and detention center population.”

59. The State Department 2011 Human Rights Report on Syria further concluded that, “[o]ther serious problems included disappearances; torture and abuse; poor prison and detention center conditions; arbitrary arrest and detention; denial of fair public trial; arbitrary interference with privacy; and lack of press, Internet, and academic freedom.” And, “[a]s in previous years, government forces [in 2011] detained, arrested, and harassed journalists and other writers for works deemed critical of the state.”

8. Assange Endangered Foreign Police and Military Who Received Counter-Narcotics and Counter-Terrorism Training from the United States

60. The State Department cables that Assange published in unredacted form contained hundreds of “Leahy Vetting Requests.” The term “Leahy law” refers to two U.S. statutory provisions prohibiting the U.S. Government from using funds for assistance to units of foreign security forces where there is credible information implicating that unit in the commission of gross violations of human rights. One statutory provision applies to the State Department and the other applies to the Department of Defense. The State Department Leahy law was made permanent under section 620M of the Foreign Assistance Act of 1961, 22 U.S.C. § 2378d, *see* <https://www.state.gov/leahy-fact-sheet/>.

61. In cases where an entire unit is designated to receive assistance, the State Department vets the unit and the unit’s commander. When an individual security force member is nominated for U.S. assistance, the State Department vets that individual as well as that individual’s unit. Vetting begins in the unit’s home country, where the U.S. embassy conducts consular, political, and other security and human rights checks. Frequently, an additional review is conducted by analysts at the State Department in Washington, D.C. The State Department

evaluates and assesses available information about the human rights records of the unit and the individual, reviewing a full spectrum of open source and classified records. *See* <https://www.state.gov/leahy-fact-sheet/>.

62. As part of the Leahy vetting process, the embassies frequently send cables called “Leahy Vetting Request” to the State Department in Washington, D.C. WikiLeaks published many of these “Leahy Vetting Requests” without redaction. Often, these requests were less than a page and simply provided the full name and personal identifying information of the person being vetted, including date of birth; gender; military identification number, if applicable; place of birth; position; and organization. The cables would then note something to the effect that “Post possesses no credible evidence of gross violations of human rights by the individuals listed below and requests that the department conduct Leahy vetting check.”

63. By publishing the names and personal identifying information of particular individuals who received counter-terrorism and/or counter-narcotics training from the United States, Assange put those individuals at grave risk.

64. Indeed, based on information provided to the United States government, the United States assessed that violent non-state groups have attempted to use WikiLeaks disclosures to identify and target military and/or police in their country who were engaged in counter-terrorism and/or counter-narcotics operations.

9. Assange’s Disclosures Caused Harm to the State Department’s Ability To Report On Human Rights Abuses

65. At the Manning court martial, Ambassador Michael Kozak, who led the State Department’s WikiLeaks Person at Risk Task Force, testified that the WikiLeaks disclosures had caused, and would continue to cause, a chilling effect on dissidents and human rights activists around the world, making them afraid to report human rights abuses to U.S. embassies.

Ambassador Kozak reported that WikiLeaks caused incredible harm to “the credibility of the United States.” He described U.S. diplomats seeking to report on human rights abuses as “in the same position as newspaper reporters” in that “if you go out and reveal all your sources every time, not too many people will talk to you.” Ambassador Kozak further testified that the WikiLeaks disclosures have “meant that some people, some activists in a democracy and human rights field ... are no longer active. So that’s had an obvious effect on those particular countries where those individuals came from, that you just lost some leaders in that field.” Ambassador Kozak added that some human rights activists living under repressive regimes have told him personally that WikiLeaks has made them “nervous” about reporting human rights abuses to the U.S. embassy in the future. Other State Department personnel similarly reported that the WikiLeaks disclosures caused a reduced willingness of dissidents and human rights activists in repressive regimes to report abuses and other valuable information to the United States.

C. If Assange is Extradited, He Can Challenge the Superseding Indictment Before Independent Federal Judges and a Jury

66. The United States established three equal and independent branches of government to provide a system of checks and balances against unjust decision-making. In the United States, federal judges (the judicial branch) are nominated by the president (the executive branch) and confirmed by the Senate (the legislative branch). The Constitution guarantees that federal judges who have been nominated by the president and confirmed by the Senate “shall hold their offices during good behavior.” U.S. Const. Art. III, Sec. 1. In practice, this guarantee provides federal judges with life-tenure, and insulates them from political interference. *See* Federalist Paper, No. 78 (A. Hamilton) (“The standard of good behavior for the continuance in office of the judicial magistracy, is certainly one of the most valuable of the modern improvements in the practice of government. In a monarchy it is an excellent barrier to the

despotism of the prince; in a republic it is a no less excellent barrier to the encroachments and oppressions of the representative body. And it is the best expedient which can be devised in any government, to secure a steady, upright, and impartial administration of the laws.”). Indeed, courts in the United States have a long history of independent and impartial decision-making, dating back to the Supreme Court’s decision in *Marbury v. Madison* in 1803.

67. If Assange is extradited, he will have an opportunity to challenge the charges in the superseding indictment. Any such challenge would be decided by independent federal judges – first at the trial level, and then upon appeal. Assange would have one appeal as of right, and other discretionary appeals up to the United States Supreme Court. *See* Title 28, United States Code, Section 1291; U.S. Supreme Court Rule 10.

68. For example, Assange could file a pre-trial motion to challenge the superseding indictment on the basis of selective prosecution. To succeed on such a motion, Assange would have to demonstrate that “the prosecution had a discriminatory effect and that it was motivated by a discriminatory purpose.” *Wayte v. United States*, 470 U.S. 598, 608 (1985). Meeting this heavy burden requires the defendant to establish both (1) that “he has been singled out while others similarly situated have not been prosecuted; and (2) that the decision to prosecute was invidious or in bad faith, *i.e.*, based upon such impermissible considerations as race, religion, or the desire to exercise his constitutional rights.” *United States v. Greenwood*, 796 F.2d 49, 52 (4th Cir. 1986).

69. Assange also would have the opportunity to challenge the superseding indictment on the basis that his conduct was protected by the free speech provisions of the First Amendment to the U.S Constitution. Similarly, to the extent Assange believes that Title 18, United States Code, Sections 793 or 1030 is unconstitutionally vague, as the Shenkman Affidavit appears to

assert, *see* Shenkman Aff. ¶¶ 29, 35, 41, he could challenge those laws and their application to him as “void-for-vagueness” under the Fifth Amendment to the U.S. Constitution. A statute is unconstitutionally vague if it fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement.

70. Assange could assert the above-mentioned arguments in a number of ways. He could file pre-trial motions with the trial judge, motions following closure of the government’s direct case at trial, and again following the closure of all evidence in his case. If convicted, he would have a right to appeal these rulings once as of right to an appellate court as well as discretionary appeals up to the United States Supreme Court.

71. To be clear, the United States has arguments against these potential challenges to the superseding indictment, and does not believe that they would have any merit; otherwise, it would not have proceeded with the charges. Without binding the United States to any position here, however, we could advance a number of arguments in response to those challenges. For example, concerning selective prosecution, the United States could argue that because of Assange’s unprecedented conduct, there are no other similarly situated individuals, and even if there were, there was no invidious decision to prosecute. Concerning any First Amendment challenge, the United States could argue that foreign nationals are not entitled to protections under the First Amendment, at least as it concerns national defense information, and even were they so entitled, that Assange’s conduct is unprotected because of his complicity in illegal acts and in publishing the names of innocent sources to their grave and imminent risk of harm. *See also* paragraphs 7-9 (summarizing relevant First Amendment Law). Concerning any void-for-vagueness claim, the United States could point out that courts are not to expect statutes to

provide “[p]erfect clarity and precise guidance.” *Williams*, 553 U.S. at 304; *see also United States v. Saunders*, 828 F.3d 198, 207 (4th Cir. 2016) (“[A] statute need not spell out every possible factual scenario with ‘celestial precision’ to avoid being struck down on vagueness grounds.”). Moreover, I am confident that our use of the grand jury in this investigation was proper, as explained in Section V, below. Regardless of the arguments the United States will ultimately assert, however, what is important here is that Assange will have an opportunity to challenge the alleged facts before an independent jury, and challenge the law supporting the charges in the superseding indictment before independent United States courts. Those courts are most familiar with the nuances of United States law, and are best suited to address any legal or constitutional challenges that Assange may have to his prosecution.

II. Any Bias Among Potential Jurors Can Be Ferreted Out Through the Robust Jury Selection Process Employed in United States Federal Courts

72. If he is extradited to the United States, Assange will be afforded the right to require the government to prove the charges against him to a unanimous and impartial jury beyond a reasonable doubt. Assange has claimed, however, that he will not receive a fair trial in the U.S. District Court for the Eastern District of Virginia, because of alleged negative statements about him that have been publically reported and because of the nature of the jury pool in the Eastern District of Virginia, which is alleged to have a large number of government workers and/or government contractors. In response, I summarize here some of the rules and procedures employed by U.S. federal courts to ensure that a potential juror is not influenced by exposure to pretrial publicity or by the juror's employer.

73. The Sixth Amendment to the Constitution of the United States guarantees that in all criminal prosecutions, the defendant shall enjoy the right to trial by an impartial jury. Even pervasive and adverse pretrial publicity, however, need not lead to an unfair trial. *See, e.g.,*

United States v. Skilling, 561 U.S. 368, 384 (2010) (widespread negative coverage about Enron did not prevent a former Enron executive from receiving a fair trial).

74. It is not uncommon in the course of voir dire for a venire member to disclose familiarity with a case by virtue of pre-trial publicity. Indeed, this occurs just as often in locally notorious cases as in cases of national interest. *See, e.g., United States v. John Walker Lindh*, 212 F. Supp. 2d 541, 549 (E.D. Va. 2002) (regarding the selection of a jury for an American captured in Afghanistan fighting for the Taliban). Yet, what ultimately matters to a U.S. judge is not simply whether a potential juror has heard or read about a case, but whether a prospective “juror can lay aside his impression or opinion and render a verdict based on the evidence presented in court.” *Irvin v. Dowd*, 366 U.S. 717, 722–23 (1961). As the United States Supreme Court stated in *Irvin*:

To hold that the mere existence on any notion as to the guilt or innocence of an accused, without more, is sufficient to rebut the presumption of a prospective juror’s impartiality would be to establish an impossible standard. It is sufficient if the juror can lay aside his impression or opinion and render a verdict based on the evidence presented in court.

Id. at 723.

75. If Assange is extradited to face trial in the United States, the district judge would conduct a thorough voir dire of all potential jurors, in the presence of attorneys for both the government and the defendant, to ensure the selection of a fair and impartial jury that is able to set aside any pre-conceived notions regarding this case, and to render an impartial verdict based solely on the evidence presented in the case and the district court’s instructions of law. Only those prospective jurors found to be capable of fair and impartial jury service after careful voir dire will be declared eligible to serve as jurors. *See Lindh*, 212 F. Supp. 2d at 552. The defendant can challenge any number of jurors for good cause. Moreover, even if the district court

judge disagrees that such good cause exists, the defendant will be entitled to challenge ten jurors without any cause at all (other than race or sex). *Flowers v. Mississippi*, 139 S. Ct. 2228, 2243 (2019); Fed. R. Crim. P. 24(b)(2). These without cause challenges are known as “peremptory challenges.”

76. The U.S. District Court for the Eastern District of Virginia in particular has been the venue for many high profile criminal trials, including trials of defendants accused of crimes involving national security. Past experience provides reasonable assurance that a sufficient number of qualified, impartial jurors would be identified as a result of the voir dire in this case. *See Lindh*, 212 F. Supp. 2d at 552. After all, a jury seated in this district refused to return the death verdict sought by the United States against Zacharias Moussaoui, who pleaded guilty to the conspiracy to murder thousands of Americans on 9/11, even though as part of that conspiracy, a hijacked airliner was crashed into the Pentagon, just a few miles away from the very courthouse in which the jury sat. *See United States v. Moussaoui*, 591 F.3d 263, 265 (4th Cir. 2010).

77. Any potential for prejudice in this case is also mitigated by the large size of the jury pool in Northern Virginia. *Mu’Min v. Virginia*, 500 U.S. 415, 429 (1991). After all, more than 1,100,000 people reside in Fairfax County, and Fairfax is but one county in the Alexandria Division of the Eastern District of Virginia. *See Country of Fairfax, Virginia, Demographic Reports* (2019), <https://www.fairfaxcounty.gov/demographics/sites/demographics/files/assets/demographicreports/fullreport.pdf>; *see also Gentile v. State Bar of Nev.*, 501 U.S. 1030, 1044 (1991) (noting that there is a reduced likelihood of prejudice where venire was drawn from a pool of over 600,000 individuals); *United States v. Taylor*, 942 F.3d 205, 223 (4th Cir. 2019) (noting that the likelihood of prejudice from extensive pretrial publicity was reduced by the fact that the City of Baltimore had a population of approximately 620,000).

78. All prospective jurors in this case will be questioned carefully as to what they have seen, read, or heard about the case and whether they have formed any opinions or impressions. No juror will be qualified to serve unless the district judge is satisfied that the juror is (i) able to put aside any previously formed opinions or impressions, (ii) prepared to pay careful and close attention to the evidence as it is presented in the case, and finally (iii) able to render a fair and impartial verdict, based solely on the evidence adduced at trial and the district court's instructions of law. *See Lindh*, 212 F. Supp. 2d at 549.

79. The district judge will follow a similar process to determine whether any potential jurors would be biased based on their employment by the U.S. government or a government contractor. "A juror employed by the government is not disqualified from a case in which the government is a party simply by reason of his employment. To challenge for cause, a party must show 'actual partiality growing out of the nature and circumstances of [the] particular case.'" *United States v. Tibesar*, 894 F.2d 317, 319 (8th Cir. 1990) (citations omitted). *See Zia Shadows, L.L.C. v. City of Las Cruces*, 829 F.3d 1232, 1246–47 (10th Cir. 2016) (a juror employed by the government could be disqualified if the juror's answers "establish actual bias").

80. The district judge will ask questions to ascertain whether any prospective juror's employment would render such juror incapable of being fair in a case in which the U.S. government is a party. Further, the judge will ask questions to determine whether any prospective juror can put aside pre-existing views about the U.S. government, and decide the case based purely on the evidence and the instructions from the judge. In any event, if Assange

believes that a juror determined by the judge to be qualified to serve is, in fact, biased against him, he can exercise one of his ten peremptory challenges to strike the juror without cause.²

81. The particular practices that judges in our district use to select jurors vary, but all act to ensure that the jurors ultimately selected are able to render a fair and impartial verdict. For example, in a highly publicized terrorism case in which I was involved, the judge ordered the parties to submit a proposed jury questionnaire. Four days before jury selection started, the judge used the submissions of the parties to craft a detailed questionnaire and provide it to an unusually large jury pool of 120 prospective jurors. Upon the basis of the answers to the questionnaire and individualized voir dire that occurred over two days, the district judge ultimately found 27 prospective jurors to be qualified. After the parties exercised peremptory challenges, a jury of 12 jurors and two alternates were seated to hear the evidence in the case.

III. Conditions of Confinement in the United States

82. Following extradition, Assange will be brought before a federal magistrate judge “without unnecessary delay,” which, in practice, typically means the same day as he arrives in the country, or the following day. *See* Federal Rule of Criminal Procedure 5(a)(1)(A). At the initial hearing, the magistrate judge will ensure Assange is represented by counsel, and set a time for a detention hearing to determine if pretrial detention is lawful and necessary. If Assange is ordered to be detained, the United States Marshals Service (“USMS”) will be responsible for housing him pre-trial, and, if he is convicted, until he is sentenced. If he is held in custody pre-trial, Assange will likely be held in the William G. Truesdale Adult Detention Center (“ADC”) in Alexandria, Virginia. The ADC houses federal prisoners through a contract with the USMS. In

² In contrast, in the U.S. District Court for the Eastern District of Virginia, the government is traditionally only allowed six “peremptory challenges.” *See* Federal Rule of Criminal Procedure 24(b)(2).

2018, the ADC housed an average of 373 inmates in 2018. Of these, roughly one-third were federal prisoners. The ADC is one of approximately 38 correctional facilities nationwide to be accredited by the American Correctional Association, the Commission on Accreditation for Law Enforcement Agencies, and the National Commission on Correctional Health Care.

83. If and when Assange arrives in the ADC, he will initially be held in the booking area of the facility. ADC staff will interview Assange to determine where he should be placed in the ADC. ADC staff will also complete a risk assessment to determine any risks to Assange from his detention. Using an objective point scale, the ADC staff will make a recommendation about where Assange should be housed. He will then be assigned to the appropriate housing unit. There is no solitary confinement in the ADC. The seven housing categories are:

- General Population;
- Administrative Segregation;
- Disciplinary Segregation and Pre-Hearing Segregation (the latter of which is used for inmates who are charged with but not yet found guilty of violating a Detention Center rule);
- Medical Segregation;
- Protective Custody; and
- Critical Care Mental Health Unit.

84. It is possible Assange could be placed in protective custody because of his notoriety. Protective custody is a classification for inmates who need protection from other inmates. Inmates in protective custody are not permitted to attend programs with general population inmates, but they do receive all Detention Center services, unless their presence causes a safety or security risk to the inmate or the facility.

85. It also is possible that Assange could be placed in administrative segregation status if, for example, he presents a safety risk to himself. For that to happen, the ADC would have to find that one or more of the following factors was present:

- During a prior incarceration, the inmate participated in an incident that posed a safety or security risk;
- The inmate is a safety risk to other inmates, prison staff, or one's self;
- The inmate is a security risk to the ADC;
- The ADC staff has concerns about the inmate's adjustment to incarceration;
- The inmate has an extensive criminal history or a serious charge; and/or
- The ADC does not have sufficient information about an inmate to make an informed housing decision because, for example, the inmate does cooperate in the intake and admission process.

86. Inmates in administrative segregation are housed in their cells for a maximum of 22 hours per day. They receive breaks according to an established break schedule. The inmates typically use these breaks to make personal telephone calls and attend to hygiene needs. Inmates in administrative segregation are able to attend three programs, including programs with general population inmates, per week. They also receive all ADC services. By contrast, inmates in protective custody are only permitted to interact with other inmates in protective custody. Inmates in administrative segregation do not have to choose between receiving their break and participating in a program. Prison staff assess inmates in administrative segregation or on special protocols daily. In addition, the ADC's Inmate Management team meets weekly. The Inmate Management team comprises members from the following divisions: Security, Medical, Classification, and Mental Health. The ADC may choose to restrict programs or services if its staff determines at intake, or at any other time, that participating in a program or receiving a service poses a safety or security risk.

87. Typically, there are several inmates in administrative segregation. Inmates in administrative segregation are able to speak to one other through the doors and windows of their cells. Additionally, if it is safe to do so, they may be in a day-room at the same time as other inmates. Moreover, placement in administrative segregation has no impact on an inmate's ability to meet with his or her lawyer.

88. I am aware that Assange has raised an issue as to his mental health and that it is anticipated that he will be subject to further medical examination on behalf of the United States. I will, therefore, describe the general context of the provision of medical care to prisoners in the ADC.

89. Like all facilities used by the USMS, the ADC is required to provide full medical care to prisoners. This care includes medical, dental, and mental health care. Prisoners routinely receive care for chronic conditions within the ADC. All outside medical care must be pre-approved by the USMS, based upon established health standards. In the event of an emergency, the detention facility must proceed immediately with medical treatment. If necessary, prisoners in need of urgent care are immediately transported to the hospital.

90. If necessary, I can provide more detailed information regarding mental health treatment and suicide prevention protocols at the ADC and in penitentiaries of the United States Bureau of Prisons ("BOP"). For now, I offer the following general information. At intake in the ADC, all inmates are assessed for risk of suicide. If the ADC staff determines, at intake or at any other time, that an inmate poses a risk of suicide, he will be placed in the suicide protocol. The ADC staff will consider, among other things, any mental health diagnoses and whether an inmate has communicated suicide concerns verbally or has taken actions consistent with attempting suicide.

91. The suicide protocol is as follows. The inmate is provided a safety smock and a safety blanket, placed on suicide watch, and evaluated by a mental health professional as soon as possible. If the inmate communicates a suicide plan or takes actions consistent with attempting suicide, the case is deemed acute. In acute cases, inmates are watched by a prison staff member one-on-one and continuously. In non-acute cases, inmates are checked by a prison staff member every 15 minutes. In both circumstances, inmates also are monitored through cameras. Prisoners on suicide watch are visited by mental health staff daily, and a psychologist three times per week. Only a psychologist can remove an inmate from the suicide protocol.

92. To determine whether the ADC meets basic criteria related to conditions of confinement and is suitable for use by the USMS, the USMS inspects the ADC annually. The USMS inspection process includes reviewing the ADC's average detainee population and staffing data; security; use of force; hygiene and sanitation; availability of medical care; availability of suicide prevention; and legal access and visitation. The ADC was last inspected by USMS personnel on August 5, 2019, and found to be in compliance. The Commonwealth of Virginia also conducts annual inspections of the ADC. The Virginia Department of Corrections last inspected the ADC from July 23-25, 2019. The Virginia Department of Corrections found the ADC to be in compliance with its standards. The USMS relies on the Commonwealth's inspections, in addition to its own, to determine whether to hold prisoners at the ADC.

93. During the last inspection period, which began in August 2017, there were no suicides in the ADC.

94. Inmate classification decisions are subject to appeal by an inmate. To appeal, Assange would send an Inmate Request Form to the captain of the Security Division. In addition, defendants are permitted to raise issues regarding the conditions of their pretrial

confinement with the district court judge presiding over their criminal case. In sum, there are procedural protections in place for pretrial detainees.

95. It is possible that Assange would be subjected to special administrative measures (“SAMs”) during pretrial detention and, if he is convicted, during any period of incarceration. *See* 28 Code of Federal Regulations (“C.F.R.”) § 501.2. There are two categories of special administrative measures, both of which are described in the C.F.R. 28 C.F.R. § 501.2 governs those measures intended for the protection of national security information, and 28 C.F.R. § 501.3 governs those measures based on violence or terrorism concerns. Based on my knowledge of this case and my experience as a prosecutor, any special administrative measures imposed in this case would likely be imposed under Section 501.2.

96. In order for the Attorney General to direct a warden to impose these special administrative measures, the head of a member agency of the United States intelligence community must certify that the unauthorized disclosure of classified information would pose a threat to the national security, and that there is a danger that the inmate will disclose such information. The special administrative measures must be “reasonably necessary to prevent disclosure of classified information that would pose a threat to the national security if the inmate disclosed such information.” *Id.* In other words, special administrative measures are not punitive. Rather, they must be tailored to protect the information at issue.

97. Special administrative measures may include restricting social visits, mail privileges, phone calls, access to other inmates and to the media, as well as placing an inmate in administrative segregation. Regulations generally exempt from monitoring correspondence, calls, and contacts between the inmate and his attorney. The implementing official, at the direction of the Attorney General, determines the period of time an initial special administrative

measure is imposed, up to one year. *Id.* The implementing official may also extend such special administrative measures in increments of time not to exceed one year. An extension requires, however, that the intelligence community certifies that there is a continued danger that the inmate will disclose classified information and that the unauthorized disclosure would pose a threat to the national security.

98. The affected inmate will receive written notification of the restrictions imposed and the basis for these restrictions. The bases set forth in the notification may be described as in the interest of prison security or safety, national security, or to protect against acts of violence or terrorism. In addition, the inmate must sign for and receive a copy of the notification. *See* 28 C.F.R. §§ 501.2(b), 501.3(b). Similar inmate notification and acknowledgment are also required for a renewal.

99. An affected inmate may challenge the imposed special administrative measures through the Administrative Remedy Program, 28 C.F.R. part 542. *See* 28 C.F.R. §§ 501.2(d), 501.3(e). An inmate who has exhausted all administrative remedies may challenge those special administrative measures in federal court. *Yousef v. Reno*, 254 F.3d 1214, 1222 (10th Cir. 2001).

100. If Assange is convicted, then following his sentencing, the BOP will designate him to an appropriate facility for service of any sentence of incarceration. The BOP has sole authority to designate the place of confinement for federal prisoners. *See* 18 U.S.C. § 3621. By statute, the BOP is required to consider the type of offense; the length of sentence; the defendant's age; the defendant's release residence; the need for medical or other special treatment; any placement recommendation made by the court; and guidance issued by the United States Sentencing Commission. *Id.* Once a prisoner is designated, the USMS will transport the prisoner to the designated facility. The USMS will prepare a transportation package that contains

information regarding the prisoner's physical and mental health as well as any potential alert notifications, including suicidal tendencies. Upon arrival at the designated BOP facility, the staff will conduct an intake screening and obtain the necessary information to further classify the prisoner, so that he is housed and managed in accordance with BOP guidelines and any special needs the prisoner may have.

101. Upon direction of the Attorney General, the Director of the BOP may authorize a warden to implement special administrative measures. Such measures and processes related to their implementation are the same as those discussed in the section above regarding pretrial detention. Even if SAMs are not imposed, existing BOP regulations and policies constrain, to varying degrees, an inmate's communications and contacts. Under BOP regulations, all incoming correspondence potentially is subject to monitoring, 28 C.F.R. § 540.12, as are all phone calls, 28 C.F.R. § 540.102. All visits also are monitored, although the intensity of the monitoring depends on the security level of the facility. BOP regulations generally exempt from monitoring correspondence, calls, and person contacts between the inmate and his attorney.

102. Not all inmates who are under special administrative measures are housed at the Administrative Maximum Security United States Penitentiary ("ADX"), although many are. For example, prisoners under SAMs may be housed at a medical facility if necessary. There also may be other circumstances that result in a prisoner subject to such special administrative measures being housed at a facility other than ADX.

103. If he is sentenced to a period of incarceration, it is possible that Assange will be placed under special administrative measures for at least a portion of his sentence. As outlined above, such measures are imposed on a case-by-case basis using a number of different factors. It also is possible that the government will not seek to impose SAMs on Assange, but otherwise

seek to limit and monitor his visits and communications. If that is the case, Assange may be designated to a facility with a Communications Management Unit (“CMU”). There currently are two prisons with CMUs, and neither of these prisons is ADX.

104. CMUs house inmates who, due to their offense of conviction, offense conduct, or other verified information, require increased monitoring of their communications. Designation to a CMU is not punitive. In accordance with the Code of Federal Regulations, “A CMU is a general population housing unit where inmates ordinarily reside, eat, and participate in all educational, recreational, religious, visiting, unit management, and work programming, within the confines of the CMU. Additionally, CMUs may contain a range of cells dedicated to segregated housing of inmates in administrative detention or disciplinary segregation status.” 28 C.F.R. 540.200(b). Inmates may be designated to a CMU if evidence of the following exists:

- (a) The inmate's current offense(s) of conviction, or offense conduct, included association, communication, or involvement, related to international or domestic terrorism;
- (b) The inmate's current offense(s) of conviction, offense conduct, or activity while incarcerated, indicates a substantial likelihood that the inmate will encourage, coordinate, facilitate, or otherwise act in furtherance of illegal activity through communication with persons in the community;
- (c) The inmate has attempted, or indicates a substantial likelihood that the inmate will contact victims of the inmate's current offense(s) of conviction;
- (d) The inmate committed prohibited activity related to misuse or abuse of approved communication methods while incarcerated; or
- (e) There is any other substantiated/credible evidence of a potential threat to the safe, secure, and orderly operation of prison facilities, or protection of the public, as a result of the inmate's communication with persons in the community.

28 C.F.R. § 540.201.

105. Inmates receive written notice of the initial designation to a CMU. The designation is reviewed regularly by the inmate’s Unit Team, and the inmate is provided “notice

and an opportunity to be heard, in accordance with the Bureau's policy on Classification and Program Review of Inmates." *Id.* § 540.202. "The inmate may challenge the CMU decision, and any aspect of confinement therein, through the Bureau's administrative remedy program."

Id. The restrictions in a CMU vary but include limitations on written correspondence and electronic messages, telephone communications, as well as visits. *See* §§ 540.203-205. If requested, I can provide more detail on the specifics of these limitations. Inmates in CMUs are permitted to communicate and visit with their attorneys as necessary in furtherance of litigation.

106. As noted above, SAMs are reviewed annually. Likewise, an inmate's designation is reviewed at least once every six months. Specific to ADX, inmates who demonstrate periods of clear conduct and positive institutional adjustment, may progress from the General Population Units to the Intermediate, Transitional, and Pre-Transfer Units. Those inmates successful in the Pre-Transfer Unit may transfer out to an appropriate BOP facility. The types of privileges afforded to the inmates are determined by their housing unit assignments in this stratified system, or program. It will take an inmate a minimum of 36 months to work his way through the stratified system of housing. The minimum stay in a General Population Unit is 12 months; the minimum stay in an Intermediate Unit is six months; the minimum stay in a Transitional Unit is six months; and the minimum stay in a Pre-Transfer Unit is 12 months.

107. As noted above, I understand that Assange is to be examined on behalf of the United States in relation to his mental health. Given that such examination is outstanding, I will not address here any issues that might arise as to his access to mental health care in the event that he is convicted.

IV. Access to and Use of Evidence and Classified Materials in U.S. Federal Court

108. Contrary to his claims, Assange's defense team will not be severely limited in its access to material necessary to prepare for trial. Under Rule 16 of the Federal Rule of Criminal Procedures, the U.S. government is obligated to produce, *inter alia*, "any relevant written or recorded statements of the defendant." Fed. R. Crim. P. 16(a)(1)(B). The government also must permit the defendant to inspect and copy materials such as books, papers, documents, and data that are in the government's possession if "(i) the item is material to preparing the defense; (ii) the government intends to use the item in its case-in-chief at trial; or (iii) the item was obtained from or belongs to the defendant." *Id.* 16(a)(1)(E). The government is also required to produce information that is exculpatory, *see Brady v. Maryland*, 373 U.S. 83 (1963); information that can be used to challenge a witness's credibility, *see Giglio v. United States*, 405 U.S. 150 (1972); and prior statements of any government witnesses, *see* 18 U.S.C. § 3500; Fed. R. Crim. P. 26.2. These obligations exist in all cases, regardless of whether the information is classified.

109. To fulfill its discovery obligations in this case, we expect to provide defense counsel with classified information. Further, we expect that the defendant will retain counsel who have or can obtain security clearances, or that the court will appoint counsel with security clearances. These attorneys, commonly referred to as "cleared counsel," are authorized to receive and review discoverable classified material.

110. As a practical matter, Assange will be able to review certain classified information that has been disclosed by the prosecution in accordance with its discovery obligations. The federal courthouse in Alexandria, Virginia has several secure classified information facilities ("SCIFs") that are designated for use by defense counsel. The SCIFs contain safes for the storage of hard copy documents as well as computers to review electronic evidence. The federal

courthouse is approximately one-half mile from the ADC, and defendants in national security cases are routinely transported to-and-from the defense SCIFs so that they can prepare for trial. Nevertheless, some classified information may be provided only to cleared counsel and not to the defendant.

111. The Classified Information Procedures Act (“CIPA”), Title 18, United States Code, App. 3, governs the use of classified information in a criminal prosecution. CIPA is a procedural statute; it does not change the government’s discovery obligations or alter the rules of evidence. *See, e.g., United States v. Sedaghaty*, 728 F.3d 885, 903 (9th Cir. 2013); *United States v. Wilson*, 750 F.2d 7, 9 (2d Cir. 1984) (district court did not err in applying “generally applicable evidentiary rules of admissibility” to classified materials). Thus, CIPA does not affect a defendant’s right to a fair trial. Rather, CIPA provides procedural mechanisms to protect classified information and a defendant’s rights under the Due Process Clause of the U.S. Constitution. Accordingly, courts have explained that CIPA’s fundamental purpose is to “harmonize a defendant’s right to obtain and present exculpatory material upon his trial and the government’s right to protect classified material in the national interest.” *United States v. Pappas*, 94 F.3d 795, 799 (2d Cir. 1996) (quoting *United States v. Wilson*, 571 F. Supp. 1422, 1426 (S.D.N.Y. 1983)).

112. The government may withhold potentially discoverable material on the ground that it is classified only if the trial judge agrees that it is not relevant and helpful to the defense. Under CIPA and related caselaw, the government may file a motion *ex parte* and *in camera* asking for authorization to withhold this material from the defendant. *See* 18 U.S.C. App. 3 § 4; *United States v. Moussaoui*, 382 F.3d 453, 471-72 (4th Cir. 2004). The government may seek to protect information partially or in its entirety, to substitute a summary of any classified

information that is relevant and helpful, or to substitute a statement admitting relevant facts the classified information would tend to prove. *Id.* §§ 4, 6; see *United States v. Yunis*, 867 F.2d 617, 621-25 (D.C. Cir. 1989).

113. If either party intends to disclose classified information in a pretrial proceeding or at trial, the government may request a hearing governing the use, relevance, and admissibility of the information. 18 U.S.C. App. 3 § 6(a). The hearing is *in camera* if the Attorney General certifies to the court that a public proceeding may result in the disclosure of classified information. *Id.* The United States must provide the defendant with the classified information at issue. *Id.* § 6(b)(1). The court, upon request of the defendant, may order the United States to provide the defendant, prior to trial, such details as to the portion of the indictment at issue in the hearing as are needed to give the defendant fair notice to prepare for the hearing. *Id.* § 6(b)(2).

114. In the United States, witnesses rarely testify under pseudonyms. Ordinarily, the Confrontation Clause of the Sixth Amendment to the United States Constitution guarantees a defendant the right to question an adverse witness about identifying information, including his full name and address. *Smith v. Illinois*, 390 U.S. 129, 131 (1968). A defendant's right to identifying information about witnesses is not absolute, however, and a district court has discretion to determine whether effective cross-examination is possible if the witness's identity is concealed. *Delaware v. Van Arsdall*, 475 U.S. 673, 679 (1986) (holding that the Confrontation Clause permits limitations on cross-examination "based on concerns about, among other things ... the witness' safety").

115. At this point, the trial team does not anticipate that any of its trial witnesses will testify under a pseudonym. In any event, the government cannot withhold witness identifying information unilaterally. To convince a court to authorize the withholding of identifying

information for a witness from the defendant or the public, courts require the government to show that doing so is necessary to protect the witness from harm. For example, based on the “heightened level of danger to which El Salvadorians who testify against MS-13 in U.S. courts are subject,” a U.S. federal district court permitted the government to withhold the true names of El Salvadorian witnesses from both the defendant and the public. *United States v. Ramos-Cruz*, 667 F.3d 487, 501 (4th Cir. 2012).³ In contrast, in *United States v. Sterling*, 724 F.3d 482, 517 (4th Cir. 2013), a judge in my district allowed the government to withhold the true names of CIA operatives from the jury, but not from the defendant or his lawyers, on the grounds that neither defendant nor lawyers posed a threat to the safety of the witnesses. *Sterling*, 724 F.3d at 516. As with any evidentiary ruling, a defendant can challenge in the district court and later, in the court of appeals, a witness's use of a pseudonym.

116. CIPA does not alter the Federal Rules of Evidence regarding relevance and admissibility. In other words, CIPA does not preclude the admission of evidence simply because it is classified. CIPA includes procedural mechanisms for a defendant who wishes to use classified information. The defendant must provide notice to the government of any classified information he wishes to use in a pretrial proceeding or at trial. 18 U.S.C. App. 3 § 5. The notice must provide a “brief description” of any classified information the defendant “reasonably expects to disclose or to cause the disclosure of.” *Id.* The “brief description” must provide the government sufficient notice as to the information at issue, “setting forth specifically the classified information which the defendant reasonably believes to be necessary to his defense.” *United States v. Collins*, 720 F.2d 1195, 1999 (11th Cir. 1983).

³ Mara Salvatrucha, commonly known as "MS-13", is an international criminal gang.

117. As discussed above, if the government opposes the defendant's request to use classified information, the court must hold a hearing. 18 U.S.C. App. 3 § 6(a). The hearing is *in camera* if the Attorney General certifies to the court that a public proceeding may result in the disclosure of classified information. *Id.* The defendant bears the burden of showing that the classified evidence is both relevant and admissible. *See, e.g., United States v. Miller*, 874 F.2d 1255, 1277 (9th Cir. 1989). The defendant may use classified information that is "relevant and material to the defense." *United States v. Abu Ali*, 528 F.3d 210, 248 (4th Cir. 2008). The information must be "at least essential to the defense, necessary to [the] defense, and neither merely cumulative nor corroborative." *United States v. Smith*, 780 F.2d 1102, 1110 (4th Cir. 1985) (*en banc*).

118. If the court finds that the noticed classified information is admissible, the government may request that in lieu of the disclosure of such specific classified information, the court order: (a) the substitution for such classified information of a statement admitting relevant facts that the specific classified information would tend to prove; or (b) the substitution for such classified information of a summary of the specific classified information. *See* 18 U.S.C. App. 3 § 6(c). The court shall grant the government's motion to substitute or summarize the classified information if the alternative provides the defendant with "substantially the same ability to make his defense as would disclosure of the specific classified information." *Id.* These hearings may also be held *in camera* at the government's request. In support of its request to use a summary or substitution in lieu of the actual classified information, the government may "submit to the court an affidavit of the Attorney General certifying that disclosure of classified information would cause identifiable damage to the national security of the United States and explaining the basis

for the classification of such information.” *Id.* This affidavit is to be examined *in camera* and *ex parte*.

119. CIPA also imposes a duty of reciprocity on the government. *See* 18 U.S.C. App. 3 § 6(f). “Whenever the court determines pursuant to subsection (a) that classified information may be disclosed in connection with a trial or pretrial proceeding, the court shall, unless the interests of fairness do not so require, order the United States to provide the defendant with the information it expects to use to rebut the classified information.” *Id.* This obligation may continue through the duration of the proceedings. *Id.* If the United States fails to comply with this duty, “the court may exclude any evidence not made the subject of a required disclosure and may prohibit the examination by the United States of any witness with respect to such information.”

120. Entering classified information into evidence need not alter its classification status. To protect classified information from unnecessary disclosure, a court may order that only portions of an exhibit be admitted into evidence and may excise any classified information. *Id.* § 8. During the examination of any witness, the government may object to any question or line of inquiry that may result in the disclosure of classified information. *Id.* Following such objection, the court shall take “suitable action” to safeguard against the compromise of classified information. *Id.* This action may include a proffer from the parties concerning the nature of information sought and the nature of the information at risk of disclosure.

V. Manning Has Been Treated Fairly and According To Law.

121. In his affidavit, Robert J. Boyle has made a number of allegations concerning grand jury proceedings in the United States involving Chelsea Manning. At the outset, it is important for this court to note the extent of due process Manning has received from U.S. courts

in response to her refusal to provide testimony to the grand jury. As outlined below, two federal trial judges have independently considered and rejected her many claims, as has a three judge panel on the court of appeals.

122. Set out below is an overview of the relevant aspects of the federal grand jury system in the United States, a brief description of Manning’s legal proceedings, and specific responses to Boyle’s opinions regarding the legality of Manning’s proceedings under U.S. law. In summary, Boyle’s opinions should not be given any weight for the following reasons: (1) Boyle, as a nonparticipant in the grand jury proceedings, lacks the necessary information to render his opinion; (2) Manning was properly subpoenaed to testify before the grand jury in connection with a legitimate criminal investigation; (3) Manning has already raised, and the U.S. courts have already rejected, the exact same arguments advanced by Boyle; and (4) in any event, Assange will have an opportunity to raise these arguments in the U.S. judicial system after he is extradited.

A. Overview of the Grand Jury System in the United States

1. Functions of the Grand Jury

123. “The institution of the grand jury is deeply rooted in Anglo-American history.” *United States v. Calandra*, 414 U.S. 338, 342 (1974). It was “brought to [the United States] by the early colonists and incorporated in the Constitution by the Founders.” *Costello v. United States*, 350 U.S. 359, 362 (1956). “[T]he Founders thought the grand jury so essential to basic liberties that they provided in the Fifth Amendment that federal prosecution for serious crimes can only be instituted by ‘a presentment or indictment of a Grand Jury.’” *Calandra*, 414 U.S. at 343. The Grand Jury Clause of the Fifth Amendment to the U.S. Constitution states, in full, that “[n]o person shall be held to answer for a capital, or otherwise infamous crime, unless on a

presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger.” U.S. Const. amend. V.

124. The American grand jury “was intended to operate substantially like its English progenitor.” *Costello*, 350 U.S. at 362. Its “mission is to clear the innocent, no less than to bring to trial those who may be guilty.” *United States v. Dionisio*, 410 U.S. 1, 16-17 (1973). To achieve those ends, the grand jury “serves two interrelated but distinct functions.” SARA SUN BEALE ET AL., GRAND JURY LAW & PRACTICE § 1:7 (2d ed. 1997).

125. First, the grand jury serves as “an investigatory body charged with the responsibility of determining whether or not a crime has been committed.” *United States v. R. Enters., Inc.*, 498 U.S. 292, 297 (1991). The grand jury conducts “ex parte investigation[s] to determine whether a crime has been committed and whether criminal proceedings should be instituted against any person.” *Calandra*, 414 U.S. at 343-44. It has “broad investigative powers,” *Dionisio*, 410 U.S. at 15, and generally may “inquire into all information that might possibly bear on its investigation until it has identified an offense or has satisfied itself that none has occurred,” *R. Enters.*, 498 U.S. at 297.

126. Second, the grand jury protects individuals from “hasty, malicious and oppressive,” *Wood v. Georgia*, 370 U.S. 375, 390 (1962), or otherwise “unfounded criminal prosecutions,” *Branzburg v. Hayes*, 408 U.S. 665, 686-87 (1972). Under the Fifth Amendment, federal prosecutors must obtain an indictment from a grand jury to prosecute an individual for a felony offense, *see* U.S. Const. amend. V, unless the individual waives the right to be charged by indictment, *see* Fed. R. Crim. P. 7(b). In determining whether to return an indictment, the grand jury alone deliberates and decides whether there is probable cause to believe that the individual committed the crime. *See Kaley v. United States*, 571 U.S. 320, 328 (2014); *United States v.*

Williams, 504 U.S. 36, 48 (1992). Thus, the grand jury serves as a “kind of buffer or referee between the Government and the people.” *Williams*, 504 U.S. at 47.

127. In the Eastern District of Virginia, a grand jury consists of 23 members who generally meet for three (3) consecutive days per month for six (6) to 18 months. See Jury Service FAQ’s, United States District Court for the Eastern District of Virginia, available at <http://www.vaed.uscourts.gov/jury/jury-service.htm> (last visited Jan. 7, 2020). The grand jurors take an oath that “binds them to inquire diligently and objectively into all federal crimes committed within the district about which they have or may obtain evidence, and to conduct such inquiry without malice, fear, ill will, or other emotion.” Handbook for Federal Grand Jurors, *supra*, at 7. To return an indictment, at least 16 grand jurors must be present and at least 12 must vote in favor of it. See Fed. R. Crim. P. 6(f); Handbook for Federal Grand Jurors, *supra*, at 7.

128. The grand jury “belongs to no branch of the institutional Government.” *Williams*, 504 U.S. at 47. “[T]he Fifth Amendment’s constitutional guarantee [of the grand jury] presupposes an investigative body acting independently of either prosecuting attorney or judge.” *Id.* at 49 (quoting *Dionisio*, 410 U.S. at 17-18) (internal quotation marks omitted). While prosecutors present evidence to the grand jury and ask the grand jury to return indictments, the grand jury is not a part of, or subservient to, the Executive Branch. See *United States v. (Under Seal)*, 714 F.2d 347, 349 (4th Cir. 1983) (recognizing the “simple, but fundamental, concept that the grand jury serves an independent investigatory function and is ‘not meant to be the private tool of the prosecutor’” (quoting *United States v. Fisher*, 455 F.2d 1101, 1105 (2d Cir. 1972))).

2. The Ex Parte and Secretive Nature of Grand Jury Proceedings

129. “A grand jury proceeding is not an adversary hearing in which the guilt or innocence of the accused is adjudicated.” *Calandra*, 414 U.S. at 343. Instead, a grand jury

proceeding is an “ex parte investigation to determine whether a crime has been committed and whether criminal proceedings should be instituted against any person.” *Id.* at 343-44. The grand jury hears evidence presented by prosecutors and then deliberates in private to decide whether probable exists to charge an individual by indictment. *See* BEALE ET AL., *supra*, § 1:6; Handbook for Federal Grand Jurors, *supra*, at 4-5, 11-13. “The target of the grand jury’s investigation is not entitled to be present, and witnesses are not entitled to have counsel accompany them into the grand jury room (although the witness may leave the room to consult with counsel).” BEALE ET AL., *supra*, § 1:6. If the grand jury finds probable cause to charge an individual, the accused then has a constitutional right to an adversarial, fair trial to adjudicate his guilt or innocence. *See* U.S. Const. amend. VI.

130. In addition to their ex parte nature, the general rule is that grand jury proceedings are conducted in secret. The secretive nature of grand jury proceedings serves to protect the accused as well as the integrity of the system:

First, if preindictment proceedings were made public, many prospective witnesses would be hesitant to come forward voluntarily, knowing that those against whom they testify would be aware of that testimony. Moreover, witnesses who appeared before the grand jury would be less likely to testify fully and frankly, as they would be open to retribution as well as to inducements. There also would be the risk that those about to be indicted would flee, or would try to influence individual grand jurors to vote against indictment. Finally, by preserving the secrecy of the proceedings, we assure that persons who are accused but exonerated by the grand jury will not be held up to public ridicule.

Douglas Oil Co. of Cal. v. Petrol Stops Nw., 441 U.S. 211, 219 (1979).

131. To safeguard these interests, the law imposes secrecy obligations on participants (except for witnesses) in grand jury proceedings. *See* Fed. R. Crim. P. 6(e)(2). The general rule is that participants, including government attorneys, may “not disclose a matter occurring before the grand jury.” *Id.* R. 6(e)(2)(B). These secrecy obligations are subject to a number of carefully

delineated exceptions. *See id.* R. 6(e)(3); *United States v. Sells Eng'g, Inc.*, 463 U.S. 418, 424-25 (1983).

3. The Power of the Grand Jury to Subpoena Witnesses

132. As part of its broad investigative powers, the grand jury may subpoena witnesses to testify before it. *See Branzburg*, 408 U.S. at 688. Generally speaking, prosecutors will “advise grand jurors as to what witnesses should be called” and issue the appropriate subpoenas. Handbook for Federal Grand Jurors, at 8. When a witness appears before the grand jury, the prosecutors usually will question him first and then allow the grand jurors an opportunity to question him. *See id.* at 9. The grand jury may also request that the prosecutors call additional witnesses. *Id.* at 8.

133. Every person called as a “witness is bound not only to attend but to tell what he knows in answer to questions framed for the purpose of bringing out the truth of the matter under inquiry.” *Blair v. United States*, 250 U.S. 273, 282 (1919). The grand jury “has a right to every man’s evidence, except for those persons protected by a constitutional, common-law, or statutory privilege.” *Branzburg*, 408 U.S. at 688 (quoting *United States v. Bryan*, 339 U.S. 323, 331 (1950)) (internal quotation marks omitted). “The duty to testify [before the grand jury] has long been recognized as a basic obligation that every citizen owes his Government.” *Calandra*, 414 U.S. at 345.

134. There are limits to this power, however. In calling witnesses, a grand jury cannot “violate a valid privilege, whether established by the Constitution, statutes, or the common law.” *Id.* at 346. As particularly relevant here, the Fifth Amendment to the U.S. Constitution generally precludes individuals from being compelled to incriminate themselves before the grand jury. *See Kastigar v. United States*, 406 U.S. 441, 443-45 (1972). That said, under federal law, a court can

grant a witness “use immunity,” which generally prevents the witness’s testimony from being used against the witness, *see* 18 U.S.C. § 6002, and then compel the witness to testify before the grand jury, even if the testimony would otherwise incriminate him, *see* 18 U.S.C. § 6003(a); *Kastigar*, 406 U.S. at 462.

135. Where a person refuses to comply with a grand jury subpoena to testify, courts have the inherent authority to enforce the subpoena through its civil-contempt powers. *See Shillitani v. United States*, 384 U.S. 364, 370 (1966). That inherent authority is supplemented by the recalcitrant witness statute, which allows a court to order a witness’s confinement when the witness refuses, “without just cause shown,” to comply with the court’s order to testify before the grand jury. 28 U.S.C. § 1826(a). The witness may be confined “until such time as the witness is willing to give such testimony” or for “the life of . . . the term of the grand jury,” whichever is earlier, but not to “exceed eighteen months.” *Id.* In addition to confinement, the court may impose other sanctions tailored to compel compliance with its order, such as fines. *See Int’l Union, United Mine Workers of Am. v. Bagwell*, 512 U.S. 821, 827 (1994); *In re Grand Jury Proceedings*, 280 F.3d 1103, 1109-10 (7th Cir. 2002).

136. The purpose of civil-contempt sanctions is that they are “coercive and avoidable through obedience.” *Bagwell*, 512 U.S. at 827. That means the contemnor must be able to “end the sentence and discharge himself at any moment by doing what he had previously refused to do.” *Gompers v. Buck’s Stove & Range Co.*, 221 U.S. 418, 442 (1911). Because “the contemnor is able to purge the contempt and obtain his release by committing an affirmative act,” he is considered to “carr[y] the keys of his prison in his own pocket.” *Bagwell*, 512 U.S. at 828 (quoting *Gompers*, 221 U.S. at 442) (internal quotation marks omitted).

4. Limitations on the Grand Jury's Investigative Powers

137. While the grand jury's investigative powers are broad, they can be used only in furtherance of a legitimate function of the grand jury. "[P]ractices which do not aid the grand jury in its quest for information bearing on the decision to indict are forbidden." (*Under Seal*), 714 F.2d at 349. For example, the grand jury cannot "engage in arbitrary fishing expeditions" or "select targets of investigation out of malice or an intent to harass." *R. Enters.*, 498 U.S. at 299. Likewise, "prosecutors cannot use grand jury proceedings for the 'sole or dominant purpose' of preparing for trial on an already pending indictment." *United States v. Alvarado*, 840 F.3d 184, 189 (4th Cir. 2016) (quoting *United States v. Moss*, 756 F.2d 329, 332 (4th Cir. 1985)). That said, even after returning an indictment, the grand jury's investigative powers may still be used if the investigation relates to a superseding indictment involving additional defendants or additional crimes by an indicted defendant. *See Alvarado*, 840 F.3d at 190; *Moss*, 756 F.2d at 332.

138. Courts maintain a supervisory role to resolve allegations of grand jury abuse. *See Calandra*, 414 U.S. at 346; *Branzburg*, 408 U.S. at 688. While the grand jury enjoys a great degree of "operational separateness from its constituting court," it does not have the power to compel compliance with its subpoenas and "must appeal to the court when such compulsion is required." *Williams*, 504 U.S. at 48-49. A court will not require compliance with a grand jury subpoena when it would abuse the grand jury process or infringe on a valid privilege. *See id.* Where a grand jury subpoena is used for an improper purpose, the court may quash it. *See (Under Seal)*, 714 F.2d at 349-50.

5. Department of Justice Regulations on Prosecutors' Conduct Before the Grand Jury

139. In addition to the limitations imposed by judicial oversight, the U.S. Department of Justice's internal policies and procedures regulate federal prosecutors' conduct before the grand jury. For example, federal prosecutors are directed to observe the following standard of conduct:

In dealing with the grand jury, the prosecutor must always conduct himself or herself as an officer of the court whose function is to ensure that justice is done and that guilt shall not escape nor innocence suffer. The prosecutor must recognize that the grand jury is an independent body, whose functions include not only the investigation of crime and the initiation of criminal prosecution but also the protection of the citizenry from unfounded criminal charges. The prosecutor's responsibility is to advise the grand jury on the law and to present evidence for its consideration. In discharging these responsibilities, the prosecutor must be scrupulously fair to all witnesses and must do nothing to inflame or otherwise improperly influence the grand jurors.

Justice Manual 9-11.010, *available at* <https://www.justice.gov/jm/jm-9-11000-grand-jury#9-11.010> (last visited Jan. 7, 2020). These internal policies and procedures further protect witnesses and the targets of investigation from governmental overreach.

B. Background on Chelsea Manning

140. Chelsea Manning is a former intelligence analyst in the United States Army. In October 2009, Manning deployed to Iraq. During that deployment, Manning downloaded hundreds of thousands of classified documents and transmitted them to one or more agents of WikiLeaks, including Assange, for disclosure on its website. The classified documents included, among other things, significant activity reports related to the ongoing wars in Iraq and Afghanistan, Guantanamo Bay detainee assessment briefs, and United States Department of State cables.

141. In May 2010, Manning was arrested for these disclosures, and was prosecuted in a military court-martial. In February 2013, Manning pleaded guilty to lesser-included offenses of some but not all of the outstanding charges. Manning did not have a plea agreement with the prosecution.

142. When Manning entered guilty pleas to the lesser-included offenses, the military judge conducted a “providence inquiry” pursuant to the Rules for Courts-Martial. A providence inquiry is simply a colloquy designed to “ensure that a plea is voluntary and that there is a factual basis for the plea.” *Partington v. Houck*, 723 F.3d 280, 282-83 (D.C. Cir. 2013). The Rules for Courts-Martial provide that “[t]he military judge shall not accept a plea of guilty without making such inquiry of the accused as shall satisfy the military judge that there is a factual basis for the plea.” Manual for Courts-Martial, United States, R.C.M. 910(e), at II-102 (2012 ed.), available at https://www.loc.gov/rr/frd/Military_Law/pdf/MCM-2012.pdf (last visited Jan. 7, 2020). The discussion notes to the rule explain that “[t]he accused need not describe from personal recollection all the circumstances necessary to establish a factual basis for the plea. Nevertheless the accused must be convinced of, and able to describe all the facts necessary to establish guilt.” *Id.*

143. At Manning's providence inquiry, Manning first read a voluntary statement to provide a factual basis for the guilty pleas. Then, the military judge questioned Manning specifically about the factual basis of certain elements of the lesser-included offenses to which Manning was pleading guilty. In other words, Manning chose what facts to admit to support the guilty pleas, and the military court engaged in a limited inquiry to ensure the factual basis for the pleas. Manning was not subjected to exhaustive questioning about the offenses or the totality of the circumstances.

144. After Manning entered guilty pleas to the lesser-included offenses, the military prosecutors elected to go forward with the more serious offenses with which Manning was charged. Manning was ultimately convicted of Espionage Act and other offenses related to the unauthorized disclosures, while acquitted of other charges. In 2013, Manning was sentenced to 35 years of imprisonment. In January 2017, the President of the United States commuted Manning's sentence so that Manning would be released in May 2017, after serving approximately seven years in prison.

C. Manning's Grand Jury Proceedings⁴

145. In January 2019, Manning was subpoenaed to testify before a grand jury empaneled in the Eastern District of Virginia. The Honorable Claude M. Hilton, a federal judge who sits on the United States District Court for the Eastern District of Virginia, entered an order requiring Manning to testify and granting her use immunity. After Manning raised concerns that her testimony could still be used against her in future court-martial proceedings, a general court-martial convening authority in the Department of Army issued its own order granting Manning use immunity. These immunity orders eliminated any concern that compelling Manning to testify would violate her Fifth Amendment rights.

146. Manning's grand jury appearance date was set for March 5, 2019. Before her scheduled grand jury appearance, Manning filed an extensive motion to quash the subpoena. As

⁴ All of the publicly filed documents in this litigation can be found on PACER, <https://www.pacer.gov/>, a website developed by the Administrative Office of the United States Courts to provide public access to records of the U.S. courts. The litigation involved the following dockets: *In re Grand Jury Subpoena for Chelsea Manning*, No. 1:19-dm-00003-CMH-1 (E.D. Va.) (Judge Hilton); *United States v. John Doe 2010R03793*, No. 1:19-dm-00012-AJT-2 (E.D. Va.) (Judge Trenga); *In re Grand Jury Subpoena*, 19-1287 (4th Cir.) (Fourth Circuit).

particularly relevant here, Manning alleged, among other things, that prosecutors had issued the subpoena for improper purposes, such as to harass and retaliate against her.

147. On March 5, 2019, Judge Hilton, who oversaw the relevant grand jury, held a hearing on the motion to quash. After hearing extensive argument from the parties on the issues, Judge Hilton denied Manning's motion. Manning's grand jury appearance was scheduled for the next day.

148. Manning appeared before the grand jury but refused to answer questions posed to her. Judge Hilton therefore conducted a hearing on March 8, 2019, to determine whether Manning should be held in civil contempt for disobeying his order that she testify before the grand jury. At the hearing, at which Manning was represented by counsel, Judge Hilton found that Manning did not have just cause to refuse to answer the questions posed to her. Judge Hilton held Manning in civil contempt and ordered that she be incarcerated until she purged herself of the contempt or for the life of the grand jury.

149. Approximately one week later, Manning filed an appeal to the United States Court of Appeals for the Fourth Circuit. On appeal, Manning argued, among other things, that Judge Hilton had erred in holding that she failed to demonstrate any evidence of grand jury abuse. She claimed that prosecutors improperly used the grand jury process to harass and retaliate against her, and to prepare for trial against an already indicted defendant. On April 22, 2019, a three-judge panel from the United States Court of Appeals for the Fourth Circuit filed an order "find[ing] no error in the district court's rulings and affirm[ing] its finding of civil contempt."

150. Shortly thereafter, on May 9, 2019, the term of the grand jury expired. Consistent with the terms of Judge Hilton's contempt order, Manning was released from incarceration on that date. On May 8, 2019, however, Manning was served with a second subpoena to appear

before another grand jury empaneled in the Eastern District of Virginia. In connection with this subpoena, The Honorable Anthony J. Trenga, another federal judge who sits on the United States District Court for the Eastern District of Virginia, and the Department of Army again issued orders granting Manning with use immunity. Judge Trenga oversaw the second grand jury that Manning was called to testify before.

151. After being served with the second subpoena, Manning publicly announced that she would not testify in front of the grand jury and informed prosecutors, through counsel, that she would refuse to answer the same questions posed to her in her prior grand jury appearance. The prosecutors therefore scheduled a hearing with Judge Trenga on May 16, 2019.

152. The day before the hearing, Manning filed two motions, including a Motion to Quash. As relevant here, Manning sought to quash the grand jury subpoena on the ground that prosecutors were improperly using the grand jury proceedings to prepare for trial on an already indicted defendant, Julian Assange. On April 11, 2019, after Assange was arrested, the United States unsealed an indictment charging him with one count of conspiracy to commit computer intrusion.

153. To refute Manning's argument while also maintaining grand jury secrecy, the prosecutors submitted an ex parte pleading that described for Judge Trenga the nature of the grand jury's ongoing investigation. This pleading demonstrated that Manning's testimony was directly relevant to an ongoing investigation into charges or targets that were not included in the pending indictment. Due to the grand jury secrecy rules, this pleading remains under seal, and I cannot disclose its contents.

154. At the hearing on May 16, 2019, Judge Trenga heard argument on Manning's motions and denied both of them. Judge Trenga then questioned Manning directly to determine

whether she would testify in front of the grand jury. Manning clearly and unequivocally stated that she would not testify in front of the grand jury, despite Judge Trenga's order that she do so. Manning claimed that she objected on principle to the grand jury system and that imprisonment would not compel her to testify. Judge Trenga found that Manning did not have just cause to refuse to testify and held her in civil contempt. Judge Trenga ordered that Manning be incarcerated until she purges herself of her contempt or for the life of the grand jury, but in no event to exceed 18 months. Judge Trenga also directed that Manning pay a conditional fine of \$500 per day after 30 days from the issuance of his order, if she still had not complied by that time. *See id.* Judge Trenga further directed that, if Manning still had not complied within 60 days of the order, the fine would increase to \$1000 per day. *See id.*

155. Two weeks later, on May 31, 2019, Manning filed a motion requesting that Judge Trenga reconsider the sanctions. She argued that the sanctions were improper and that the superseding indictment returned against Assange on May 23, 2019, had eliminated the need for her testimony. In opposing Manning's motions, the prosecutors filed with Judge Trenga another ex parte pleading that explained why Manning's testimony remained relevant and essential to an ongoing investigation into charges or targets that are not included in the superseding indictment against Assange. On August 5, 2019, Judge Trenga issued an order denying Manning's motion to reconsider. Even though she had the right, Manning did not appeal Judge Trenga's rulings.

156. As of this filing, Manning continues to refuse to comply with the court's order to testify in front of the grand jury and therefore remains incarcerated and incurring fines.

D. Response To Boyle's Conclusions

157. In his statement, Boyle reaches (at 25-26) two principal conclusions. First, Boyle argues (at 25) that Manning will never testify and, as a result, "her continued confinement is now

punitive and consequently has become an abuse of the grand jury process.” Second, Boyle argues (at 25) that Manning was improperly subpoenaed before the grand jury “to gather evidence for use at Assange’s criminal trial and/or to get a preview of Manning’s trial testimony, should she be called as a defense witness.” As explained below, Boyle’s opinions are unpersuasive.

158. As an initial matter, Manning’s grand jury subpoena, refusal to testify, and subsequent confinement for contempt have little or no bearing on this extradition proceeding. If this information is being submitted to demonstrate that Assange is being prosecuted unfairly or some type of abuse of process, it should be noted that subpoenaing convicted defendants, such as Manning, to obtain additional evidence about criminal conduct in which they may have been involved is a common occurrence, as is holding recalcitrant witnesses in contempt. If anything, the history of Manning’s guilty plea, subsequent conviction on other counts, pardon, and litigation over her grand jury testimony demonstrate the extraordinary level of due process which she has been accorded.

159. In any event, Boyle is unqualified to render his opinions. His own affidavit reflects that he was not involved in Manning’s grand jury proceedings. As a nonparticipant, Boyle lacks the necessary facts to opine on whether Manning was properly subpoenaed before the grand jury. Boyle is not privy to the purpose and direction of the grand jury’s investigation, or the reasons why Manning has been subpoenaed to testify. Without this knowledge, Boyle lacks the critical information necessary to assess whether Manning’s grand jury testimony was properly sought. Because Boyle’s allegations of impropriety necessarily rest on conjecture, his opinions are not entitled to any weight.

160. In contrast, as a government attorney who was involved in Manning's grand jury litigation, I am privy to the information necessary to assess whether her grand jury testimony was properly sought. Unlike Boyle, I know the purpose and direction of the grand jury's investigation, and the reasons why Manning has been subpoenaed to testify. In this setting, however, the law on grand jury secrecy precludes me from divulging any matters that occurred or are occurring before the grand jury. *See* Fed. R. Crim. P. 6(e)(2)(B). Still, I am able to represent the following: Manning was lawfully subpoenaed by a grand jury to testify in connection with a legitimate, ongoing criminal investigation, and the United States did not subpoena Manning to testify for the sole or dominant purpose of preparing for trial on an already pending indictment.

161. Further, Manning extensively litigated the propriety of the grand jury subpoenas in the United States courts. As previously described, she challenged the subpoenas in front of two different federal judges who sit on the United States District Court for the Eastern District of Virginia—Judge Hilton and Judge Trenga. Manning had the opportunity to appeal their rulings to the United States Court of Appeals for the Fourth Circuit, and she did so once. On each of these occasions, the United States courts rejected Manning's arguments challenging the propriety of the grand jury subpoenas.

162. Boyle's opinions simply rehash arguments that Manning made in the United States courts. As discussed above, after prosecutors subpoenaed Manning to appear before the grand jury in May 2019, Manning filed a Motion to Quash the subpoena. *See* Motion to Quash Grand Jury Subpoena, *United States v. John Doe 2010R03793*, No. 1:19-dm-00012-AJT-2 (E.D. Va. May 16, 2019) (Dkt. No. 7). In that motion, Manning made the same argument raised by Mr. Boyle—that prosecutors were improperly using the grand jury process in an attempt to obtain

evidence to use against Assange at trial. *Id.* at 5-8. We opposed Manning's motion and filed an ex parte motion with the court "show[ing] her testimony is directly relevant and important to an ongoing investigation into charges or targets that are not included in the pending indictment." Gov't's Resp. in Opp'n to Chelsea Manning's Mots. to Quash and for Disclosure of Electronic Surveillance, at 1-2, *United States v. John Doe 2010R03793*, No. 1:19-dm-00012-AJT-2 (E.D. Va. May 16, 2019) (Dkt. No. 5). After receiving this information and hearing argument, Judge Trenga denied Manning's motion in its entirety. *See Order, United States v. John Doe 2010R03793*, No. 1:19-dm-00012-AJT-2 (E.D. Va. May 16, 2019) (Dkt. No. 9).

163. Likewise, Judge Trenga has rejected the argument that Manning's confinement is impermissibly punitive. At Manning's May 16, 2019 contempt hearing, her attorney argued that her continued confinement would be impermissibly punitive. *See Tr. of Hr'g*, at 9-13, *United States v. John Doe 2010R03793*, No. 1:19-dm-00012-AJT-2 (E.D. Va. June 13, 2019) (Dkt. No. 18). Judge Trenga rejected Manning's argument and ordered her confinement. *See id.* at 23-26. After the hearing, Manning moved for Judge Trenga to reconsider the civil-contempt sanctions that he imposed, arguing again that she would never testify and therefore the civil-contempt sanctions had become impermissibly punitive. *See Motion to Reconsider Sanctions*, at 3-9, *United States v. John Doe 2010R03793*, No. 1:19-dm-00012-AJT-2 (E.D. Va. May 31, 2019) (Dkt. No. 14). Judge Trenga again denied Manning's motion. *See Order, United States v. John Doe 2010R03793*, No. 1:19-dm-12-AJT-2 (E.D. Va. Aug. 5, 2019) (Dkt. No. 28).

164. Because Boyle's legal opinions have already been litigated and rejected in the United States courts, they should be afforded no weight here.

165. Finally, Assange will have an opportunity to raise arguments related to the improper use of the grand jury system in the United States. Federal courts retain supervisory

authority to address allegations of grand jury abuse, *see Calandra*, 414 U.S. at 346, and they may take remedial action when prosecutors have engaged in grand jury abuse, *see Alvarado*, 840 F.3d at 189; (*Under Seal*), 714 F.2d at 351. For example, if a defendant proves that prosecutors improperly used the grand jury for the sole or dominant purpose of preparing for trial, the district court can preclude prosecutors from using that evidence at trial. *See Alvarado*, 840 F.3d at 189-90; *United States v. Leung*, 40 F.3d 577, 581 (2d Cir. 1994). In addition, a defendant may seek dismissal of an indictment by establishing that “the violation substantially influenced the grand jury’s decision to indict, or . . . there is grave doubt that the decision to indict was free from the substantial influence of such violations.” *Bank of Nova Scotia v. United States*, 487 U.S. 250, 256 (1988) (quoting *United States v. Mechanik*, 475 U.S. 66, 78 (1986)) (internal quotation marks omitted). While I am confident that prosecutors did not engage in grand jury abuse and these arguments would not have a meritorious basis, the point is that Assange will have a forum in the United States courts to raise his allegations.

VI. Assange’s Actions Unambiguously Constituted a Conspiracy to Violate the Computer Fraud and Abuse Act

166. Assange argues that the “[t]he password hash ‘conspiracy’ amounts (at its highest) to a bare request from Manning, with no evidence of agreement, or information being sent.” Defense, Summary of Issues ¶ 6. As an initial matter, the Superseding indictment explicitly alleges that “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, a United States government network used for classified documents and communications.” Superseding Indictment ¶ 15 (emphasis added). Upon Assange’s extradition, we intend to prove this agreement, beyond a reasonable doubt, through a variety of evidence, including “electronic messages Manning sent to and received from ASSANGE using her personal computer.” *See*

Affidavit in Support of Request for Extradition of Julian Paul Assange, sworn out by one of my colleagues on June 4, 2019 (hereinafter referenced as the "June 14th Affidavit"), at ¶ 88(a).

167. These electronic messages are described extensively in the affidavit that was submitted to the U.S. court by an FBI Special Agent, in support of the initial criminal complaint in this case.⁵ In these electronic messages, Manning asked Assange whether he was good at “hash-cracking” to which Assange replied “yes.” A password “hash” refers to a password that for security has been converted via an algorithm from its original plain text into a string of numbers and letters. “Hash-cracking” refers to the process of attempting to glean the original plain text password from its corresponding password hash. Assange responded, “yes,” indicating he was good at hash-cracking and stated that he had “rainbow tables,” which are tools used to crack password hashes. Manning then provided Assange with a password hash and indicated that she had taken the hash from the “SAM” or Systems Account Manager, a reference to the location where Microsoft’s operating system stored hashed passwords at the time. Assange then asked Manning questions about the password hash in order to help Assange crack it, such as “any more hints about this lm ... no luck so far.” A more detailed account of this exchange is described at paragraphs 86-92 of the affidavit submitted in support of the initial criminal complaint in this case.

168. Cracking the password hash could have allowed Manning to log onto a classified Department of Defense account under a username that did not belong to her, thus making it “more difficult for investigators to identify Manning as the source of disclosures of classified information.” June 14th Affidavit, ¶ 87. Based on this, Assange asserts that “[t]he object alleged

⁵ The affidavit is publicly available through PACER, <https://www.pacer.gov> (as explained above, in Note 2), as Docket Item #2 in the case *United States v. Assange*, 1:18cr111.

was not to gain unauthorised access but to cover tracks.” Summary of Issues ¶ 6. This misses the point. The object was to gain unauthorized access to a classified Department of Defense account. The larger goal such unauthorized access furthered was to obscure Manning’s identity so that she could continue to steal classified documents on behalf of Assange. *See* June 14th Affidavit ¶ 87 (“the purpose of ASSANGE’s password hash-cracking agreement with Manning was to enable Manning to continue to steal classified documents from the United States to provide to ASSANGE with less risk of being detected by the United States.”).

169. In his affidavit, Carey Shenkman suggests that the Computer Fraud and Abuse Act (CFAA) is unconstitutionally vague. Shenkman Aff. ¶¶ 35, 40-41. In fact, the CFAA’s basic prohibition against intentionally gaining access to a computer “without authorization,” Title 18, United States Code, Section 1030(a)(1), is common throughout the world. *See* Council of Europe, Convention on Cybercrime, Sec. 1, Art. II (“Each party shall ... establish as criminal offenses under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A party may require that the offense be committed by infringing security measures, with the intent of obtaining computer data...”); ORIN S. KERR, *COMPUTER CRIME LAW* 40 (4th ed. 2018) (“Every state and the federal government has an unauthorized access statute.”). Indeed, as noted in the Opening Note, the United Kingdom’s Computer Misuse Act similarly prohibits “Unauthorised access to computer material.” Opening Note ¶ 57.

170. In an attempt to make CFAA appear unclear and arbitrary, Shenkman points to a disagreement among U.S. courts as to whether CFAA applies to individuals who have authorized access to a computer system, but abuse that authorization by accessing information for a purpose prohibited by the entity that owns the computer system. *See* Shenkman Aff. ¶45 n.146-47.

Similarly, Shenkman quotes Professor Orin Kerr, a leading U.S. scholar, as suggesting that CFAA is “so ‘extraordinarily broad’ that without limitation it is unconstitutionally vague.” *Id.* ¶ 35 (quoting Orin Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561 (2010)). But the Kerr article, upon which Shenkman relies, refers to the same dispute referenced above: whether CFAA applies to individuals who have authorized access to a computer system, but exceed the scope of that authorization and use that access for a purpose that is prohibited by the computer’s owner. *See* Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1562 (2010). Kerr merely argues that CFAA would be unconstitutionally vague *if* it were applied to such individuals. *Id.* at 1572. But Kerr acknowledges that there are some “obvious” violations of CFAA, such as when one intentionally obtains and uses the password of another to access an account without permission. *See id.* at 1576 (“To be sure, there are some obvious cases. If A guesses B’s password, and logs into B’s email account to read B’s email, A’s access to the computer is clearly unauthorized.”); *see also* KERR, *COMPUTER CRIME LAW*, at 49 (“circumvention of code-based restrictions to a computer constitutes ‘access without authorization’”).

171. Agreeing and attempting to obtain access to a password in order to access an account without authorization is precisely what Assange has been charged with in this case. Assange has been charged with conspiring to crack (Count 18) and attempting to crack (Count 5) a password hash to an account on a classified U.S. Department of Defense computer system. There is no question that neither Assange nor Manning was authorized to access this account—that is the whole reason why they needed to crack a stolen password hash in the first place. Circumventing a technical restriction on authorization to a computer system is the paradigmatic example of “unauthorized access.” *See* KERR, *COMPUTER CRIME LAW*, at 48 (“Indeed, bypassing

password gates using stolen or guessed passwords is a common way to ‘hack’ into a computer.”) Any uncertainty about how CFAA might apply in completely different circumstances has no application here.

172. Assange has retained a forensic expert who submitted a long forensic report challenging the evidence in support of the hacking charge. *See* Affidavit of Patrick Eller of Metadata Forensics, LLC. The crux of Eller’s affidavit seems to be that it would have been very difficult, if not impossible, for Assange’s hash-cracking agreement to achieve its ultimate purpose of assisting Manning in the theft of national security information. But it is well-settled that impossibility is not a defense to a conspiracy charge. *See United States v. Jimenez Recio*, 537 U.S. 270, 272, 275 (2003); *United States v. Min*, 704 F.3d 314, 321 (4th Cir. 2013). Eller also suggests that Manning and Assange’s hash-cracking agreement might have been simply for “technical curiosity” or “potential business opportunities.” Eller Aff. ¶ 78. Whether Assange agreed to help Manning crack a password hash for the reasons Eller suggests or to help Manning gain unauthorized access to a U.S. government account in order to steal classified documents is a question for a jury to decide after hearing all the evidence from both sides.

VII. No Privileged Materials Related to Assange Will Be Used in this Case

173. I am aware of an allegation that a Spanish citizen, David Morales Guillen, and the Spanish company UC Global, carried out acts that allegedly impinged on the privacy of Assange, and on the privacy of his lawyers, by placing bugging devices and other means inside the Embassy of the Republic of Ecuador in London, allegedly without the consent of those affected. I am aware of the further allegation that Guillen and UC Global provided the information thus obtained to third parties or institutions, including agents of the government of

the United States. Finally, I am aware that these allegations are being investigated under the direction of a judge in Spain.

174. I am not in a position to confirm or deny the allegations described above. I can, however, assure this Court that, if Assange is extradited to the United States, no privileged conversations between Assange and his lawyers or doctors will be used against him. I also can confirm that, if the fruits of any surveillance of Assange in the Embassy exist (and regardless of who undertook that surveillance), the prosecutors assigned to this case will not review or use any privileged communications.

175. Moreover, even were this court to assume, arguendo, the truth of the allegations under investigation in Spain, any use of privileged information against Assange would be barred by American law. In courts of the United States, the confidences of wrongdoers made to their attorneys with respect to past wrongdoing are protected by the attorney-client privilege. *See United States v. Zolin*, 491 U.S. 554, 562 (1989). In U.S. federal courts, “[t]he common law—as interpreted by United States courts in the light of reason and experience—governs a claim of privilege,” unless a contrary statute, constitutional provision, or Supreme Court rule applies. Federal Rule of Evidence 501. The United States Supreme Court has recognized the attorney-client privilege under federal law as “the oldest of the privileges for confidential communications known to the common law.” *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981). It exists “to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice.” *Id.* The Supreme Court has recognized that attorney-client privilege requires that clients be free to “make full disclosure to their attorneys” of past wrongdoings, *Fisher v. United States*,

425 U.S. 391, 403 (1976), in order that the client may obtain “the aid of persons having knowledge of the law and skilled in its practice,” *Hunt v. Blackburn*, 128 U.S. 464, 470 (1888).

176. U.S. federal courts also protect confidential communications made in the course of diagnosis or treatment between a patient and his licensed psychiatrist, psychologist, or social worker. *Jaffee v. Redmond*, 518 U.S. 1 (1996). In recognizing this common law privilege, the United States Supreme Court has noted, “[l]ike the spousal and attorney-client privileges, the psychotherapist-patient privilege is rooted in the imperative need for confidence and trust” as effective psychotherapy “depends upon an atmosphere of confidence and trust in which the patient is willing to make a frank and complete disclosure of facts, emotions, memories, and fears.” *Id.* (quotations omitted).

177. Finally, the U.S. Department of Justice has established procedures to prevent agents and prosecutors from receiving and viewing privileged materials related to matters they are investigating or prosecuting. In any case in which privileged communications are inadvertently obtained during an investigation, a team of lawyers and investigators, separate from the prosecution team, is established to protect the privacy of such information. This separate team, known as a “filter” team, identifies potentially privileged material (or information to which the prosecution team arguably is not entitled) and separates it, to ensure that the prosecution team receives only non-privileged and unprotected information. The filter team may attempt to resolve questions of potential privilege through negotiation with a defendant’s lawyers or litigation and will create a record to establish what steps were taken with the materials in question.

178. If Assange comes to believe that any evidence offered by the United States during any criminal proceedings in the United States was based on privileged material, he could move the court to have such evidence excluded. *See* Federal Rule of Criminal Procedure 12(b)(3)

(motions to suppress evidence should be filed prior to trial); Federal Rule of Evidence 1101(c) (“The rules on privilege apply to all stages of a case or proceeding.”). Like all other motions Assange might make if extradited to the United States, this motion would be considered by an independent judge and could be the subject of an appeal.

VIII. U.S. Courts Ensure That Guilty Pleas Are Knowing, Voluntary, and Supported By The Facts

179. The United States Supreme Court has explained that “a guilty plea is a grave and solemn act to be accepted only with care and discernment.” *Brady v. United States*, 397 U.S. 742, 748 (1970). A guilty plea is valid only if done voluntarily, knowingly, and intelligently, with sufficient awareness of the relevant circumstances and likely consequences. *Id.*

180. In order for a guilty plea to be valid, the U.S. Constitution imposes the minimum requirement that a guilty plea be the voluntary expression of the defendant’s own choice. *Id.* It must reflect “a voluntary and intelligent choice among the alternative courses of action open to the defendant.” *North Carolina v. Alford*, 400 U.S. 25, 31 (1970). Accordingly, and pursuant to Rule 11(b)(2) of the Federal Rules of Criminal Procedure, a trial court is required to ensure that a guilty plea is made voluntarily, and not as a result of force, threats, or promises made by the government that are not part of a plea agreement disclosed to the court.

181. Assange suggests that, if brought to the United States, the plea bargaining system will compel him to plead guilty regardless of the facts of his case. To the contrary, the principle is long accepted in the United States that a guilty plea must provide a trustworthy basis for believing that the defendant is, in fact, guilty. *Henderson v. Morgan*, 426 U.S. 637, 651-52 (1976) (White, J., concurring). Accordingly, Rule 11(b)(3) of the Federal Rules of Criminal Procedure prohibits a U.S. federal court from entering a judgment upon a guilty plea without determining that there is a factual basis for such a plea. Thus, before accepting a guilty plea, a

court must make clear exactly what a defendant admits to, and whether those admissions are factually sufficient to constitute the alleged crime. *United States v. DeFusco*, 949 F.2d 114, 116, 120 (4th Cir. 1991). In short, Assange will not be allowed to plead guilty unless he agrees that he is guilty, and a district judge finds a trustworthy factual basis for his guilty plea.

IX. Facts Relevant To Estimating the Potential Sentence In This Case

182. Eric Lewis alleges in his affidavit that Assange is “highly likely to be sentenced to imprisonment that will constitute the rest of his likely natural lifespan.” Lewis Aff. ¶ 47. Mr. Lewis’s affidavit suffers from critical flaws. For one, Lewis heavily relies on the statutory maximum of 175 years, without acknowledging that only a tiny fraction of all federal defendants receive statutory maximum sentences.

183. The law that controls sentencing in federal courts in the United States sentence is 18 U.S.C. 3553. Pursuant to that statute, the court shall impose a sentence sufficient, but not greater than necessary, to comply with the need for the sentence imposed to (a) reflect the seriousness of the offense, promote respect for the law, and provide just punishment for the offense; (b) afford adequate deterrence to criminal conduct; (c) protect the public from further crimes of the defendant; and (d) provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner.

184. In determining the particular sentence to be imposed, the district court shall consider the following factors:

- (1) the nature and circumstances of the offense and the history and characteristics of the defendant;
- (2) the need for the sentence imposed to --
 - (a) reflect the seriousness of the offense, promote respect for the law, and provide just punishment for the offense;

- (b) afford adequate deterrence to criminal conduct;
 - (c) protect the public from further crimes of the defendant; and
 - (d) provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner;
- (3) the kinds of sentences available;
- (4) the kinds of sentence and the sentencing range established for the applicable category of offense committed by the applicable category of defendant as set forth in the guidelines issued by the U.S. Sentencing Commission and any pertinent policy statement issued by the U.S. Sentencing Commission;
- (5) the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and
- (6) the need to provide restitution to any victims of the offense.

After weighing each of these factors, the sentencing court will arrive at an appropriate sentence. This determination is within the sentencing court's broad discretion and is subject to appellate review under a reasonableness standard or for any procedural defects.

185. As noted above, a key factor to be considered by a sentencing court in the United States is the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct. Lewis relies heavily on the sentence initially imposed on Manning, but fails to account for the key fact that, while parole is unavailable in the federal civilian justice system, defendants with sentences of more than a year of incarceration in the military system generally are considered for parole after serving a third of their sentence. As a result, a sentence imposed in a military court of a term of years of imprisonment tends, in practical terms, to be the equivalent of a much lower term of years of imprisonment imposed in a federal civilian court. Moreover, Manning's sentence was, in any event, commuted to a term much shorter than what was originally imposed. Accordingly, the sentence imposed on Manning by the military judge will be of limited use as a factor of

consideration for a judge considering the appropriate sentence for Assange. Instead, in seeking to avoid an unwarranted sentence disparity for Assange, his sentencing judge likely will consider sentences recently imposed in U.S. civilian courts for unauthorized disclosures of classified information to the media. *See United States v. Sterling*, 860 F.3d 233 (4th Cir. 2017) (sentenced to 42 months); *United States v. Albury*, 18-cr-00067-WMW (D. Minn. Oct. 26, 2018) (sentenced to 48 months); *United States v. Winner*, 17-cr-00034-JRH-BKE (S.D. Ga. Aug. 24, 2018) (sentenced to 63 months).

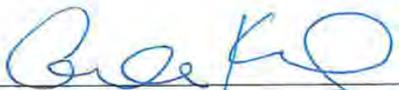
186. Lewis also fails to note that sentences above the range calculated by the United States Sentencing Guide are very rare. The sentencing court has the ability to sentence a defendant above the recommended sentencing guidelines range, but such above-guidelines sentences are rare. According to the United States Sentencing Commission, in 2018, out of 68,902 sentences for which data was collected, sentencing courts imposed sentences within the guidelines range in approximately 51% of cases, below the guidelines range in approximately 46% of cases, and above the guidelines range in approximately 3% of cases. 2018 Datafile, US Sentencing Commission FY18, <https://www.ussc.gov/sites/default/files/pdf/research-and-publications/annual-reports-and-sourcebooks/2018/Table29.pdf>.

187. If a defendant is convicted of multiple offenses, the sentencing court may run the sentences concurrently or consecutively. *See* 18 U.S.C. § 3584(a). The terms may not run consecutively for an attempt and for another offense that was the sole objective of the attempt. *Id.* The court is to follow the factors listed in section 3553(a) in determining whether to impose concurrent or consecutive terms. *See* § 3584(b). None of the offenses charged in the superseding indictment requires imposition of a consecutive or mandatory minimum sentence.

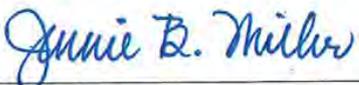
188. In short, it is difficult to estimate a possible sentence at this early stage of a criminal proceeding. There are many factors that contribute to the imposition of an actual sentence, and it is difficult to address every conceivable permutation that could occur.

Conclusion

189. The facts and information contained in this Declaration in Support of the Request for the Extradition of Julian Paul Assange are true and correct according to the best of my knowledge, information, and belief.


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

SUBSCRIBED and SWORN to before me
this 17th day of January 2020.



Notary Public

My commission expires 6/30/2020
Alexandria, Virginia



**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

**SUPPLEMENTAL DECLARATION IN SUPPORT OF REQUEST FOR
EXTRADITION OF JULIAN PAUL ASSANGE**

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

1. I am a citizen of the United States.

2. I am an Assistant United States Attorney in the Eastern District of Virginia, and have been so employed since 1991. I received my Bachelor's degree from Princeton University in 1979, and a Juris Doctor degree from New York University School of Law in 1982. Before joining the United States Attorney's Office, I served as a trial attorney in the United States Department of Justice, and as a defense attorney in the United States Army's Judge Advocate General's Corps. My duties as an Assistant United States Attorney include the prosecution of persons charged with violations of the criminal laws of the United States, including laws prohibiting computer intrusion and mishandling of national security information. For my work as an Assistant United States Attorney, I have received various awards, including the Attorney General's Award for Excellence in Furthering the Interests of U.S. National Security, and, on three separate occasions, the FBI Director's Award for Outstanding Counterterrorism Investigation. Based on my training and experience, I am an expert in the criminal laws and procedures of the United States.

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 United States District Court for the Eastern District of Virginia. I make this declaration for the limited purpose of providing additional information relevant to several objections that Assange has made to this U.S. request for his extradition. The statements in this declaration are based on my experience, training, and research, as well as information provided to me by other members of the U.S. government, including members of the Federal Bureau of Investigation (FBI), the United States Department of Justice, and other federal agencies.

4. This declaration does not respond to every assertion or allegation made in the defense case. I understand that a number of the defense's allegations can be answered by reference to matters which have already been decided as a matter of extradition law in the United Kingdom. If I have not addressed a matter in this declaration, it should not be regarded as an acceptance of its accuracy or its truthfulness.

I. There Has Been No Abuse of Process

5. I understand that attorneys for Julian Paul Assange (hereinafter, "Assange") have made a number of claims alleging that privileged communications have been collected by the United States. As I stated in my previous declaration, paragraph 175, no privileged conversations between Assange and his lawyers or doctors will be used against him. I add that to the best of my knowledge, information, and belief, the allegations in the superseding indictment and the affirmations made in the affidavits or declarations submitted by the United States in support of this extradition request contain no legally privileged material, and were not derived from legally privileged material. I make this statement, however, above what the law requires. While privileged evidence cannot be introduced against Assange at any trial, the suppression of evidence

derived from privileged information is proper only if the privilege is constitutionally based and not a testimonial or evidentiary privilege. *United States v. Squillacote*, 221 F.3d 542, 560 (4th Cir. 2000). Assange is not, therefore, entitled to a hearing to require the government to establish an independent legitimate source for any disputed evidence.

6. In an unsigned statement submitted on or around January 13, 2020, Gareth Peirce alleged that materials belonging to Assange were taken from the Ecuadorian Embassy in London at the time of Assange's arrest, and that some of those materials were privileged and/or necessary to assist Assange in defending against the superseding indictment. *See* Second Statement of Gareth Peirce ¶¶ 6-12. I can again assure the Court that, as required by American law, no privileged materials will be used against Assange during criminal proceedings in the United States. Moreover, as I noted in paragraph 177 of my previous declaration, pursuant to established U.S. Department of Justice procedures, any potentially privileged materials in the possession of the Department of Justice are reviewed by a team of lawyers and investigators, separate from the prosecution team. This separate team, known as a "filter" team, is responsible for resolving questions of potential privilege through discussions with Assange's lawyers or litigation before an impartial judge and for creating a record to establish the steps taken with respect to any materials deemed to be privileged.

7. Finally, as discussed in Section IV of my prior declaration, Assange and his lawyers will have access to information in the possession of the prosecution team as required by the rules, laws and constitution of the United States, including evidence relevant and material to Assange's defense. *See, e.g.*, Fed. R. Crim. P. 16, Fed. R. Crim. P. 26.2; 18 U.S.C. § 3500; *Brady v. Maryland*, 373 U.S. 83 (1963); *Giglio v. United States*, 405 U.S. 150 (1972); *United States v. Abu Ali*, 528 F.3d 210, 248 (4th Cir. 2008) ("[T]he government may protect classified information from

disclosure, but if the district court determines, in the exercise of its discretion, that an item of classified information is relevant and material to the defense that item must be admitted unless the government provides an adequate substitution.”) (internal quotations omitted).

II. *Zakrzewski* Abuse of Process

8. In his affidavit, Patrick Eller, a forensic examiner retained by lawyers for Assange, faults the United States for stating in the superseding indictment, “Manning provided ASSANGE with part of a password hash stored on United States Department of Defense computers connected to the Secret Internet Protocol Network.” Superseding Indictment, Count 18, Overt Act 2. Eller asserts that this falsely implies, “the password hash itself is broken up and split between the SAM and system file,” whereas, in fact, the password hash “is stored in full in the SAM file, but encrypted with a key (which is not part of the hash) generated from data in the SAM file and system file.” Eller Aff. ¶ 32. Thus, Eller believes it is more accurate to say that Manning provided Assange with an “encrypted hash” rather than “a portion of a hash.” Eller ¶ 65. Eller is correct that password hashes stored on the Security Accounts Manager (SAM) file are encrypted and that what Manning provided Assange was the hash as stolen from a SAM file. The superseding indictment used the term “portion of a hash” to make clear that—ordinarily—one would need more than what Manning gave Assange in order to derive the password hash. *See* Superseding Indictment ¶ 18 (“Had Manning retrieved the full password hash and had ASSANGE and Manning successfully cracked it, Manning may have been able to log onto computers under a username that did not belong to her.”).

9. It is not clear that anything turns on whether one calls what Manning gave to Assange a “part of a password hash” or an “encrypted hash.” It appears that Eller’s point is to suggest that it was not possible for Assange and Manning’s hash-cracking agreement to succeed.

Although we do not concede that the success of the conspiracy was impossible, I again note that impossibility is not a defense to conspiracy. See *United States v. Jimenez Recio*, 537 U.S. 270, 272, 275 (2003).

10. In the “Summary of Issues” submitted to this Court on December 17, 2019, Assange’s attorneys asserted, “Under US law, receipt/publication of classified information is lawful (*Bartnicki v Vopper* (2001) 532 US 514) and illegality only arises if the publisher actually participated in illegality in obtaining the material.” Assange Statement of Issues ¶ 12. But *Bartnicki* - - the authority upon which Assange relies for this assertion - - had nothing to do with the publication or receipt of classified information. In *Bartnicki*, the United States Supreme Court held that the First Amendment protected a publisher’s disclosure of the contents of an illegally intercepted telephone conversation. See *id.* at 535. The illegally intercepted telephone conversation at issue in that case related to a dispute between a teachers’ union and a school board. See *id.* at 518-19. *Bartnicki* did not involve classified information, much less classified information that is related to the national defense of the United States - - and that discloses the names of sources - - which the United States has charged Assange with disclosing. As I explained in paragraphs 8 and 9 of my previous declaration, the First Amendment generally does not protect the intentional outing of classified intelligence sources.

11. *Bartnicki* is distinguishable from this case in another important respect. As the Supreme Court observed in *Bartnicki*, the publisher at issue in that case “played no part in the illegal interception.” *Id.* at 525. Instead, the publisher “found out about the interception only after it occurred” and “never learned the identity of the person or persons who made the interception.” *Id.* Moreover, the publisher’s “access to the information was obtained lawfully,” *id.*, that is, no law prohibited the publisher from receiving the intercept. In fact, the Supreme Court emphasized

that its “holding . . . does not apply to punishing parties for obtaining the relevant information unlawfully.” *Id.* at 532 n.19. In contrast, as alleged in the superseding indictment, Assange was complicit in the illegal acts to obtain or receive the classified documents, and he agreed and attempted to obtain classified information through computer hacking. As I explained in paragraph 7 of my previous declaration, the First Amendment did not protect Assange in engaging in such conduct.

12. In the same “Statement of Issues,” Assange’s attorneys asserted, “[t]he allegations that Manning’s disclosures were connected to the WikiLeaks ‘most wanted list’ is again flatly contradictory to the evidence,” and “Manning’s ultimate transmission of data does not, in fact, correlate to any suggested agreement, nor does what was sent by Manning correlate to what Assange is alleged to have sought.” Assange Statement of Issues ¶ 12. To the contrary, as summarized in the affidavit of Kellen S. Dwyer in support of extradition, dated June 4, 2019, Manning searched classified databases for information responsive to Assange’s solicitations contained in WikiLeaks’s “Most Wanted Leaks”:

- a. According to forensic evidence obtained from U.S. DoD computers, beginning in 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, solicited CIA detainee interrogation videos. On November 28, 2009, according to forensic evidence obtained from U.S. DoD computers, Manning searched “Intelink,” a classified U.S. DoD network search engine, 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. *See* Dwyer Aff. ¶ 19.
- b. On December 8, 2009, according to forensic evidence obtained from U.S. DoD computers, 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. *See* Dwyer Aff. ¶ 20.

13. Moreover, many of the classified document sets that Manning in fact stole from the U.S. government and provided to Assange were consistent with the materials Assange solicited through the WikiLeaks website and its “Most Wanted Leaks.” For instance, consistent with WikiLeaks’s “Most Wanted Leaks” solicitation of “Iraq and Afghanistan U.S. Army Rules of Engagement 2007-2009 (SECRET),” Manning stole and transmitted to Assange multiple rules of engagement files. Dwyer Aff ¶ 33. Similarly, consistent with WikiLeaks’s solicitation of bulk databases of “classified, censored, or otherwise restricted material of political, diplomatic, or ethical significance,” between on or about March 28, 2010, and April 9, 2010, Manning used a United States Department of Defense computer to download over 250,000 U.S. Department of State cables, which she subsequently provided to Assange. Dwyer Aff. ¶ 12.

III. Response re: Wiley Declarations Regarding Prison Conditions

14. I have reviewed three different declarations signed by R. Wiley. At the time he signed these affidavits, Mr. Wiley was the Warden at the United States Department of Justice, Federal Bureau of Prisons (“BOP”) facility known as the United States Penitentiary, Administrative Maximum (“ADX”), which is located in Florence Colorado. These declarations were filed in the following extradition matters: *United States v. Abu Hamza* (Magistrate Court at Westminster Oct. 3, 2007); *United States v. Syed Talha Ahsan*, 3:06CR194(JCH) (D. Conn. May 11, 2009); and *United States v. Khalid Al Fawwaz*, S(10) 98 Cr. 1023(KTD) (S.D.N.Y. Dec. 6, 2009) (collectively, the “Wiley Declarations”). In sum and substance, these affidavits described the facilities, policies, and procedures at the ADX.

15. My understanding is that, in large part, the Wiley Declarations continue to describe accurately the conditions at ADX. Of course, the statistics regarding staffing numbers,

inmate numbers, and inmate designations have changed. The overall structure of the ADX is largely unchanged, but enhancements outlined below have since been put in place.

16. Since the last Wiley declaration, the following Program Statements and Institutional Supplements (the “Policies”), which contain substantive provisions regarding, among other matters, screening and diagnosis of mental illness, provision of mental health care, suicide prevention, and conditions of confinement to reduce the risk of development or exacerbation of mental illness have been updated or revised:

- a. Program Statement, *Treatment and Care of Inmates with Mental Illness* (updated for all BOP facilities);
- b. ADX Institutional Supplement, *Treatment and Care of Inmates with Mental Illness*;
- c. ADX Institutional Supplement, *Suicide Prevention Program*;
- d. ADX Institutional Supplement, *Control Unit Programs*;
- e. ADX Institutional Supplement, *General Population and Step-Down Unit Operations*; and
- f. ADX Institutional Supplement, *High Security Adult Alternative Housing Program*.

17. Since the last Wiley declaration, the following general changes have been made to the ADX:

- a. The ADX no longer operates a Special Housing Unit (Z-Unit). The Z-Unit was recently renamed C-Unit and is now one of five (5) general population units;
- b. There are currently five (5) general population units (C, D, E, F, and G);
- c. The Intermediate step of the Step-Down Program is in J/A Unit;
- d. The Transitional and Pre-Transfer steps of the Step-Down Program are in B/A Unit;
- e. The K/A Unit now houses the Reentry Preparation Program Unit; and

- f. The K/B Unit now houses the High Security Adult Alternative Housing Program.
18. Since the last Wiley declaration, the BOP has developed and activated units for mental health treatment at the following institutions:
- a. A secure mental health unit at the United States Penitentiary in Atlanta, Georgia.
 - b. A second secure mental health unit at the United States Penitentiary in Allenwood, Pennsylvania.
 - c. A secure Steps Toward Awareness Growth and Emotional Strength (STAGES) Program at the United States Penitentiary, High Security, in Florence, Colorado, specifically designed for inmates with personality disorders.
19. Since the last Wiley declaration, BOP has undertaken the following initiatives to improve mental health treatment at BOP and, in particular, at the ADX:
- a. Developing and implementing behavior-related incentive programs for inmates housed at ADX;
 - b. Using and enhancing an at-risk recreation program to identify inmates who are not participating in any recreation programs, attempting to educate them on wellness, and encouraging their participation in a structured recreation program;
 - c. Constructing, maintaining, and employing facilities for group therapy at ADX;
 - d. Constructing, maintaining, and employing areas for private psychological and psychiatric counselling sessions in all housing units at ADX;
 - e. Allowing telepsychiatry sessions to take place in private without the presence of correctional officers;
 - f. Screening all inmates housed at ADX as of August 2014, to determine, among other things, whether the inmates have a mental illness. This included a screening record review of all inmates and in-depth clinical interviews of approximately 130 inmates by outside psychiatrists and non-ADX Bureau psychologists;
 - g. Clarifying that psychotropic medications are available to any inmate for whom such medication is prescribed, regardless of the inmate's housing assignment;
 - h. Ensuring that inmates receiving psychiatric medications at the ADX are seen by a psychiatrist, physician, or psychiatric nurse every ninety (90) days, or more often as clinically indicated for, at a minimum, the first year;

- i. Ensuring that during the screening and classification process identifies inmates with mental illnesses, provides accurate diagnoses, and assesses the severity of the mental illness or suicide risk;
- j. Developing and implementing procedures to ensure that Health Services notifies the psychiatrist, psychiatric mid-level provider, psychiatric nurse, or physician and Psychology Services of inmates who refuse or consistently miss doses of their prescribed psychotropic medications;
- k. Requiring Health Services staff to take steps to ensure that psychotropic medications are prescribed so that they are distributed on pill line;
- l. Assessing all inmates at ADX periodically to determine whether mental illness has developed since the last screening;
- m. At the classification stage, using mental health care levels as defined in the Program Statement, *Treatment and Care of Inmates with Mental Illness*;
- n. Excluding certain inmates with a Serious Mental Illness, as defined in the Bureau's Program Statement 5310.16, *Treatment and Care of Inmates with Mental Illness*, from ADX, except when extraordinary security needs exist. When extraordinary security needs exist, ensuring those inmates are provided treatment and care commensurate with their mental health needs, which includes the development of an individualized treatment plan in accordance with the Policies;
- o. Taking steps to ensure the prompt identification of inmates who develop signs or symptoms of possible mental illness while incarcerated at ADX, to permit timely and proper diagnosis, care, and treatment;
- p. Taking steps to ensure the reasonable access to clinically appropriate mental health treatment for all inmates with mental illness at ADX;
- q. Considering a commitment order under 18 U.S.C. § 4245, or other applicable statute or regulation, for inmates who have a need for, but who do not agree to participate in, a Secure Mental Health Unit or for a treatment program at a Medical Referral Center. An inmate's refusal to be designated to a Secure Residential Mental Health Unit or Medical Referral Center, or a court's denial of a commitment order, is not grounds or justification to house an inmate with a Serious Mental Illness at ADX. However, if a court denies commitment or determines that an inmate does not have a Serious Mental Illness, permitting that inmate to be placed at ADX if needed for security and safety reasons and providing treatment commensurate with his mental health care level;
- r. Housing certain inmates in need of inpatient psychiatric care at a Medical Referral Center;
- s. If an inmate with Serious Mental Illness who continues to be housed at ADX due to extraordinary security needs declines treatment consistent with his mental

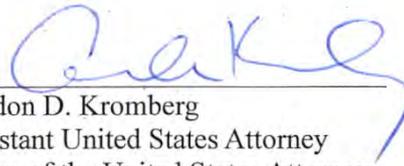
health care level, taking steps to develop and implement a treatment plan that includes regular assessment of the inmate's mental status, rapport-building activities, and other efforts to encourage engagement in a treatment process, and, at a minimum, a weekly attempt to engage the inmate;

- t. Offering inmates with Serious Mental Illness who continue to be housed at ADX due to extraordinary security needs between 10 and 20 hours of out-of-cell therapeutic and recreational time per week consistent with their individualized treatment plan;
- u. Taking steps to support inmates with mental illness through creation of wellness programs and recreational activities, specialized training of staff, and care coordination teams;
- v. Developing procedures for heightened review of requests and referrals for mental health services;
- w. Ensuring that any calculated use of force or use of restraints involving an inmate at ADX with a mental illness is applied appropriately to an inmate with such conditions, as set forth in the Policies;
- x. Excluding mental health clinicians from participation as a use of force team member in a calculated use of force situation, other than for confrontation avoidance.
- y. Merging BOP's Electronic Medical Record (BEMR) and Psychology Data System (PDS);
- z. Staffing and hiring four additional full-time psychologists at ADX, one psychiatric nurse, and one psychology technician, with one of the four additional full-time psychologist positions facilitating trauma-informed psychological programming (Resolve Treatment (Trauma) Coordinator);
- aa. Ensuring that the ADX Care Coordination and Reentry (CCARE) Team meets monthly, pursuant to the applicable section ADX Institutional Supplement regarding *Treatment and Care of Inmates with Mental Illness*;
- bb. Ensuring that a Mental Health Transfer Summary is completed in BEMR/PDS every time an inmate with mental illness (CARE2-MH, CARE3-MH, and CARE4-MH) transfers out of ADX, pursuant to the ADX Institutional Supplement regarding *Treatment and Care of Inmates with Mental Illness*;
- cc. Ensuring the collaboration of Psychology and Health Services staff, beginning no later than 12 months before an inmate's anticipated release with Community Treatment Specialist (CTS) regarding ADX inmates CARE2-MH or higher releasing to an residential re-entry center or home detention, pursuant to the applicable section of the ADX Institutional Supplement regarding *Treatment and Care of Inmates with Mental Illness*;

- dd. Hiring a full-time Social Worker for FCC Florence, whose priority is those inmates housed at ADX and who provides Reentry Planning Services within 1 year of an inmate's projected release date, as appropriate, and pursuant to the applicable section of the ADX Institutional Supplement regarding *Treatment and Care of Inmates with Mental Illness*;
- ee. Taking steps to ensure that discipline is applied appropriately to inmates with Serious Mental Illnesses or Mental Illness, as set forth in the Policies; and
- ff. Enhancing mental health training provided to Bureau staff.

Conclusion

20. The facts and information contained in this Supplemental Declaration are true and correct according to the best of my knowledge, information, and belief.


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



Jennie B. Miller
2/19/2020

**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

**SECOND SUPPLEMENTAL DECLARATION IN SUPPORT OF
REQUEST FOR EXTRADITION OF JULIAN PAUL ASSANGE**

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

1. I have made two 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 those previous declarations. *See* Gordon Kromberg, Declaration in Support of Request for Extradition of Julian Paul Assange ¶¶ 1-4 (Jan. 17, 2020) (hereafter, “First Declaration”); Gordon Kromberg, Supplemental Declaration in Support of Request for Extradition of Julian Paul Assange ¶¶ 1-3 (Feb. 19, 2020) (hereafter, “Second Declaration”).

2. This declaration responds to certain of the defense’s allegations raised before this Court, but it does not respond to all of them. I understand that a number of the defense’s allegations can be answered by reference to matters that have already been decided as a matter of extradition law in the United Kingdom or by argument from facts in the record before the Court. If I have not addressed a matter in this declaration, it should not be regarded as an acceptance of its accuracy or its truthfulness. The statements in this declaration are based on my experience, training, and research, as well as information provided to me by other members of the U.S.

government, including members of the Federal Bureau of Investigation ("FBI"), the United States Department of Justice, and other federal agencies.

I. Assange's Claims of Prejudicial Delay Because of Political Motivation Are Meritless.

3. I am aware that Assange and his legal team have claimed that the political motivations of the current administration drove the decision to charge him, representing a reversal of course from an alleged decision in 2013 by a prior administration, and that this delay has prejudiced his ability to defend himself. Specifically, I am aware that Assange and his legal team assert that the alleged delay prejudices Assange's ability to defend himself because, had he known about the charges earlier, he could have retained evidence and undertaken investigation into the allegations.

A. Assange and His Legal Team Have Presented No Evidence to Overcome the United States' Representation that Its Charges Are Not Politically Motivated.

4. As I have previously emphasized, the superseding indictment does not reflect political bias or motivation. *See* First Declaration ¶ 11. As explained, federal prosecutors are forbidden from taking into account such considerations when making charging decisions. *See id.* ¶¶ 10-13. As I have represented, the superseding indictment against Assange is not based on Assange's political opinions, but, instead, on the evidence and the rule of law. *See id.* ¶ 17.

5. Assange and his legal team's arguments—and the affidavits filed in support—primarily rely on a select number of news articles. Based on those articles and the hearsay within them, they invite the Court to infer that the decision to prosecute was politically motivated. As a prosecutor involved in this case, however, I reemphasize that this prosecution is founded on objective evidence of criminality, and focused upon Assange's complicity in

criminal conduct and his dissemination of the names of individuals who provided information to the United States. *See id.* ¶¶ 6, 13, 17.

B. Assange Cannot Be Prejudiced By Delay Because He Knew of the Nature of the Criminal Investigation that Transferred from One Administration to Another.

6. **Assange’s arguments are contradicted by judicial findings, made in the U.S.**

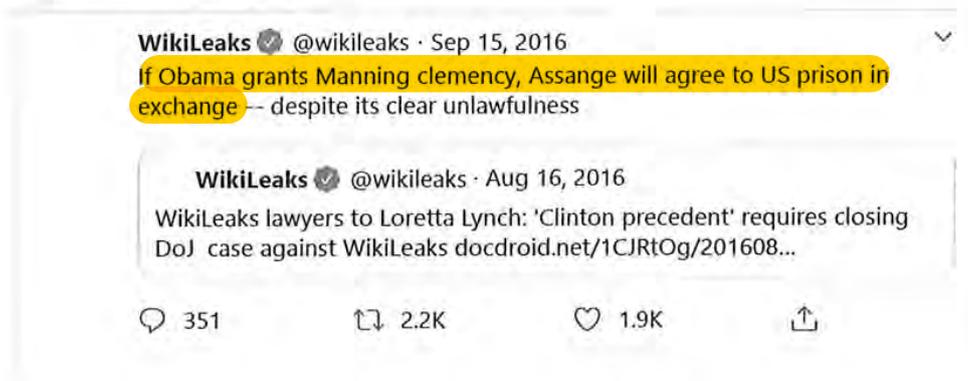
District Court of the District of Columbia, that the investigation into the unauthorized disclosure of classified information on the WikiLeaks website remained ongoing when the present administration came into office. On March 4, 2015, **United States District Judge Barbara J. Rothstein** wrote that she was “persuaded that there is an ongoing criminal investigation. . . . Defendants [the United States Department of Justice] have provided sufficient specificity as to the status of the investigation, and sufficient explanation as to why the investigation is of long-term duration.” *Electronic Privacy Information Center v. Department of Justice Criminal Division*, 82 F. Supp. 3d 307, 322 (D.D.C. 2015) (involving a lawsuit over a Freedom of Information Act request). Then, on the basis of two declarations submitted by an FBI official (the latter of which was made on May 17, 2016), **United States District Judge Amit P. Mehta** found “no reason to doubt that there is an ongoing investigation of individuals other than” Chelsea Manning. *Manning v. U.S. Department of Justice*, 234 F. Supp. 3d 26, 35 (D.D.C. Jan. 11, 2017) (involving a lawsuit over a Freedom of Information Act request by Chelsea Manning). Judge Mehta further wrote that the “government repeatedly and explicitly states that an investigation is pending. . . . Nor has there been such a protracted passage of time since the government first learned of WikiLeaks’ publication of classified material for the court to doubt whether any investigation of others might still be ongoing.” *Id.*

7. Not only have U.S. courts made findings as to the existence of an ongoing investigation, but Assange and his representatives have publicly indicated their understanding

that the investigation continued from 2010—and well after 2013—through the end of the previous administration in 2017.

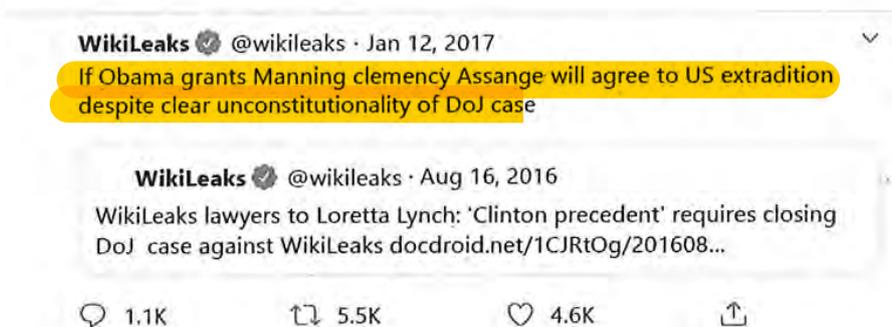
8. For purposes of these extradition proceedings, Assange has placed heavy emphasis on news reports claiming that a decision was made not to prosecute him in 2013. *See, e.g.*, Transcript of Proceedings in the Crown Court at Woolwich, at 54 (Feb. 24, 2020). At the time, however, Assange’s representatives expressed skepticism of those news reports, noting that Assange was never notified of any decision not to prosecute. *See* Sari Horwitz, *WikiLeaks Publisher Unlikely to Face U.S. Charges*, Washington Post (Nov. 26, 2013) (“WikiLeaks spokesman Kristinn Hrafnsson said last week that the anti-secrecy organization is skeptical ‘short of an open, official, formal confirmation that the U.S. government is not going to prosecute WikiLeaks.’”); *id.* (“‘We have repeatedly asked the Department of Justice to tell us what the status of the investigation was with respect to Mr. Assange,’ said Barry J. Pollack, a Washington attorney for Assange. ‘They have declined to do so. They have not informed us in any way that they are closing the investigation or have made a decision not to bring charges against Mr. Assange. While we would certainly welcome that development, it should not have taken the Department of Justice several years to come to the conclusion that it should not be investigating journalists for publishing truthful information.’”).

9. Indeed, in 2016, WikiLeaks tweeted that “precedent” required the Department of Justice to close the case against WikiLeaks, and that, in exchange for the then-administration’s grant of clemency to Chelsea Manning (with whom a grand jury has charged Assange for conspiring to commit the criminal offenses alleged in the superseding indictment at issue in these extradition proceedings), Assange would agree to U.S. prison. Here is the tweet:



@wikileaks, Twitter (Sept. 15, 2016) (8:09 AM), <https://twitter.com/wikileaks/status/776437869376262144?lang=en>.

10. Moreover, on January 12, 2017 (eight days before the transition to the current administration), WikiLeaks tweeted that, in exchange for the then-administration's agreement to grant clemency to Manning, Assange would agree to extradition to the United States. Here is that tweet:



@wikileaks, Twitter (Jan. 12, 2017) (11:40 AM), <https://twitter.com/wikileaks/status/819630102787059713?lang=en>.

11. Attached to both of these tweets was a letter from Assange's lawyer to Attorney General Loretta Lynch, concerning public acknowledgements by the Department of Justice of the ongoing criminal investigation of Assange between 2010 and 2016. This lawyer requested

closure of the then six-year investigation, into the very charges at issue in this extradition. The letter stated, in relevant part, as follows:

Dear General Lynch:

As you are aware, on November 29, 2010, the United States Department of Justice announced it was commencing an investigation of potential crimes committed by WikiLeaks and its founder, Julian Assange. As recently as March 15, 2016, the Department of Justice in a publicly filed court document confirmed that this "investigation continues to this day." See Defendants' Motion for Summary Judgment, *Manning v. U.S. Department of Justice and the Federal Bureau of Investigation*, 15-cv-01654-APM (D.D.C.), DE 12 at 1, 11. On May 19, 2016, in a subsequent publicly filed pleading, the Department reiterated the on-going nature of the investigation. See Defendants' Reply in Support of Motion for Summary Judgment and Opposition to Plaintiff's Cross-Motion for Summary Judgment, *Manning v. U.S. Department of Justice and the Federal Bureau of Investigation*, 15-cv-01654-APM (D.D.C.), filed May 19, 2016, DE 16 at 1 ("[T]he FBI's ongoing investigation is focused on any civilian involvement in Manning's leak of classified records published on WikiLeaks, and not on an investigation of Manning herself."). There are three distinct components of the Department currently conducting the investigation(s): the Criminal Division, the National Security Division, and the Federal Bureau of Investigation. See, e.g., *Electronic Privacy Information Center v. Department of Justice, Criminal Division, et al.*, 12-cv-127 BJR (D.D.C.), Memorandum Opinion dated March 4, 2015, DE 40, at 1, 4.

As Mr. Assange's criminal defense counsel in the United States, I have repeatedly sought information from the Department of Justice regarding this now nearly-six-year-old investigation. Despite the fact that the Department has continually publicly confirmed through court filings and statements to the press that it is conducting an on-going criminal investigation of Mr. Assange, the Department has provided me no substantive information whatsoever about

* * *

the status of the investigation. Two developments during the pendency of this investigation cause me to write to you to ask that you publicly announce the closure of the criminal investigation with no criminal charges.

See Letter from Barry J. Pollack to Loretta E. Lynch, Attorney General of the United States (Aug. 16, 2016), available at <https://www.docdroid.net/1CJRtOg/20160816-letter-to-us-attorney-general-loretta-e-lynch.pdf> (last viewed Mar. 10, 2020).

12. In essence, Assange has known of and followed this investigation for almost a decade. As early as 2010, the media was publicly reporting that the Department of Justice had confirmed it was investigating Assange for his acts in connection with the Manning disclosures.¹

¹ See, e.g., Luke Harding et al., *The US Embassy Cables, Behind the Leak: Julian Assange: Interpol Puts WikiLeaks Founder on Wanted List as Legal Threats Mount*, The Guardian (Dec. 1,

Further, the specific concerns of the United States that Assange's publications endangered the lives of innocent informants and sources were well publicized.²

13. Contemporaneous news reports reflect statements Assange made in response to the announcements of the investigation into him in 2010.³ Moreover, through the years, Assange

2010) ("WikiLeaks founder Julian Assange was last night facing growing legal problems around the world, with the US announcing that it was investigating whether he had violated its espionage laws."); Charlie Savage, *U.S. Weighs Prosecution of WikiLeaks Founder, but Legal Scholars Warn of Steep Hurdles*, N.Y. Times (Dec. 2, 2010) ("Attorney General Eric H. Holder Jr. has confirmed that the Justice Department is examining whether Mr. Assange could be charged with a crime . . ."); Charlie Savage, *Building Case for Conspiracy by WikiLeaks*, N.Y. Times (Dec. 16, 2010) ("Federal prosecutors, seeking to build a case against the WikiLeaks leader Julian Assange for his role in a huge dissemination of classified government documents, are looking for evidence of any collusion in his early contacts with an Army intelligence analyst suspecting of leaking the information.").

² See, e.g., Greg Jaffe & Joshua Partlow, *Mullen Says Leak Put Troops and Afghans in Danger; WikiLeaks Documents Include Names of Informants Helping U.S.*, Washington Post (July 30, 2010) ("The U.S. military's top officer charged Thursday that WikiLeaks founder Julian Assange, in releasing tens of thousands of secret documents, had endangered the lives of American troops and Afghan informants who have assisted U.S. forces. . . . A Washington Post search of the 76,000 reports released by WikiLeaks turned up at least 100 instances dealing with Afghan informants. In some of the reports the informants' names and villages are listed along with the names of the insurgent commanders that they had discussed with U.S. and Afghan officials."); Scott Shane, *WikiLeaks Leaves Names of Diplomatic Sources in Cables*, N.Y. Times (Aug. 30, 2011) ("In a shift of tactics that has alarmed American officials, the antisecrecy organization WikiLeaks has published on the Web nearly 134,000 leaked diplomatic cables in recent days, more than six times the total disclosed publicly since the posting of the leaked State Department documents began last November. A sampling of the documents showed that the newly published cables included the names of some people who had spoken confidentially to American diplomats and whose identities were marked in the cables with the warning 'strictly protect.' State Department officials and human rights activists have been concerned that such diplomatic sources, including activists, journalists and academics in authoritarian countries, could face reprisals, including dismissal from their jobs, prosecution or violence.").

³ See, e.g., Ravi Somaiya, *From WikiLeaks Founder, a Barrage of Interviews*, N.Y. Times (Dec. 18, 2010) ("In a series of media appearances Thursday and Friday the WikiLeaks founder Julian Assange railed against what he called an 'illegal' and 'aggressive' investigation of him and his Web site by the United States and dismissed accusations of sexual misconduct in Sweden as 'politically motivated.' Free on bail after nine days in prison in Britain, where he is fighting extradition to Sweden, Mr. Assange said a United States espionage indictment against him was imminent. In earlier comments, he and his supporters had called the Swedish extradition proceeding a 'holding' action intended to keep him within the law's grasp while the United

continued to make public statements reflecting that he was tracking the ongoing criminal investigation. Two of Assange's books—*Cyberpunks: Freedom and the Future of the Internet*, first published in 2012, and *When Google Met WikiLeaks*, first published in 2014—contain subchapters in which Assange acknowledged that the WikiLeaks investigation continued. See Julian Assange, *Cyberpunks: Freedom and the Future of the Internet*, at 13-19 & n.16 (2012) (citing an investigative timeline that is available at http://www.alexao'Brien.com/timelineus_versus_manning_assange_wikileaks_2012.html); Julian Assange, *When Google Met WikiLeaks*, at 220-23 & n.311 (2014/2016) (ebook) (citing, in relevant part, *Electronic Privacy Information Center v. Department of Justice Criminal Division*, No. 1:12-cv-00127, the same Freedom of Information Act case, in the U.S. District Court for the District of Columbia, that I referenced above, in Paragraph 6).

14. I do not vouch for the accuracy of descriptions by Assange, his legal team, or the media, but note only that these public accounts demonstrate that he knew of the existence and ongoing nature of the investigation by the United States into his alleged criminal activities.

C. Assange Cannot Complain About Prejudice Because He Actively Attempted to Evade Justice.

15. Assange's conduct in staying in the Embassy of Ecuador to avoid U.S. prosecution plainly corroborates that he understood that he continued to face prosecution.

States completed its investigation.”); Charlie Savage, *U.S. Prosecutors, Weighing WikiLeaks Charges, Hit the Law Books*, N.Y. Times (Dec. 8, 2010) (“After WikiLeaks released a batch of government documents concerning Iraq and Afghanistan in July, Mr. Holder and the director of the Federal Bureau of Investigation, Robert S. Mueller III, both said the leaks were being investigated, and Mr. Assange said United States officials had previously warned his organization that there had been ‘thoughts of whether I could be charged as a co-conspirator to espionage, which is serious.’”).

16. As the Court is well aware, Assange fled to, and remained in, the Embassy of Ecuador in London from June 2012 to April 2019. Assange’s own lawyers have informed this Court that he hid in the Embassy of Ecuador to avoid prosecution in the United States. *See* Statement of Jennifer Robinson ¶ 3 (Feb. 14, 2019) (“Mr. Assange had been granted asylum by Ecuador because of [the ongoing investigation and reports of a sealed indictment,] and he remained in the embassy to protect himself from US extradition.”); Statement of Gareth Peirce ¶ 6 (Oct. 18, 2019) (“Mr Assange on June 19th 2012 took refuge inside the Ecuadorian Embassy in London and applied for asylum. The basis of his application was a fear of his re-extradition from Sweden to the United States, a country from which he feared persecution. He believed that a sealed case against him was prepared in the US, for the organisation of which he was at the time a director, WikiLeaks, having published information on war crimes committed by the US in Iraq and Afghanistan.”).

17. Likewise, Assange made public statements that he was remaining in the Embassy of Ecuador to avoid prosecution in the United States. For example, in 2013, the WikiLeaks website posted an affidavit by Assange concerning alleged monitoring of his activities and search and seizure of his property. In this affidavit, Assange acknowledged that he was “granted asylum after a formal assessment by the government of Ecuador in relation to the current and future risks of persecution and cruel, inhuman and degrading treatment in the United States in response to my publishing activities and my political opinions. I remain under the protection of the embassy of Ecuador in London for this reason.”

D. Assange Will Be Able to Raise Claims About Prejudicial Delay and Selective Prosecution in the United States.

18. Finally, and importantly, Assange will have an opportunity to raise these exact arguments in the United States. The Fifth Amendment to the U.S. Constitution guarantees that “[n]o person shall . . . be deprived of life, liberty, or property, without due process of law.” U.S.

Const. amend. V. The United States Supreme Court has recognized that a criminal defendant may seek dismissal of an indictment on the ground that the government's delay in bringing the indictment violated his right to due process. See *United States v. Gouveia*, 467 U.S. 180, 192 (1984); *United States v. Lovasco*, 431 U.S. 783, 789-91 (1977); *United States v. Marion*, 404 U.S. 307, 324-25 (1971). To establish such a claim of preindictment delay, the defendant must demonstrate that the delay caused him actual prejudice. See *United States v. Uribe-Rios*, 558 F.3d 347, 358 (4th Cir. 2009). If the defendant demonstrates actual prejudice, courts will then "consider the government's reasons for the delay, balancing the prejudice to the defendant with the Government's justification for the delay." *Id.* (internal quotation omitted). As someone who knew of the investigation and actively took steps to evade prosecution for almost seven years, it will be difficult for Assange to demonstrate this prejudice. See *Barker v. Wingo*, 407 U.S. 514, 536 (1972) ("But barring extraordinary circumstances, we would be reluctant indeed to rule that a defendant was denied this constitutional right [to a Speedy Trial] on a record that strongly indicates, as does this one, that the defendant did not want a speedy trial.").

19. Moreover, as described in paragraph 68 of the First Declaration, Assange can file a pre-trial motion to challenge the superseding indictment on the basis of selective prosecution. To succeed on such a motion, Assange would have to demonstrate that the prosecution "had a discriminatory effect and that it was motivated by a discriminatory purpose." *Wayte v. United States*, 470 U.S. 598, 608 (1985). Meeting this heavy burden requires the defendant to establish "both (1) that he has been singled out while others similarly situated have not been prosecuted; and (2) that the decision to prosecute was invidious or in bad faith, *i.e.*, based upon such impermissible considerations as race, religion, or the desire to exercise his constitutional rights." *United States v. Greenwood*, 796 F.2d 49, 52 (4th Cir. 1986) (internal quotation omitted).

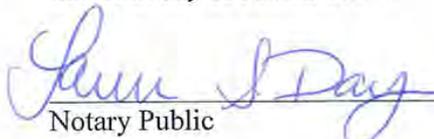
20. In short, Assange will have a forum in the United States courts to raise his allegations of prejudicial delay and selective prosecution. The United States courts—the tribunal responsible for resolving the charges against him—will be best positioned to address whether there has been any such violation.

Conclusion

21. The facts and information contained in this Declaration are true and correct according to the best of my knowledge, information, and belief.


Gordon D. Kromberg
Assistant United States Attorney
Office of the United States Attorney
Eastern District of Virginia

SUBSCRIBED and SWORN to before me
this 12th day of March 2020.


Notary Public

My commission expires May 31, 2021
Alexandria, Virginia



**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

**THIRD SUPPLEMENTAL DECLARATION IN SUPPORT OF
REQUEST FOR EXTRADITION OF JULIAN PAUL ASSANGE**

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

1. I have made three 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, “First Declaration”); Gordon Kromberg, Supplemental Declaration in Support of Request for Extradition of Julian Paul Assange ¶¶ 1-3 (Feb. 19, 2020) (hereafter, “Supplemental Declaration”); Gordon Kromberg, Second Supplemental Declaration in Support of Request for Extradition of Julian Paul Assange ¶ 1 (Mar. 12, 2020) (hereafter, “Second Supplemental Declaration”).

2. This declaration responds to certain of the defense’s “Zakrzewski abuse” allegations raised before this Court at the hearing on February 25, 2020, but it does not respond to all of them. I understand that a number of the defense’s allegations can be answered by reference to matters that have already been decided as a matter of extradition law in the United Kingdom or by argument from facts in the record before the Court. If I have not addressed a

matter in this declaration, it should not be regarded as an acceptance of its accuracy or its truthfulness. The statements in this declaration are based on my experience, training, and research, as well as information provided to me by other members of the U.S. government, including members of the Federal Bureau of Investigation (FBI), the United States Department of Justice, and other federal agencies.

I. Assange’s “Zakrzewski Abuse” Arguments Improperly Seek to Litigate the Merits of the Allegations at the Extradition Stage.

3. At the hearing on February 25, 2020, Assange’s counsel made a series of highly charged accusations that the United States knowingly made false allegations in its extradition request. Assange’s counsel, for example, described various allegations as “a knowingly false account,” “utter rubbish,” and “lies, lies and more lies.” Transcript of Extradition Hearing, at 7-8 (Feb. 25, 2020) (hereafter, “Extradition Hr’g Tr.”). I categorically reject such accusations. As a federal prosecutor on the case, I affirm that, to my knowledge and belief, the United States has not made any knowingly false allegations to support its extradition request.

4. The accusation that a lawyer, and a federal prosecutor in particular, knowingly made a false allegation is a serious one in the American legal system. The Virginia Rules of Professional Conduct—the ethical rules that govern the practice of law in the Commonwealth of Virginia—expressly prohibit lawyers from knowingly making false statements or introducing false evidence.¹ These ethical rules, moreover, impose additional responsibilities on prosecutors.

¹ See Va. Rules of Prof’l Conduct r. 3.3(a)(1) (“A lawyer shall not knowingly . . . make a false statement of fact or law to a tribunal.”); *id.* r. 3.3(a)(4) (“A lawyer shall not knowingly . . . offer evidence that the lawyer knows to be false. If a lawyer has offered material evidence and comes to know of its falsity, the lawyer shall take reasonable remedial measures.”); *id.* r. 4.1(a) (“In the course of representing a client a lawyer shall not knowingly . . . make a false statement of fact or law.”); *id.* r. 8.4(c) (“It is professional misconduct for a lawyer to . . . engage in conduct involving dishonesty, fraud, deceit or misrepresentation which reflects adversely on the lawyer’s fitness to practice law.”).

Id. r. 3.8. A prosecutor, for example, “shall . . . not file or maintain a charge that the prosecutor knows is not supported by probable cause.” *Id.* r. 3.8(a). Federal prosecutors are subject to sanction by the courts, governing bar authorities, *and* the Department of Justice if they violate these Rules of Professional Conduct.²

5. Federal prosecutors have abided by these ethical guidelines when preparing its extradition request. The United States’ extradition request faithfully and accurately reflects its case against Assange. Each allegation is premised upon the evidence identified in the request. As demonstrated below, Assange has not shown that any of the allegations are false.

6. Instead, in his “Zakrzewski abuse” submissions, Assange essentially argues that the United States should have anticipated the defenses and theories of the case that he might raise and included them in its extradition request or in the indictment itself. But that is the purpose of a trial on the merits, not the function of an extradition request or charging document. As demonstrated in the Superseding Indictment, as well as the affidavit and declarations previously filed on behalf of extradition by the United States, Assange’s arguments are contested issues of law and fact that will be addressed at trial in front of an independent judge and jury in the United States.

7. At trial in the United States, Assange will have a constitutional right to present evidence, call witnesses on his behalf, confront and cross-examine the government’s witnesses,

² *See, e.g.*, E.D. Va. Local Rules, Appendix B, FRDE Rule IV(B) (“Acts or omissions by an attorney admitted to practice before this Court, individually or in concert with any other person or persons, which violate the Virginia Rules of Professional Conduct adopted by this Court shall constitute misconduct and shall be grounds for discipline, whether or not the act or omission occurred in the course of any attorney-client relationship.”); Office of Professional Responsibility, U.S. Department of Justice, *available at* <https://www.justice.gov/opr/professional-misconduct> (last visited Mar. 22, 2020) (describing the role of the Department of Justice’s Office of Professional Responsibility in investigating allegations of professional misconduct by federal prosecutors).

and assert his defenses. *See, e.g.*, U.S. Const. amend. VI (guaranteeing criminal defendants the rights, among other things, “to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defence”); *Crane v. Kentucky*, 476 U.S. 683, 690 (1986) (recognizing that the U.S. Constitution “guarantees criminal defendants ‘a meaningful opportunity to present a complete defense’” (quoting *California v. Trombetta*, 467 U.S. 479, 485 (1984))); *Strickland v. Washington*, 466 U.S. 668, 684-85 (1984) (recognizing that the U.S. Constitution guarantees criminal defendants the right to a fair trial).³

II. Assange Has Failed to Show that the United States Made Any Misrepresentations in Its Extradition Request.

8. In the following section of the declaration, I refute a number of particular arguments that Assange’s counsel made in arguing that the United States knowingly made false allegations to support its extradition request. As I stated at the beginning of this declaration, I do not attempt to respond to every single accusation, and my failure to address a particular accusation does not signify that the United States accepts the accusation as true or meritorious. *See infra* ¶ 2.

A. The nature and purpose of the hash-cracking agreement

9. During the February 25, 2020 hearing, the defense argued that the United States’ allegations concerning the hash-cracking agreement between Assange and Manning were “provably wrong” and “a knowingly false account of the conduct that occurred.” Extradition

³ As discussed in paragraph 67 of the First Declaration, Assange will also have a right to appeal his conviction and sentence if he believes the trial court committed any error. *See Coppedge v. United States*, 369 U.S. 438, 441-42 (1962) (recognizing that “a defendant has a right to have his conviction reviewed by a Court of Appeals”).

Hr'g Tr. 7. As demonstrated below, the defense's arguments are misleading regarding the nature of the United States' allegations, and fail to show that the allegations are false.

i. State Department cables

10. The defense asserted that the Superseding Indictment alleged that the hash-cracking agreement was for the specific purpose of gaining anonymous access to the Net Centric Diplomacy database from which Manning stole the State Department cables. *See* Extradition Hr'g Tr. 10-11. According to the defense, the purpose of the hash-cracking agreement could not possibly have been to gain anonymous access to the Net Centric Diplomacy database, because the database tracked access by IP address rather than username. *Id.* at 11. This argument, however, is misleading, because it does not accurately describe the nature of the United States' allegations.

11. Contrary to the defense's assertion, the United States has not alleged that the purpose of the hash-cracking agreement was to gain anonymous access to the Net Centric Diplomacy database or, for that matter, any other particular database. Instead, Count 18 of the Superseding Indictment generally alleged that the "primary purpose of the conspiracy was to facilitate Manning's acquisition and transmission of classified information related to the national defense of the United States so that WikiLeaks could publicly disseminate the information on its website." The Superseding Indictment further asserted that "had ASSANGE and Manning successfully cracked [the password hash], Manning may have been able to log onto computers under a username that did not belong to her" and "[s]uch a measure would have made it more difficult for investigators to identify Manning as the source of disclosures of classified information." Superseding Indictment ¶ 18. As this language plainly reflects, the United States alleged that the purpose of the hash-cracking agreement was to facilitate the acquisition and

transmission of classified, national defense information generally, not to access a particular database or set of documents.

12. Cracking the password hash could have furthered the alleged goals of the conspiracy in many ways that have nothing to do with how the Net Centric Diplomacy database (or any other of the particular databases) tracks access. Stealing hundreds of thousands of documents from classified databases, as Manning did, was a multistep process. It required much more than simply gaining access to the databases on which the information was stored. For example, Manning had to extract large amounts of data from the database, move the stolen data onto a government computer (here, Manning's SIPRNet computer), exfiltrate the stolen documents from the government computer to a non-government computer (here, Manning's personal computer), and ultimately transmit the stolen documents to the ultimate recipient (here, Assange and WikiLeaks). Each step in this process can leave behind forensic artifacts on the computers or computer accounts used to accomplish the crime. Therefore, the ability to use a computer or a computer account not easily attributable to Manning could be a valuable form of anti-forensics. Put another way, Manning needed anonymity not only on the database *from which* the documents were stolen (e.g., the Net Centric Diplomacy database), but also on the computer *with which* the documents were stolen (e.g., the SIPRNet computer). The hash-cracking agreement, at a minimum, could have furthered the latter goal.

13. Manning's trial itself illustrates the point. Army forensic investigators were able to find important forensic evidence on the **Bradley.Manning** user account contained on the SIPRNet computers that Manning used (that is, on Manning's assigned SIPRNet account). This evidence, which was introduced at Manning's trial, included files that Manning viewed and/or saved, and scripts that Manning stored while signed into an Army SIPRNet computer under

Manning's own username. *See, e.g.*, Manning Court-Martial Tr. 8347 (“Within the user profile **Bradley.Manning** there was a folder called bloop and within there, there was files.zip. The files.zip contained over 10,000 complete Department of State cables.”); *id.* at 8355 (“[W]ithin the Windows temp folder there were two files, both have the SID, the security identifier of the user profile **Bradley.Manning** and these two files each contain several hundred complete Department of State cables.”); *id.* at 9168 (“Within the **Bradley.Manning** user profile, that video was present.”); *id.* at 9190 (“Within .22, in the **bradley.manning** user profile, files with [the] name [redacted] appeared in several locations.”); *id.* at 10635 (“Within the22 computer on the **bradley.manning** user profile, I examined the NTuser.dat. In there it maintained the last ten batch files which would have been accessed.”).

14. To give just one example, Manning used a custom script, created with a program called Wget (the “Wget script”), to download the State Department cables from the Net Centric Diplomacy database (exfiltrating 250,000 State Department Cables manually would likely have been prohibitively time-consuming). At Manning’s trial, the Army introduced forensic evidence showing that the Wget script had been stored on a SIPRNet computer under the **Bradley.Manning** user profile. *See id.* at 8354 (“Q. What other Wget related information did you find on this computer? A. Within Windows prefetch files there showed . . . prefetch files where I captured Wget being run from the **Bradley.Manning** user profile on several occasions.”); *id.* at 10608 (“Wget.exe was run from documents and settings bradley.manning/mydocuments/yada, folder 060000”); *id.* at 10638 (“Q. [D]id you find a folder on Private First Class Manning’s SIPRNet computer that contained a batch file and the associated files pulled using Wget? A. I did. Q. And where did you find that? A. Within the **bradley.manning** user profile”). If Assange had successfully cracked the password hash to

the FTP account, however, Manning could have used that account for the theft and Army investigators might have missed such forensic artifacts or, even if they found them, might not have been able to attribute them to Manning.

15. This is simply one way that the hash-cracking agreement may have contributed to the broad criminal purpose of the conspiracy alleged in Count 18 in the Superseding Indictment. There may be others, and the Superseding Indictment does not limit the prosecution to proving any one particular theory at trial. I simply raise these points to make clear that efforts by the defense to knock down a particular theory are misleading, when such a theory was never raised by the United States in the first place.

ii. Significant activity reports, detainee assessment briefs, and Iraq Rules of Engagement

16. At the February 25, 2020 hearing, the defense also claimed that the Superseding Indictment alleged that the purpose of the hash-cracking agreement was to allow Manning to gain anonymous access to the Guantanamo Bay detainee assessment briefs, the Iraq Rules of Engagement, and the Afghanistan and Iraq war-related significant activity reports. *See* Extradition Hr'g Tr. 31-34, 41-42. After characterizing the allegations in this way, the defense then argued that the purpose of the hash-cracking agreement could not possibly have been to gain anonymous access to these documents, either because Manning had already provided them at the time of the agreement (in the case of the significant activity reports), *see id.* at 41-42, or because Manning could not access them from the FTP user account (in the case of the rules of engagement), *see id.* at 32-34, or because access to the documents were tracked by IP address and not user names (in the case of the detainee assessment briefs and the significant activity reports), *see id.* at 31, 41.

17. Again, however, the defense's arguments are misleading, because they do not accurately describe the allegations made by the United States. The Superseding Indictment does

not allege that the purpose of the hash-cracking agreement was to gain anonymous access *to those particular documents* (i.e., the detainee assessment briefs, the significant activity reports,⁴ or the Iraq Rules of Engagement). Rather, the purpose of the agreement was to gain access to the FTP account, which could have been used for Manning's ongoing theft of classified information generally. For the reasons stated above, such anonymous access could assist Manning in preventing investigators from learning of any future activities conducted on Manning's SIPRNet computer. This could include activities related to the theft and transmission of the State Department cables and any other theft and/or transmission of classified information that Manning might have committed in the future, but for the arrest in May 2010.

B. The "Most Wanted Leaks" list

18. Next, I address three particular arguments that the defense made with respect to Assange's use of the "Most Wanted Leaks" list to solicit classified, national defense information of the United States.

19. First, the defense argued that the "Most Wanted Leaks" webpage was collaborative and allowed anyone to edit it. *See* Extradition Hr'g Tr. 12-13. Even assuming that is true, it is irrelevant. The United States never alleged that Assange drafted all of the items on the Most Wanted Leaks list. Rather, the United States has maintained that Assange used the list to encourage and cause individuals to illegally obtain and disclose information to WikiLeaks. Whether the preparation of the list was collaborative makes no difference to that allegation. What matters is that Assange posted the list on WikiLeaks, and personally solicited and encouraged others to break the law to obtain and provide responsive information.

⁴ As the defense points out (at 41-42), such an allegation would not have made sense with respect to the detainee assessment briefs and significant activity reports, because Manning transmitted those document sets to Assange before they entered into the hash-cracking agreement.

20. The extradition request contains specific examples of when Assange actively encouraged others to obtain information on the Most Wanted Leaks list. For example, as outlined in the extradition request, Assange spoke at a “Hack in the Box Security Conference” in 2009 in Malaysia, where he encouraged people to search for the Most Wanted Leaks list and for those with access to obtain and give to WikiLeaks information responsive to that list. *See* Affidavit in Support of Request for Extradition of Julian Paul Assange ¶ 16 (June 4, 2019) (hereafter, “Extradition Aff.”). As another example, the extradition request notes that, under the general category “Bulk Databases,” the Most Wanted Leaks list specifically sought the “Central Intelligence Agency (CIA) Open Source Center database.” *Id.* ¶ 15(a). As alleged, when Manning brought up the Open Source Center database in a chat with Assange on March 8, 2010, Assange informed Manning “that’s something we want to mine entirely, btw.” *Id.* ¶ 31(b). As these examples reflect, regardless of who drafted the information listed on the Most Wanted Leaks list, Assange actively encouraged others to obtain and provide it.

21. Second, the defense repeatedly argued that certain materials that Manning provided—namely, the Afghanistan and Iraq war-related significant activity reports, the Guantanamo Bay detainee assessment briefs, and the U.S. Department of State cables—were not specifically listed on the Most Wanted Leaks. *See* Extradition Hr’g Tr. 8, 14, 30-31, 41. But the United States never alleged that the Most Wanted Leaks specifically listed these documents.

22. Instead, the United States alleged generally that the WikiLeaks website solicited “*classified, censored, or otherwise restricted material of political, diplomatic, or ethical significance.*” Extradition Aff. ¶ 12. Further, the United States alleged that the Most Wanted Leaks list included broad categories of information, such as “bulk databases and military and intelligence categories.” *Id.* ¶ 21. As alleged, Manning acted consistent with the list in

downloading “four nearly complete databases from departments and agencies of the United States,” including “approximately 90,000 Afghanistan war-related significant activity reports, 400,000 Iraq war-related significant activities reports, 800 Guantanamo Bay detainee assessment briefs, and 250,000 U.S. Department of State cables.”⁵ *Id.*

23. These allegations were—and remain—accurate. Assange has not shown that they were false. If Assange wants to contest whether the Most Wanted Leaks list solicited these databases because it did not specifically list them, he is free to make those arguments to the jury at trial. But the United States did not misrepresent the facts in its extradition request.

24. Finally, the defense argued that the “Most Wanted Leaks” had been shortened significantly by May 2010. *See* Extradition Hr’g Tr. 13. But that was after Manning had already supplied troves of responsive classified information to Assange and around the time of Manning’s arrest. *See* Superseding Indictment ¶¶ 12-13.

C. Risk to the safety of sources by Assange’s dissemination of documents

25. During the February 25, 2020 hearing, the defense argued that the United States knowingly made “obviously and provably false” allegations that Assange’s publication of the Afghanistan and Iraq war-related significant activity reports and State Department cables put human sources at risk. *See* Extradition Hr’g Tr. 8. The United States, however, has offered evidence of the risk to sources caused by Assange’s publication of these documents. *See* First Declaration ¶¶ 25-65; Extradition Aff. ¶¶ 38-45. As explained below, Assange’s arguments do not establish that these allegations were knowingly false. Instead, Assange’s arguments reflect,

⁵ I also observe that the United States has not charged Assange with aiding and abetting Manning’s theft or transmission of the Iraq and Afghanistan significant activity reports. Rather, the aiding and abetting and knowing receipt charges were explicitly limited to the detainee assessment briefs, the State Department cables, and the rules of engagement. *See* Superseding Indictment, Counts 2-4, 6-14.

at most, his defenses to contested issues of law and fact, which he will have an opportunity to litigate in the United States.

i. Significant activity reports

26. At the hearing, the defense argued that the court-martial evidence established that the significant activity reports did not contain any “sensitive names.” Extradition Hr’g Tr. 42. Specifically, the defense pointed to the testimony of two witnesses called by Manning in the court-martial—Captain Steven Lim and Chief Warrant Officer 2 Joshua Ehresman—who testified that significant activity reports did not contain the names of “key sources.” *Id.* at 42-43. Neither Captain Lim nor Chief Warrant Officer Ehresman, however, testified that the significant activity reports did not contain the names of *any* sources. Instead, Captain Lim and Chief Warrant Officer Ehresman testified only as to whether significant activity reports contained the names of “*key*” sources. The defense ignored that important qualification.

27. The United States has not alleged that the significant activity reports revealed the names of “key sources.” As reflected in the extradition request, the United States has alleged that “[t]he significant activity reports from the Afghanistan and Iraq wars that ASSANGE published included names of local Afghans and Iraqis who had provided information to U.S. and coalition forces.” Extradition Aff. ¶ 39; *see also id.* ¶ 82 (“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 public outing of such local Afghans and Iraqis put them in danger, regardless of whether they were considered “key” sources. Nor does 18 U.S.C. § 793(e)—the statute that the United States has charged Assange with violating by publishing these documents—require the prosecution to prove that the disclosed sources were “key.” Because the United States did not, and was not, required to limit its charges to the

identification of “key” sources, the testimony of the two witnesses highlighted by the defense in no way suggests that the allegations were inaccurate.

28. In fact, other testimony from Manning’s court-martial supports the United States’ allegations in this case. Most notably, Brigadier General Robert Carr, who oversaw the Information Review Task Force (IRTF), testified about how the significant activity reports included the names of local nationals who provided U.S. soldiers with information. *See, e.g.*, Manning Court-Martial Tr. 11337 (“Q. And, sir, that example you gave, would those reports sometimes include those local nationalist names? A. In many cases they were.”); *id.* at 11348 (“When this data all came out and the hundreds of names that were in there, they were not necessarily -- not all of these names were legitimate intelligence sources that were committed to operating on our behalf. They were relationships of local villagers that were cooperating with patrols and Soldiers as they went through as they talked from the police chief to the captain so that they would begin to work together in a security operation.”); *id.* at 11372 (“First, let’s talk about these conversations with local nationals that show up in the CIDNE reporting, both CIDNE-I and CIDNE-A, right? So, sir, there were names listed in those reporting? A. In some of the reporting, yes.”). General Carr further described the extensive efforts that the U.S. Department of Defense undertook to notify such individuals of their disclosure to mitigate the risk of harm. *See id.* at 11348-50, 11370, 11384-86, 11402-04. As this testimony reflects, the issue of source safety was not, as the defense has wrongly suggested, uncontested at Manning’s court-martial trial.

29. Most importantly, the United States has previously described the IRTF, its duty-to-notify efforts, and the evidence of the potential harm to sources caused by Assange’s disclosures. *See* First Declaration ¶¶ 27-29, 36-43.

30. Relying on Manning’s plea statement, the defense also argued that Manning included a message that *Manning* had sanitized the reports of source-identifying information before uploading them to WikiLeaks. *See* Extradition Hr’g Tr. 43. The defense advanced this argument to suggest that Assange thought the significant activity reports had been stripped of identifying information that would put the lives of informants at risk. *See id.* This argument is misleading.

31. The evidence shows that Assange was concerned with protecting the identity of *WikiLeaks*’ sources—in this case, Manning. WikiLeaks publicly stated it sanitizes documents of metadata that would reveal a source who wants to remain anonymous. WikiLeaks also said that none of what it does is possible without sources, described as those who come forward and leak information, noting that WikiLeaks had never lost a source and none of its sources had been prosecuted. *See, e.g.,* Wikileaks vs. The World | Julian Assange Speech at 25C3 (2008), *available at* <https://videogold.de/wikileaks-vs-the-world-julian-assange-speech-at-25c3-2008>, at 5:39-6:08, 52:30-53:20. Indeed, Assange has stated that redacting for “harm minimization” is “disturbing” as it is “a very, very dangerous slippery slope.”⁶ Julian Assange, When WikiLeaks Met Google, at 177 (2014/2016).

⁶ Assange stated the following:

We have all sorts of other projects about syndicating our submission system to third parties. It disturbs me that we are redacting at all. It is a very, very dangerous slippery slope. And I’ve already said that we go through this not merely to minimize harm but for political considerations, to stop people distracting from the important part of the material by instead hyping up concerns about risks It’s a pragmatic, tactical, decision to keep the maximum impact there, instead of having to be distracted. But here we are already engaging in a rather dangerous compromise, although not nearly to the same degree as the newspapers do. We have collaborated with them and seen that some of them are just appalling. We released an analysis of their redactions versus what actually needed to be redacted, and it is extremely interesting.

Julian Assange, When WikiLeaks Met Google, at 177 (2014/2016).

32. The defense also selectively quoted from Manning's statement, presumably to try to prove its point. In Manning's plea statement, Manning quoted the message as stating the following: "It's already been sanitized of any source-identifying information. You might need to sit on this information, perhaps 90 to 100 days, to figure out how to best release such a large amount of data and to protect the source. This is possibly one of the more significant documents of our time, removing the fog of war and revealing the true nature of 21st-century asymmetric warfare. Have a good day." Manning Court-Martial Tr. 6760. When read in full, it is obvious that the "source" to be protected was *Manning*, and that the reports supplied to WikiLeaks had been sanitized to remove any information that would identify Manning as the source from whom they were received. That explains why Manning referred to "source" in the singular, and urged Assange to wait a few months before disclosing the documents.

33. Finally, the defense argued that Assange undertook "harm minimization" and redaction efforts to protect sources before publishing the reports. Extradition Hr'g Tr. 43-44. This, again, is misleading. It does not matter if Assange took measures to protect sensitive information in some of the documents. As alleged in the extradition request, he still published the names of local Afghans and Iraqis who provided information to U.S. and coalition forces, which created a grave and imminent risk that the individuals he named would suffer serious physical harm and/or arbitrary detention. *See* Extradition Aff. ¶ 39. The United States has described evidence showing that Assange *knew* that dissemination of the documents naming the sources endangered those individuals. *See id.* ¶¶ 44-45. If Assange wants to defend against these allegations by offering evidence of efforts he undertook to protect other sources, he is free

to raise this issue in United States courts. But his evidence of those efforts does not suggest that the United States' allegations were false.

ii. State Department cables

34. The defense also challenged the United States' allegation that Assange put human sources at risk by disseminating the State Department cables. *See* Extradition Hr'g Tr. 15-28.

35. Importantly, the defense did not question the veracity of certain core factual allegations that the United States made. Assange did not dispute that he initially "published some of the cables in redacted form beginning in November 2010." Extradition Aff. ¶ 44. Assange did not dispute that he then "published over 250,000 cables in September 2011, in unredacted form, that is, without redacting the names of the human sources." *Id.* Assange did not even dispute that he knew public release of the unredacted cables put the sources at risk. *See* Extradition Hr'g Tr. 27 (arguing that Assange called the U.S. Government over the telephone prior to release of the information "saying that he feared for the safety of informants").

36. The defense instead argues that Assange was justified in publishing the unredacted cables because others released them a day or two before him. As background, the defense claims that, in the summer of 2010, WikiLeaks shared the unredacted cables with a reporter from the Guardian, David Leigh, by posting an encrypted file containing the cables on the WikiLeaks website. *See* Letter Statement of Christian Grothoff, at 1 (Feb. 12, 2020) (hereafter, "Grothoff Statement"). The defense claims that, in February 2011, Leigh published a book that contained the password to the encrypted file. *See* Extradition Hr'g Tr. 23; Grothoff Statement 3. The defense further asserts that no one connected the password with the encrypted file until August 25, 2011, when Der Freitag announced it had obtained the encrypted file, decrypted the file using a password found on the Internet, and accessed the unredacted cables. *See* Extradition Hr'g Tr. 20, 24; Grothoff Statement 4. According to the defense, Assange called

the State Department the same day, warning that release of the unredacted cables was imminent and that people's lives would be at risk "[u]nless we do something." Extradition Hr'g Tr. 25. The defense argued that other actors—including Cryptome and Pirate Bay—were then able to access the unredacted cables and released them in the August 31, 2011 to September 1, 2011 timeframe. *See* Extradition Hr'g Tr. 26-27; Grothoff Statement 4. Only after that time, the defense claims, did Assange publish the unredacted cables on the WikiLeaks website on September 2, 2011. *See* Grothoff Statement 4.

37. This argument is, at most, a defense theory that Assange can raise in United States courts. It does not establish that the United States made any false allegations in its extradition request. The fact remains that, on his high-profile WikiLeaks website, Assange published unredacted State Department cables that revealed the names of human sources, knowing that the release of such information posed a danger to their safety. While Assange may challenge - - on the basis of an assertion that other actors released the information a day or two before him - - whether his publication of the unredacted cables created such a risk, the relevance and merits of such a defense will be issues for United States courts to resolve. The United States' position is that Assange's dissemination and publication of the unredacted cables placed sources at a risk of harm - - regardless of whether other actors released the information a day or two before him (particularly when Assange is responsible for originally disseminating the file with the unredacted cables that those actors accessed).

38. Publicly available information, moreover, suggests that Assange's defense theory is materially incomplete. On or about August 29, 2011, WikiLeaks posted a statement on its website announcing, "Over the past week, WikiLeaks has released 133,887 US diplomatic cables from around the world – more than half of the entire Cablegate material (251,287 cables)." The

statement noted that “[t]he decision to publish 133,877 cables was taken in accordance with WikiLeaks’ commitment to maximising impact, and making information available to all.” Soon thereafter, a number of major news outlets expressed alarm that these cables revealed the names of sources. *See, e.g.,* Ken Dilanian, *New WikiLeaks Cables Name Sources; Human Rights Groups and the U.S. Voice Alarm About Safety of Those Who Confided*, L.A. Times (Aug. 31, 2011) (“Previously, cables released by WikiLeaks had the names of [confidential] sources redacted, but analysts who have examined the cables released in recent days say that does not seem to be occurring.”); Scott Shane, *WikiLeaks Leaves Names of Diplomatic Sources in Cables*, N.Y. Times (Aug. 30, 2011) (“In a shift of tactics that has alarmed American officials, the antisecrecy organization WikiLeaks has published on the Web nearly 134,000 leaked diplomatic cables in recent days, more than six times the total disclosed publicly since the posting of the leaked State Department documents began last November. A sampling of the documents showed that the newly published cables included the names of some people who had spoken confidentially to American diplomats and whose identities were marked in the cables with the warning ‘strictly protect.’”). While I cannot vouch for the accuracy of these articles, they indicate that Assange began publishing cables that identified confidential sources before Cryptome, Pirate Bay, and others published unredacted cables.

39. It is also worth observing that, after the extradition hearing, a number of key actors in the defense’s account have disputed the veracity of its claims. For example, David Leigh and the Guardian have publicly disputed Assange’s attempt to shift blame to them. The Guardian released a statement that “it is entirely wrong to say the Guardian’s 2011 Wikileaks book led to the publication of unredacted US government files.” Ben Quinn, *Julian Assange Was ‘Handcuffed 11 Times and Stripped Naked’; WikiLeaks Founder’s Lawyers Complain of*

Interference After First Day of Extradition Hearing, The Guardian (Feb. 25, 2020). The Guardian explained, ““The book contained a password which the authors had been told by Julian Assange was temporary and would expire and be deleted in a matter of hours. The book also contained no details about the whereabouts of the files. No concerns were expressed by Assange or Wikileaks about security being compromised when the book was published in February 2011. Wikileaks published the unredacted files in September 2011.”” *Id.* And David Leigh stated, ““It’s a complete invention that I had anything to do with Julian Assange’s own publication decisions. His cause is not helped by people making things up.”” *Id.*

40. While I am not in a position to vouch for the accuracy of these statements, I highlight them to note that Assange’s account is a subject of dispute. The point is that the defense’s arguments merely raise factual disputes of dubious legal significance that should be resolved by the United States courts responsible for addressing the merits of the charges, not in an extradition proceeding.

D. Iraq Rules of Engagement

41. Finally, the defense argued that Manning uploaded the Iraq Rules of Engagement to WikiLeaks at the same time Manning uploaded the so-called “Collateral Murder” video. *See Extradition Hr’g Tr.* at 35-37. The defense made this argument to suggest that Manning obtained the Rules of Engagement on Manning’s own, without encouragement, as context for the video. *See id.* In making this argument, the defense relied on Manning’s plea statement that the Rules of Engagement were uploaded to WikiLeaks with the “Collateral Murder” video. *See id.* at 35-37.

42. The United States has described at length the circumstances in which Manning made that plea statement. *See First Declaration* ¶¶ 140-44. As previously described, Manning was not subject to cross-examination it. *See id.* ¶ 143. Instead, the military judge engaged in a

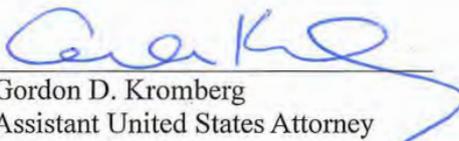
limited inquiry to ensure a factual basis for the plea. *See id.* ¶¶ 142-43. In fact, when given the opportunity at the court-martial, Manning elected not to testify. *See Manning Court-Martial Tr.* 10313 (“MJ: All right. PFC Manning, you have not testified, is that your decision? ACC: Yes, Your Honor.”). As a result, the United States has never had the opportunity to cross-examine Manning about the offense.⁷

43. The United States disputes the veracity of Manning’s account about when the Rules of Engagement were downloaded and uploaded. In Manning’s plea statement, Manning stated that the Collateral Murder video and Rules of Engagement were uploaded on February 21, 2010. *See Manning Court-Martial Tr.* 6768. As discussed in the extradition request, however, forensic computer evidence reflects that Manning downloaded the Rules of Engagement on or about March 22, 2010, and then provided them to WikiLeaks. *See Extradition Aff.* ¶ 33. Thus, this evidence shows that Manning did not obtain and provide to WikiLeaks the Rules of Engagement until about a month after Manning claims to have provided to WikiLeaks the “Collateral Murder” video.

⁷ I also observe that Manning had reasons to omit relevant facts from the plea statement. Because Manning was not charged at the court-martial with a conspiracy offense, it was unnecessary to disclose the full extent of any agreement with Assange and WikiLeaks. To the contrary, it was in Manning’s interest to avoid making any statements that could be used against her in a separate prosecution for conspiracy.

Conclusion

44. The facts and information contained in this Declaration are true and correct according to the best of my knowledge, information, and belief.


Gordon D. Kromberg
Assistant United States Attorney
Office of the United States Attorney
Eastern District of Virginia

SUBSCRIBED and SWORN to before me
this 12th day of March 2020.


Notary Public



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 serviceses [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 “#antiseconing 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/Antisecon/Lulzsec 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 eIChe.

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 is 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 unredacted 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

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 (CMH)

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

Counts 15-17: 18 U.S.C. § 793(e)
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

I. 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 services [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 “#antiseconing 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/Antisecon/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 following³:

- 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

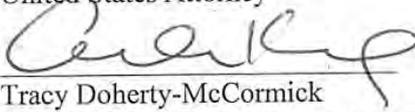
Pursuant to Federal Rule of Criminal Procedure 32.2(a), the United States of America gives notice to the defendant, JULIAN PAUL ASSANGE, that, if convicted of any of the counts of this Second Superseding Indictment, he shall forfeit to the United States, pursuant to 18 U.S.C. §§ 793(h) and 981(a)(1)(C), 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

Pursuant to the E-Government Act,
The original of this page has been filed
under seal in the Clerk's Office

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

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA)
)
 v.) No. 1:18cr111
)
JULIAN PAUL ASSANGE,)
)
 Defendant.)

**FOURTH SUPPLEMENTAL DECLARATION IN SUPPORT OF
REQUEST FOR EXTRADITION OF JULIAN PAUL ASSANGE**

I, Gordon D. Kromberg, declare and state:

1. I have made four previous declarations and one affidavit 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 those previous declarations. *See* Gordon D. Kromberg, Declaration in Support of Request for Extradition of Julian Paul Assange ¶¶ 1-4 (Jan. 17, 2020) (hereafter, “First Declaration”); Gordon D. Kromberg, Supplemental Declaration in Support of Request for Extradition of Julian Paul Assange ¶¶ 1-3 (Feb. 19, 2020) (hereafter, “Second Declaration”); Gordon D. Kromberg, Second Supplemental Declaration in Support of Request for Extradition of Julian Paul Assange ¶ 1 (Mar. 12, 2020) (hereafter, “Third Declaration”); Gordon D. Kromberg, Third Supplemental Declaration in Support of Request for Extradition of Julian Paul Assange (Mar. 24, 2020)¹ (hereafter, “Fourth Declaration”); and Affidavit in Support of Request for

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

Extradition of Julian Paul Assange on Second Superseding Indictment ¶¶ 2-3 (July 14, 2020) (hereafter, "Affidavit in Support of Second Superseding Indictment").

2. I make this declaration for the limited purpose of providing additional information relevant to several objections to the U.S. request for his extradition, that Assange has made in the evidence most recently served on his behalf. The statements in this declaration are based on my experience, training, and research, as well as information provided to me by other members of the United States Department of Justice and other federal agencies.

3. This declaration does not respond to every assertion or allegation made in the defense case. Rather, it focuses on responding to statements served on Assange's behalf in July 2020, particularly related to the William G. Truesdale Adult Detention Center ("ADC") in Alexandria, Virginia, and the United States Bureau of Prisons ("BOP"). This declaration also clarifies the law regarding the definition of "national defense information" in the United States for purposes of Section 793 of Title 18 of the United States Code. If I have not addressed in this declaration a matter raised by Assange, it should not be regarded as an acceptance of the accuracy or truthfulness of such matter.

I. The ADC Will Safely House Assange Pretrial

4. As detailed in the First Declaration, see ¶¶ 80-91, it is likely that Assange will be housed at the ADC, in Alexandria, Virginia. In his affidavit (dated June 20, 2020), Joel Sickler claims that Assange will be placed in solitary confinement and unable to have visitors. *See* Sickler Aff. ¶¶ 8 and 9. Mr. Sickler makes the general allegation that U.S. prisons at all levels, including state facilities such as the ADC, are overcrowded, understaffed, and are ill-equipped to deal with

the COVID-19 pandemic. *See id.* ¶¶ 10, 11, 28-38. At least as to the ADC and BOP facilities, Mr. Sickler is mistaken.

A. The ADC Has Adequate Health Care Resources and COVID Protocols

5. The ADC can handle Assange's physical and mental health needs. As an initial matter, the ADC is not overcrowded, as Mr. Sickler implies. Based on the single-bunking of inmates, the total capacity of the facility is 300 male inmates and 40 female inmates. Although the ADC has double-bunked inmates, it has not done so in the recent past. Over the last 12 months, the ADC has housed an average of 240 male inmates and 20 female inmates.

6. The ADC will provide Assange with quality mental health care. Mental health treatment at the ADC is provided by contract with the Alexandria Community Services Board. One clinical supervisor, ten full-time therapists, and one part time therapist are assigned to the ADC. The staff is comprised of six licensed clinical social workers ("LCSWs"), two licensed professional counselors ("LPCs"), one licensed clinical psychologist, and three Masters-level therapists who are nearing eligibility for licensure as licensed professional counselors. In addition, the ADC employs a psychiatrist who provides 20 hours of psychiatric services per week.

7. Under normal circumstances, all therapists would work during weekday business hours, and one therapist would work a partial day on Saturdays. Due to COVID-19, the clinical supervisor and half of the therapists currently are at the jail daily, with the other half of the therapists available to provide telemedicine. After-hours services are available and are provided by the Alexandria CSB Emergency Services team. This team consists of LCSWs and LPCs. While at the ADC, Assange could be seen by an outside mental health professional, subject to approval

by the USMS. Mental health treatment is available to all inmates, regardless of where they are housed within the ADC.

8. On occasion, federal prisoners at the ADC are transferred to other BOP facilities. Based upon my experience and discussions with the USMS, these transfers are *not* made because the ADC is unable to handle prisoners' mental health needs. Rather, they are made because a federal judge has ordered that the inmate receive an evaluation to determine whether such inmate is competent to stand trial, or because the inmate has a serious health condition that requires specialized health care in a hospital setting.

9. The ADC employs detailed and rigorous COVID-19 protocols. *See* Exhibit A to this Declaration. Among other things, all inmates are issued a cloth mask, which they must wear any time they are out of their cells, and the temperatures of all inmates are taken on a daily basis. The protocols are updated on a regular basis to reflect current best practices. According to the USMS, only one inmate at the ADC has tested positive for COVID-19. That inmate was a new arrestee. Staff placed the arrestee in quarantine, and the arrestee subsequently tested negative and was released.

B. Assange Will Be Able to See Visitors, Meet With His Attorneys, and Participate in Programs at the ADC

10. As I discussed in the First Declaration (at ¶ 83), the ADC does not use “solitary confinement.” It is possible, but not certain, that Assange could be placed in administrative segregation, which is the most restrictive form of custody at the ADC. *Id.* ¶ 85. Even in administrative segregation, Assange would be able to communicate with other inmates through the doors and windows of his cell. Assange would be confined to his cell for no more than 22 hours per day, and have access to ADC programs as well as the day-room, law library, and other locations

within the ADC as his and the facility's schedules permitted. It is possible that Assange would receive pretrial Special Administrative Measures ("SAMs"). Even if Assange does receive pretrial SAMs, he would not be held in solitary confinement, and he would have access to other parts of the ADC.

11. Due to COVID-19, there are currently no in-person visits at the ADC. Any physical visits must be approved by the Chief of the ADC. Nevertheless, prisoners are able to meet with visitors virtually. Prisoners can have two virtual visits per week (during non-COVID times, they could have two in-person visits per week). Prisoners also are able to meet with their attorneys virtually. There are no limitations on attorney virtual visits, except that attorneys must reserve time slots. The imposition of pretrial SAMs would not impact Assange's ability to meet with his lawyers (either virtually or in-person, depending on circumstances).

II. The BOP Will House Assange Safely and Humanely, and Provide Him with Due Process

12. In his affidavit, Mr. Sickler claims that the BOP will be unable to ensure Assange's safety and meet his physical and mental health care needs. In particular, Mr. Sickler alleges that BOP facilities are overcrowded and unable to provide for inmates' mental and physical well-being. Mr. Sickler also alleges that the BOP will improperly restrict his ability to communicate with his family and attorneys, and violate his due process rights through the use of Communication Management Units ("CMUs") or the imposition of SAMs. Finally, Mr. Sickler claims that the BOP is unable either to prevent inmates from contracting COVID-19, or treat inmates who have the virus. Mr. Sickler's affidavit is inaccurate. On the contrary, and as detailed below, the BOP is a professional organization that treats its prisoners consistent with the law in the United States, and will make reasonable efforts to meet Assange's physical and mental health care needs.

A. The BOP Provides Inmates With Quality Health Care

13. As an initial matter, Mr. Sickler's statistics regarding inmate population and staffing at BOP facilities appear to be out of date. *See* Sickler Aff. ¶ 10 (citing statistics from December 31, 2019). The most recent available statistics are from June 30, 2020. *See* Federal Bureau of Prisons Program Fact Sheet, *available at* https://www.bop.gov/about/statistics/docs/program_fact_sheet_202008.pdf (last visited Sep. 1, 2020). According to the fact sheet, the BOP ended fiscal year 2019 with 4,484 fewer inmates than the prior year, marking the sixth consecutive year of decreases in the inmate population. The fact sheet does acknowledge that the BOP "remains crowded in high, medium, and low security facilities." *Id.* The relative crowding information referenced on the BOP's Fact Sheet is based on the rated capacity. The rated capacity measurement facilitates the BOP's ability to manage and distribute its inmate population on an equitable and rational basis in accord with capacity computation formulas, security considerations, and institution needs. Further, rated capacity is not necessarily the same as any institution's design or operating capacity. It is an objective measurement of inmate housing space, without regard to items such as institution age, location, or infrastructure.

14. Although these facilities are crowded according to one of the BOP's metrics, this metric alone is not reflective of the overall safety and security of the BOP's facilities. To maintain safe and secure facilities, the BOP uses a combination of tools, including staffing, inmate population management, security and custody levels, medical and mental health care levels, treatment programs, education and vocational training, and work programs.

15. Mr. Sickler also makes reference to the inmate/staff and inmate/correctional officer ratios. Relying on these ratios alone has limited utility. The BOP staffs its facilities according to a variety of factors, including security level, inmate population, and facility programs and capabilities. These variations are not captured in the overall ratios.

16. Turning to the ratios themselves, across BOP, the inmate/staff ratio is 3.8 to 1, and the inmate/correctional officer ratio is 8.0 to 1. *Id.* The BOP regards all staff, with a few exceptions, as law enforcement regardless of their actual discipline. These staff members are engaged in the supervision and management of offenders and receive the same training as correctional officers.

B. The BOP Will Meet Assange's Healthcare Needs

17. The BOP meets the health care needs of the inmate population in a variety of ways. Emergency/urgent health care is available 24 hours a day by on-site or community medical staff. All BOP staff are trained to provide first-aid, CPR, AED, and treatment of opioid overdose with naloxone. Less urgent acute medical conditions are triaged and scheduled at appropriate times. Health care staff make daily rounds in segregation units ("Special Housing Units") to triage requests for care.

18. Similar to health insurance plans, the BOP has a defined scope of services which determines the care provided to inmates in its custody. Medically necessary care is provided to all inmates. Elective health care which may improve quality of life is assessed on a case-by-case basis through a process called utilization review. Health care with limited medical value or expressly for the inmate's convenience is not routinely approved. "Extraordinary" care must be approved by the BOP medical director. Inmates with chronic conditions are seen by a physician at least once

every 12 months, or more frequently as clinically indicated, either by a physician or advance practice provider such as a nurse practitioner or physician's assistant.

19. The BOP also uses a medical classification system to identify inmates with different levels of medical and mental health needs, based on the complexity or risk of the condition or the frequency of services required. Institutions are also assigned a Care Level based upon on-site and community capabilities for providing health care. Inmates are designated to specific institutions to align their care level with the care level of the facility. Care Level 1 includes inmates who are essentially healthy or who have medical conditions that are stable and easily treated or controlled. At the other end of the spectrum are Care Level 4 inmates, with more advanced health care needs, who are housed at BOP medical centers for treatment such as 24-hour nursing care, dialysis, cancer treatments, and organ transplant services. These BOP medical centers have contracts with local health care systems of national and international renown, who provide advanced health care services to the inmate population consistent within established standards of care.

20. With regard to staffing, individual institutions maintain a multidisciplinary complement of full-time health services staff. Currently, the medical disciplines of physicians, pharmacists, advanced practice providers and nurses are filled at 90% across the agency. Full-time Regional and Central Office clinical staff supplement the institution staff and provide additional services through telepsychiatry, telehealth or periodic on-site visits. Institutions also contract with local civilian health care providers and health systems for additional services either on site at the correctional facility or in the community.

21. The BOP's Care 2 and 3 facilities are accredited by the Accreditation Association for Ambulatory Health Care ("AAAH"), and the BOP's Care 4 facilities (medical centers) are

accredited by The Joint Commission. The AAAHC and The Joint Commission are national health care accreditation organizations. In addition, all BOP institutions are also accredited by the American Correctional Association, which applies both health care standards and correctional standards.

C. The BOP Has Made Improvements to Its Mental Health Treatment Programs Since the *Cunningham* Lawsuit Was Filed

22. Mr. Sickler relies on the lawsuit of *Cunningham v. Bureau of Prisons*, Case No. 1:12-cv-01570-RPM (D. Colo.), to claim that mental health treatment at the ADX is deficient. I draw the Court's attention to the Declaration of Dr. Alison Leukefeld, that was recently served by the United States, and that addressed many of Mr. Sickler's claims regarding BOP's mental health treatment. I also draw the Court's attention to paragraphs 16 through 19 of my Second Declaration, in which I described a number of improvements to BOP mental health treatment, and policies at the ADX.

23. Many of the improvements outlined in my Second Declaration and in Dr. Leukefeld's declaration were put in place following the initiation of the *Cunningham* lawsuit referenced by Mr. Sickler. The BOP denied the allegations in the *Cunningham* litigation, and the issue of liability was never litigated. The BOP never conceded that the policies and initiatives contained within the Settlement Agreement were required by the U.S. Constitution; it asserted that those initiatives far exceed what the Constitution requires. In any event, the BOP undertook an innovative approach to address the criticisms raised by the *Cunningham* plaintiffs.

24. The parties agreed to a settlement subject to the Prison Litigation Reform Act ("PLRA"), 18 U.S.C. § 3626(c)(2), with dismissal under the theory set forth in *Kokkonen v. Guardian Life Insurance Co. of America*, 511 U.S. 375 (1994), which gives the district court

limited jurisdiction to enforce the settlement as provided in the agreement. *See* Exhibit B to this Declaration. The settlement provided for a three-year presumptive term, with a four-year “hard stop” and the ability for the BOP to move to partially or completely terminate the obligations with the Plaintiffs’ consent after two years. The Plaintiffs and the BOP each selected an expert to monitor the settlement. The experts undertook a maximum of three site visits per year. The monitoring was limited to the ADX and the Secure STAGES program at the United States Penitentiary, High Security, in Florence, Colorado. The Special Security Unit program was excluded from oversight by the monitors, although a United States Magistrate Judge was permitted to enter the unit on several occasions, and report any concerns to the monitors. The first visit, or base-line visit, by the monitors occurred the week of January 30, 2017. The last visit by the monitors occurred the week of January 20, 2020.

25. Under the settlement agreement, the BOP retained the ability to change its policies and to make decisions concerning mental health diagnoses, assignment of mental health care levels, and appropriate care for all inmates. The agreement contained significant meet and confer requirements before the plaintiffs could attempt to enforce any terms of the agreement, and allowed for the Court hold the BOP in contempt, if necessary. This never occurred. Likewise, no monetary damages were paid to the named plaintiff-inmates.

26. The presumptive term of the agreement was three years. The plaintiff-inmates had the burden to move for a one-time, one-year extension. The agreement also allowed the BOP to move for termination, in whole or in part, after two years with the plaintiffs’ consent. The plaintiffs never sought an extension, and the BOP did not move for early termination.

27. In sum, the BOP addressed the plaintiffs' criticisms through a transparent, collaborative process. As outlined in my declaration and that of Dr. Leukefeld, the BOP developed a range of progressive policies and procedures to improve and enhance mental health programs and services. The BOP also transferred of a number of prisoners from ADX. The negotiated terms of the *Cunningham* settlement had and continue to have a direct and positive impact on the safety and wellbeing of BOP staff, inmates, and the general public. As a result, mental health care at the ADX has improved through early detection of mental health issues, as well as more effective treatment, management, and stabilization.

D. Assange Will Be Able to Participate in Programs and Socialize with Others If He is Housed at the ADX

28. Mr. Sickler claims that if Assange is sent to the Administrative Maximum Security Prison ("ADX"), he will effectively live the remainder of his life in isolation. As I stated in the First Declaration, *see* ¶¶ 183-88, sentencing in the United States is driven by a variety of factors, notably including the United States Sentencing Guidelines. Similarly, prison designations are made by the BOP, which takes into account a number of different factors, including but not limited to, the length of a defendant's sentence. In short, sentencing and facility designations are difficult to predict, and, as a result, it is purely speculative to conclude that Assange would receive a life sentence and/or be designated to the ADX.

29. The philosophy of the BOP is to house all inmates in the least restrictive environment, appropriate for that inmate, in order to allow for work and self-improvement opportunities to assist in reentry efforts. The ADX is the most secure prison in the federal system. It is designed to safely house the BOP's most violent, predatory, and escape-prone inmates, in an environment providing each inmate an opportunity to demonstrate improved behavior, and the

ability and motivation to eventually reintegrate into the open population at a different facility. The unique security and control procedures implemented to control these inmates are designed to enhance the safety of staff, inmates, and visitors. Of the approximately 129,000 inmates in the BOP's custody, just over 300 are currently housed at the ADX (which has a maximum capacity of 490); in other words, the ADX houses less than one quarter of one percent of the BOP's inmate population. Through regular, careful, case reviews, the BOP ensures that the ADX is used only for those individuals for whom its security and controls are necessary.

30. All inmates at the ADX are single-celled. The sizes of the cells range from 75 to 87 square feet. The cells in six of the nine housing units (B, C, D, E, F, and G units) are approximately 87 square feet, which does not include the inner sallyport area of the cell, which is 17 square feet. Each cell has a solid outer door and an inner grill. The wall next to the door for each cell also has an approximately 12-by-48 inch window. Each cell solid outer door has an approximately 5-by-18 inch window, which looks out on to the housing unit range. Each cell also has a 5-by-38 inch window that looks outside, providing the inmate with natural lighting, as well as a shower in the cell. The cells in the remaining 3 units (H, J, and K units), have approximately 75.5 square feet of living space and do not have an inner sallyport or a shower. Each cell has a solid outer door, with a 5-by-18 inch window, which looks out on to the range. Each cell also has a 5-by-38 inch window that looks outside, providing the inmate with natural lighting.

31. Each cell at the ADX has a light, which the inmate may turn on and off as needed. These lights have three settings (dim, medium, and bright). The inmate controls the setting of the lights from inside his cell and can turn the light completely off. The inmate is required to turn the light on when staff are interacting with him at the front of his cell. Each cell has a bed with a

mattress and bedding, a sink, a desk, a shelf, and a chair. Inmates may have certain personal items in their cells, such as photographs, reading materials, and legal papers.

32. With the exception of inmates in disciplinary segregation, each ADX inmate has a 13" television in his cell, which generally provides channels for closed circuit institutional programming (recreation, education, religious services, and psychology), broadcast channels, radio stations, and digital music channels. One of the television channels that is utilized to provide bulletins to the inmates also shows the date and time. The televisions and select broadcast channels are paid for through profits from inmate commissary or canteen purchases.

33. Even if Assange is to be housed at the ADX, he would have ample opportunity to participate in programs and socialize with inmates and members of the public. ADX Inmates are provided with access to both indoor and outdoor recreation, with the amount of time varying by unit, as explained below. When inmates go to outside recreation, they have access to sunlight and fresh air. Generally, the areas contain pull-up and dip bars, and inmates can play with handballs and soccer balls. Inmates may request instruction in aerobic exercise from ADX Recreation staff. Inmates have access to psychology programming (individual and group sessions), educational programming (group and individual), wellness programs, weekly leisure games via the ADX closed circuit television system, weekend "brain teaser" games, arts and crafts, a weekly movie program, and special holiday activities.

34. Contrary to the assertions in Mr. Sickler's affidavit, there is no contradiction between close controls and the provision of basic amenities and life-enhancing programs. Inmates housed at the ADX may subscribe to periodicals; may borrow leisure reading materials from the institution's library; may take GED, Adult Continuing Education, and correspondence classes;

may paint, draw, or crochet; may participate in a weekly bingo game; and may participate in art, essay, and poetry contests. Inmates may make purchases from the commissary, including food items, toiletries, pens, paper, and religious items.

35. From February 1, 2020, through August 15, 2020, 222 inmates at the ADX participated in some type of group or individual programming. The following are examples of the group programs available at the ADX:

- 7 Habits for Highly Effective People (taught in English and Spanish)
- Threshold
- How to Draw
- Managing Diabetes
- Five Love Languages
- GED Testing, Tutoring, Lectures
- Wellness Recovery Action Planning
- Positive Psychology for the Long Term Incarcerated
- Release Preparation Programming
- Money Smart
- Victim Impact

36. The ADX also has a robust creative arts program, which is known as “CAP.” The CAP is designed to expose participants to a variety of different artistic methods, ideologies, and entrepreneurial techniques that can better prepare them for re-entry. The CAP also centers on teaching inmates to develop a stronger work ethic through channeling their “artist spirit.” There are three unique phases to the program—CAP History, a CAP Exploratory phase, and CAP

Business. Some of the educational material used is on loan through the National Gallery of Art in Washington, D.C. In an attempt to better prepare for life on the outside for creative individuals, the CAP also teaches inmates the business side of the creative industries.

37. Inmates at the ADX are encouraged to engage with family and friends in the community through social visits, correspondence, and telephone calls. All inmates are ordinarily given the opportunity to have up to five in-person social visits per month, unless they are subject to some sort of visitation restriction. These visits are non-contact and have been temporarily suspended due to the COVID-19 pandemic. Inmates may also make social telephone calls, the number of which depends on the inmate's housing unit, as described below. Inmates may send and receive legal and social correspondence, unless there is some sort of restriction on their correspondence privileges.

38. Inmates at the ADX are encouraged to engage with staff. The Warden, Associate Wardens, Captain, and Department Heads perform weekly rounds in each unit for the opportunity to visit with inmates. Correctional Officers perform regular 30-minute rounds throughout all three shifts on a daily basis. A member of an inmate's Unit Team visits the inmates every day. Inmates receive regular visits from medical staff, education staff, religious services staff, and psychology staff when they perform their rounds, and upon request if needed. Medical staff visit each unit daily. In addition, inmates have the ability to communicate with one another in several ways—they can and do speak to their neighbors in the cells next to, above or below them and may speak to one another during out-of-cell recreation.

39. The ADX currently operates five distinct housing programs: the Control Unit Program; the Special Security Unit ("SSU") Program; the General Population and Step-Down

Program; the Reentry Preparation Unit; and the High Security Adult Alternative Housing Program.² Each of these programs is detailed below. As explained below, each unit seeks to balance safety and security while meeting the BOP's goal of placing inmates in the least restrictive environment possible.

1. Control Unit

40. The Control Unit houses the most dangerous, violent, disruptive and assaultive inmates in the BOP's custody. The Control Unit Program provides housing for inmates who are unable to function in a less restrictive environment without posing a threat to others or the institution. This unit typically houses inmates who have assaulted or killed staff or other inmates or who have escaped or attempted escape from another institution.

41. Referral to the unit is outlined in Program Statement 5212.07, Control Unit Program, and is reviewed by the BOP's Regional Director in the region in which the inmate is housed. If the Regional Director concurs with the placement, the referral is submitted to the Regional Director of the North Central region, where the ADX is located. The Regional Director then designates a hearing administrator to conduct a hearing to review the placement referral. A mental health evaluation is a required component of the referrals to the Control Unit, and medical, psychological, and psychiatric concerns are considered during the review. Findings from the mental health evaluations, along with the full clinical record, are reviewed by the Central Office level by the Psychology Services Branch. The decision of the hearing administrator is then

² The ADX no longer operates a Special Housing Unit ("SHU") for inmates in administrative detention status.

submitted to the Executive Panel (consisting of the North Central Regional Director, and Assistant Director of the Correctional Programs Division) for final review and placement.

42. Inmates placed in the Control Unit are given a specific term of time that they will serve in the Control Unit. Inmates placed in the Control Unit are reviewed within four weeks of initial placement. Subsequent reviews are conducted on a monthly basis by the unit team, while the Executive Panel reviews each inmate's status and placement on a quarterly basis. Credit for time served is granted depending on their adjustment and readiness for release from the Control Unit.

43. Inmates housed in the Control Unit receive a minimum of seven hours of out-of-cell exercise per week and can participate in educational and psychological programming via the closed circuit televisions within their cells. Inmates receive psychology services and medical services on the same basis as inmates housed in other units at ADX. The inmates consume their meals in their cells. The inmates receive two monthly social telephone calls and may receive up to five social visits per month.

2. Special Security Unit ("SSU") Program

44. The Special Security Unit Program is designed for inmates who are subject to SAMs, which are restrictions on communications imposed by the Attorney General. *See* 28 C.F.R. §§ 501.2, 501.3. Inmates with SAMs are placed in the Special Security Unit (H Unit). As detailed in my First Declaration, see ¶¶ 95-99, a SAM may be imposed to prevent the disclosure of classified information that would pose a threat to national security if disclosed or to protect against acts of terrorism and violence. A SAM may include placing an inmate in administrative detention and restricting social visits, mail privileges, phone calls, and access to other inmates and to the

media. Inmates housed in the SSU are reviewed annually by the Attorney General to determine if the SAM status should be renewed or modified. The Attorney General's review includes an assessment of information provided by the prosecuting United States Attorney's Office and federal law enforcement officials.

45. The inmates incarcerated in H Unit have the opportunity to participate in a three-phase Special Security Unit Program (SSU Program), designed especially for SAM inmates. The purpose of the SSU Program is to confine inmates with SAMs under close controls, while providing them opportunities to demonstrate progressively responsible behavior and participate in programs in a safe, secure environment. The SSU Program balances the interests of providing inmates with programming opportunities and increased privileges with the interests of ensuring institutional and national security. The success of the inmate's participation in the SSU Program provides information that can be considered in the evaluation of whether SAMs continue to be necessary, or whether the inmate's communications can be monitored in a manner that will not compromise national or institutional security interests.

46. The inmates housed in the SSU receive a minimum of 10 hours of out-of-cell exercise per week. Generally, the inmates recreate individually in secure single recreation areas. The inmates consume their meals in their cells. The inmates receive up to four monthly social telephone calls and may receive up to five social visits.

- Phase 1. During the baseline phase of the program, an inmate may be permitted two non-legal telephone calls per month, access to a commissary list and art and hobby craft items, and escorted shower time on the inmate's range—the common area outside of a cell—three times each week.

- Phase 2. Depending upon the inmate's adjustment, he can move into Phase 2 after approximately 12 months. In Phase 2 of the Program, an inmate may be permitted three non-legal telephone calls per month and access to an expanded commissary list and additional art and hobby craft items. The inmate is allowed to be out of his cell without an escort five times each week.
- Phase 3. Placement into Phase 3 typically requires a modification of the SAMs to allow inmates to have physical contact with one another. Inmates in Phase 3 are allowed to be out on the range together in groups of up to four. An inmate in Phase 3 gains the ability to be in physical contact with other inmates in the range area outside his cell, seven days a week. Phase 3 inmates spend one-and-a-half hours per day on the range with up to three other inmates, none of whom are escorted by BOP staff. The inmates in Phase 3 eat one meal together and engage in recreational activities, including watching television, reading and playing cards. Phase 3 inmates may shower at any time they are on the range. In addition, Phase 3 inmates continue to have access to the expanded art and hobby craft list and a further expanded commissary list.

3. General Population and Step-Down Unit Program

47. The ADX has a General Population and Step-Down Unit Program that provides inmates with incentives to adhere to the standards of conduct associated with a maximum security custody program. As these inmates demonstrate good conduct and positive institutional adjustment, they may progress from the General Population Units (C, D, E, F, and G) to the Intermediate (J/A), Transitional (which

is currently located at USP Florence, adjacent to the ADX on the complex), and Pre-Transfer Units (also located at USP Florence). Inmates who are successful in the Pre-Transfer Unit may be transferred to a different BOP facility. Inmates at the ADX are encouraged to engage with family and friends in the community through social visits (currently suspended), correspondence, and telephone calls. There is no numeric limit on the number of legal visits and calls they may receive, although in-person visits currently are suspended. The other privileges afforded to the inmates are determined by their housing unit assignments in this layered program.

48. Ordinarily, the minimum time period to complete the program is 36 months. The minimum stay is ordinarily 12 months in a general population unit, six months in the intermediate program, six months in the transitional program, and 12 months in the pre-transfer program. There is no minimum or maximum time period for completion of the program.

49. General Population inmates have access to the programming and opportunities described above, including a television set in each cell. These inmates receive at least 10.5 hours of out-of-cell recreation per week (alternating between indoor and outdoor). Meals are provided to the inmates in their cells. General Population inmates are permitted to have four 15-minute social phone calls per month.

50. Inmates in the Intermediate Step receive 20.5 hours of out-of-cell recreation per week, split between out-of-cell recreation on the range and outdoor recreation. The inmates are assigned to one of four groups, with as many as eight inmates in a group. The inmates have indoor and outdoor recreation out of their cells with inmates in their assigned group. Meals are provided to the inmates by groups, with each group allowed out of their cells one at a time to come to the

front of the range, receive their meals, and then return to their cells while unrestrained. The inmates eat their meals in their cells. The inmates are unrestrained when out of their cells on the range. The inmates receive six 15-minute social telephone calls per month. Shower stalls are located on the range, and the inmates may shower any time they are out on the range. Inmates in this unit also have access to TruLincs, the BOP's email program for inmates, to communicate electronically with staff and a limited number of approved contacts outside in the community.

51. The Transitional and Pre-Transfer Units are located at USP Florence, in Bravo-A Unit. Each cell in Bravo-A Unit has approximately 80 square feet area of living space and does not have a sally port or a shower. Each cell has a solid outer door. Each cell's solid outer door has a window which looks out on to the range. Each cell also has a window that looks outside, providing the inmate with natural lighting. The inmates are assigned to a group. The inmates consume their meals on the range with the other inmates in their assigned group. Showers are located on the ranges, and inmates may shower at any time they are on the range. The inmates in these units receive a minimum of 30.5 and 35.5 hours of out-of-cell recreation per week, respectively. The inmates' out-of-cell recreation includes recreation in the unit and in the outdoor group recreation area. The inmates receive eight and ten 15-minute social telephone calls per month, respectively. Inmates in these steps also have access to TruLincs, the BOP's email program for inmates, to communicate electronically with staff and a limited number of approved contacts outside in the community.

4. The Release Preparation Program

52. The Release Preparation Program is designed to assist inmates in their transition from a restrictive housing environment to less secure housing, a Residential Reentry Center, or

facilitate successful reintegration into their communities upon release. The Release Preparation Program utilizes a system of less-restrictive housing to provide inmates with incentives to adhere to standards of conduct associated with the ADX. Specifically, the Release Preparation Program operates similar to a Privilege Incentive Program, providing an inmate in the program with increased incentives/privileges as he progresses toward the end of his sentence. The progression of an inmate in the Release Preparation Program is based on his remaining sentence length. The incentives/privileges an inmate earns in the program are based on his program participation. The Release Preparation Program, which is physically located in K/A-Unit, was activated on September 28, 2017.

53. Generally, the profile of an inmate appropriate for the Release Preparation Program depicts an individual who has demonstrated he can function in a less-secure unit in the ADX, but may be unable to complete the ADX General Population and Step-Down Program prior to his release. To be eligible for consideration for placement in the program, the inmate ordinarily must (1) be within 36 months of release from confinement; (2) have no detainers or active warrants; (3) be actively participating in and complete programs recommended by the Unit Team; (4) show positive behavior and respectful conduct towards staff and other inmates; and (5) show positive overall institution adjustment to include, but not limited to, personal hygiene and cell sanitation. Exceptions can be made on a case-by-case basis.

54. Inmates in the Release Preparation Program receive 20.5 hours of out-of-cell recreation per week, split between out-of-cell recreation on the range and outdoor recreation. The inmates are assigned to one of four groups, with as many as eight inmates in a group. The inmates have indoor and outdoor recreation out of their cells with inmates in their assigned group. The

inmates in the Release Preparation Program are offered a minimum of 18.5 hours of out-of-cell programming per week. Meals are provided to the inmates by groups, with each group allowed out of their cells one at a time, to come to the front of the range, receive their meals, and then return to their cells while unrestrained. The Unit Manager schedules one group per week to eat all three meals on the range. The other groups, when not assigned to eat their meals on the range, eat their meals in their cells. The inmates are unrestrained when out of their cells on the range. The inmates receive five 15-minute social telephone calls per month. Shower stalls are located on the range, and the inmates may shower any time they are out on the range. Inmates in this unit also have access to TruLincs, the BOP's email program for inmates.

5. High Security Adult Alternative Housing Program

55. The High Security Adult Alternative Housing Program is designed for inmates who have generally demonstrated that they can function in a less-secure environment within the ADX without posing a risk to institutional security and good order, but whose security and/or safety needs prohibit them from advancing through the Step-Down Unit Program. This program reflects the BOP's core values (correctional excellence, respect, and integrity) through a continual review of the operating procedures to determine if gradual modification is necessary, first and foremost to reflect sound security practices, and only then to safely expand inmate access to programming opportunities. This program permits close controls while providing basic amenities and life enhancing programs that allow inmates to engage socially with one another.

56. The inmates in this program are assigned to one of four groups of up to eight inmates. The unit has an enclosed common area with recreation equipment and leisure materials. These inmates receive a minimum of 24 hours of out-of-cell recreation per week. The inmates

recreate with other inmates in their assigned group on the range, or outdoors, on a large recreation yard. The inmates consume their meals in their cells. The inmates are unrestrained when out of their cells. The inmates receive four 15-minute social telephone calls per month and may receive up to five social visits per month (currently suspended). Inmates in this unit also have access to TruLincs, the BOP's email program for inmates, to communicate electronically with staff and a limited number of approved contacts outside in the community. Shower stalls are located on the range. The inmates may shower anytime they are out on the range.

E. The BOP Will Afford Assange Due Process

1. Placement in a CMU Does Not Violate Due Process and Will Not Unduly Restrict Assange's Communications

57. As stated in my First Declaration, ¶¶ 103-05, it is possible that Assange may be placed in a Communications Management Unit ("CMU").³ A CMU is a separate housing unit within another facility. Inmates are placed in a CMU because of safety and security concerns arising from their use of a communications device or communications they have made during the commission of their crime or while incarcerated. The designation to a CMU process is outlined in detail in BOP Program Statement 5214.02, Communications Management Units, attached as Exhibit C to this Declaration. As detailed in my First Declaration, *see* ¶ 105, and the BOP Program Statement, inmates are provided notice and an opportunity to be heard on the issue of designation to a CMU.

58. Contrary to Mr. Sickler's suggestion, inmates in CMUs are not cut off from the outside world. Rather, inmates are afforded the same opportunities to communicate with

³ In his affidavit, Mr. Sickler incorrectly refers to CMUs as "Contact Management Units." ¶ 43.

individuals outside of prison as regular inmates. Their communications may be more extensively monitored, however, or BOP may impose certain limitations, as noted in the BOP Program Statement, to prevent them from engaging in additional criminal conduct. *See* Exhibit C. Likewise, inmates in CMUs are able to participate in the same programs as inmates in the prisons' general populations. According to BOP officials, there are no studies or formal evidence to support Mr. Sickler's claim that inmates in CMUs experience distress or depression from monitoring of their conversations.

2. The Imposition of SAMs Does Not Violate Due Process.

59. Only a tiny fraction of federal inmates are the subject of SAMs. For example, as of September 1, 2020, of the 156,083 inmates in BOP custody, only 47 are under SAMs. Moreover, imposition of SAMs does not violate due process.

60. Contrary to Mr. Sickler's assertions, federal courts have found that the imposition of SAMs comport with due process. As a technical legal matter, the U.S. Supreme Court has held that inmates are not entitled to procedural protections before SAMs are imposed. *See Hewitt v. Helms*, 459 U.S. 460, 468 (1983) (where an inmate represents a security threat, he "must merely receive some notice"). Nevertheless, the Department of Justice has created regulations to ensure that inmates receive notice of the SAMs and an opportunity to contest them.

61. Pursuant to the SAM regulations, the inmate must receive "notification of the restrictions imposed and the basis for these restrictions." 28 C.F.R. § 501.2(b). To contest a SAM, an inmate can use the BOP's four-tiered Administrative Remedy Program, a mechanism that allows inmates to raise grievances in four steps—beginning at the prison level and culminating in a review at the BOP's national Central Office. *See* 28 C.F.R. §§ 542.10–542.19; *see also* 28 C.F.R.

§ 501.3(e) (authorizing inmate to seek review of SAMs through the BOP's administrative remedy program).

62. An inmate can also contest SAMs at the time of their renewal. This process is described in detail in an ADX policy statement.⁴ The policy provides that approximately 120 days prior to the expiration of the SAM, staff will obtain and document any comments and suggestions concerning possible renewal and/or modifications to the SAM from the inmate. Approximately 90 days prior to the expiration of the SAM, the unit team and the supervising law enforcement agency case agent assigned to the inmate's case will meet with the inmate. During this meeting, the inmate may provide information concerning possible renewal and/or modification of the SAM and discuss any other issues concerning the SAM. The information obtained from the meeting with the inmate, along with the inmate's written comments and the memorandum summarizing the discussion with the inmate, will be forwarded through Legal Services, to the Warden, the Department of Justice officials responsible for making decisions concerning the renewal and/or modification of the SAM, including the appropriate United States Attorney's Office, the FBI or other relevant law enforcement agency, and the Office of Enforcement Operations in the criminal division of the United States Department of Justice, for review. The unit team will document the meeting in the Inmate Activity Record, located in the inmate's Central File.

63. This review by Department of Justice personnel, which incorporates information from the inmate, demonstrates that the officials carefully evaluate the specifics of the inmate's

⁴ SAM inmates who are not housed at the ADX may make a statement regarding renewal or modification prior to the expiration of their SAM.

situation and critically weigh safety and security concerns in determining whether SAMs were warranted. The multiple, multi-level review processes provide procedural safeguards.

64. An inmate who is subject to a SAM can object outside the formal SAM review procedures. He can give input about his situation during other BOP reviews, including his twice-yearly Program Reviews, a classification review, and Progress Reports. This input can include the inmate requesting a modification of the SAM. For example, if the inmate wants to communicate with a previously un-retained attorney to request representation, the inmate could seek modification of the SAM. Finally, inmates can file a lawsuit in federal court to challenge SAMs.

65. The Tenth Circuit Court of Appeals has confirmed that SAMs do *not* violate due process. It held that a SAMs inmate incarcerated at the ADX had no “constitutionally protected liberty interest in avoiding” the SAMs and no entitlement to procedural due process. *Gowadia v. Stearns*, 596 F. App’x 667, 673-74 (10th Cir. 2014). However, in reaching that conclusion, the Court of Appeals correctly recognized that inmates subject to SAM do receive procedural protections. *Id.*

66. Although the imposition of SAMs ordinarily does not violate procedural due process, a SAM cannot violate an inmate’s substantive rights. For example, it is well established that prisoners retain First Amendment rights. *O’Lone v. Estate of Shabazz*, 482 U.S. 342, 348 (1987). This includes, for example, a right to free-flowing incoming and outgoing mail. *Davis v. Goord*, 320 F.3d 346, 351 (2d Cir. 2003). SAMs that infringe on First Amendment rights of free speech and association may nevertheless be lawful if they are reasonably related to legitimate penological interests. *Turner v. Safley*, 482 U.S. 78, 89 (1987).

67. Likewise, egregious and inhumane conditions of confinement may constitute “cruel and unusual punishment” in violation of the Eighth Amendment. Prison officials must “provide humane conditions of confinement by ensuring inmates receive the basic necessities of adequate food, clothing, shelter, and medical care and by taking reasonable measures to guarantee the inmates' safety.” *Craig v. Eberly*, 164 F.3d 490, 495 (10th Cir.1998) (citations omitted). To prevail on a SAM claim related to a condition of confinement, the prisoner must show that (1) the condition complained of is sufficiently serious to implicate constitutional protection, and (2) prison officials acted with deliberate indifference to inmate health or safety. *Farmer v. Brennan*, 511 U.S. 825, 834 (1994) (citations omitted).⁵

68. Mr. Sickler points to a case in which a district court judge criticized the process surrounding SAMs. He fails to point out, however, that in that very case, the judge ruled *in favor* of the United States. The judge explained that the SAMs at issue were not so restrictive as to give rise to a protected liberty interest. *Yousef v. United States*, No. 12-cv-2585-RPM, 2014 WL 1908711, at *2-5 (D. Colo. May 13, 2014) (explaining why conditions of confinement for an ADX inmate subject to SAMs did not implicate a liberty interest, and concluding “that Yousef has not shown that his conditions of confinement are so atypical and impose such a hardship as to infringe upon the limited liberty left to him under his sentences”). *See also Nicholson v. Brennan*, No. 15-cv-01999, 2017 WL 4337896, at *9 (D. Colo. Sept. 28, 2107) (holding that inmate did not have a

⁵ Although Assange could bring such a claim, courts have previously held that the general conditions of confinement at ADX, while harsh, do not amount to a deprivation of the inmates’ Eighth Amendment rights to be free of cruel and unusual punishment. *Georgacarakos v. Wiley*, Civil Action No. 07-cv-01712-MSK-MEH, 2010 WL 1291833 (D. Colo. Mar. 30, 2010); *see also Sattar v. Gonzales*, Civil Action No. 07-cv-02698-WDM-KLM, 2009 WL 606115 (D. Colo. Mar. 6, 2009).

liberty interest in avoiding the conditions imposed by SAMs). Later, the judge explicitly rejected Yousef’s argument “that the SAMs renewal process is essentially a sham designed to impose SAMs on Yousef in perpetuity.” *Yousef v. United States*, No. 12-cv-2585-RPM, 2014 WL 2892251, at *2-3 (D. Colo. June 26, 2014) (denying inmate’s motion for relief from judgment).

69. Courts subject SAMs to meaningful review. For example, in *Mohammed v. Holder*, Civil Action No. 07-cv-02697-MSK-BNB, 2011 WL 4501959 (D. Colo. Sep. 29, 2011), a district court ruled that the government was not entitled to summary judgment on a claim that it was unreasonably limiting the defendant’s mail and communications. The inmate—and the court—pointed out that the Warden at ADX had recommended that the defendant be permitted to communicate with persons outside of his immediate family.

70. Mr. Sickler also claims that the imposition of SAMs, and the requirement that Assange’s attorneys agree to abide by them, will hinder Assange’s ability to mount a defense. At this point, whether SAMs would, in fact, be imposed on Assange at the ADC (or the BOP) is, of course, mere speculation. Nevertheless, the attorney affirmation requirement helps to protect national security and public safety. Incarceration provides no guarantee that a SAMs inmate will refrain from engaging in criminal conduct. *See, e.g., United States v. Salameh*, 152 F.3d 88, 107-08 (1998) (an incarcerated terrorist transmitted coded telephone messages to his co-conspirators); *United States v. Rahman*, 189 F.3d 88, 105-06 (1999) (a convicted terrorist provided guidance from prison to his followers for future terrorist attacks). Moreover, in at least one instance, an attorney violated SAMs to help her incarcerated client communicate with fellow terrorists. Lynn Stewart was convicted for smuggling statements from her client, the notorious “Blind Sheikh” Omar Abdel Rahman, to Egyptian jihadists. *United States v. Stewart*, 590 F.3d 93, 165 (2d Cir. 2009). Stewart

was not, as Mr. Sickler suggests, merely “revealing her client’s statements to the press.” Sickler Aff. ¶¶ 43.

71. Requiring attorneys to acknowledge the imposition of SAMs and abide by them properly protects national security and public safety. As the Second Circuit found in upholding Stewart’s criminal conviction, “[w]e have no basis upon which to entertain a doubt as to the authority of the Attorney General of the United States to ensure that reasonable measures [SAMs] are designed and implemented in an attempt to prevent imprisoned criminals who are considered dangerous despite their incarceration from engaging in or facilitating further acts of criminality from their prison cells.” *United States v. Stewart*, 590 F.3d at 111-12. The attorney affirmation requirement also helps to ensure that SAMs inmates communicate confidentially only with attorneys who are apprised of the SAMs prohibition on disseminating the inmates’ communications to third parties.

72. Mr. Sickler also misrepresents the situation with regard to attorneys who represent SAMs inmates. The affirmation, which simply confirms that counsel acknowledge and promise to abide by the terms of the SAMs, does not block the access of inmates to counsel or the courts; neither does it hinder attorneys from providing full and fair representation to inmates. Recently, for example, SAMs inmate Dzhokhar Tsarnaev, the convicted Boston marathon bomber, succeeded in overturning his death sentence through the representation of his large legal team, all of whom executed affirmations of the SAMs and had access to their client. *See United States v. Tsarnaev*, No. 16-6001, -- F.3d --, 2020 WL 43815878 (1st Cir. July 31, 2020). In short, there is no evidence to justify Mr. Sickler’s unsupported contention that “most lawyers” are “frightened” of SAMs, or that their ability to represent their clients is compromised.

F. The BOP Has Protocols in Place to Protect Inmates from COVID-19.

73. The BOP has protocols in place to protect inmates from COVID-19. Starting in January 2020, the BOP implemented its Pandemic Influenza contingency plan. The BOP continues to revise and update its action plan in response to the COVID-19 pandemic, and in response to the latest guidance from experts at the World Health Organization (“WHO”), the Centers for Disease Control and Prevention (“CDC”) and the Office of Personnel Management (“OPM”).

74. On March 1, 2020, the BOP implemented modifications to its normal operations to further lessen the possibility that COVID-19 spreads among staff and inmates. This included taking measures to reasonably limit inmate exposure to other inmates while continuing to allow inmates access to programs and services that are offered under normal operating procedures, such as mental health treatment; coordinating with the United States Marshals Service to significantly decrease the number of prisoners added to facilities during this time; and limit group gatherings while affording inmates access to commissary, laundry, showers, telephone, and TRULINCS or email access.

75. During the intervening months, the BOP has regularly updated its modified operations to limit the spread of COVID-19 amongst staff and inmates. On August 5, 2020, BOP implemented Phase Nine of its Action Plan, which currently governs operations. *See Exhibit D* to this Declaration. The current modified operations plan is an extension of the previous phases. Only limited group gathering is afforded, with attention to social distancing to the extent possible, to facilitate commissary, laundry, showers, telephone, and computer access. Further, BOP has severely limited the movement of inmates and detainees among its facilities, with exceptions for medical treatment and similar exigencies.

76. Every newly admitted inmate is screened for COVID-19 exposure risk factors and symptoms and tested for COVID. Inmates who are asymptomatic and test negative are placed in quarantine. Symptomatic inmates or inmates who test positive are immediately placed in medical isolation until they are cleared by medical staff as meeting CDC criteria for release from isolation. In addition, all staff are screened for symptoms. Staff registering a temperature of 100.4 degrees Fahrenheit or higher are barred from the facility on that basis alone. A staff member with a stuffy or runny nose can be placed on leave by a medical officer.

77. Contractor access to BOP facilities is restricted to only those performing essential services (e.g. medical or mental health care, religious, etc.) or those who perform necessary maintenance on essential systems. All volunteer visits are suspended absent authorization by the Deputy Director of BOP. Any contractor or volunteer who requires access will be screened for symptoms and risk factors.

78. To limit the number of people entering the facility and interacting with inmates, social visits were stopped as of March 13, 2020. To ensure that familial relationships are maintained throughout this disruption, BOP has increased detainees' telephone allowance to 500 minutes per month. On August 31, 2020, the BOP issued a Modification of Coronavirus (COVID-19) Phase Nine Action Plan, applying to social visiting. *See* Exhibit E to this Declaration. Specifically, social visiting in the BOP is projected to resume no later than Saturday, October 3, 2020, in accordance with the guidance issued in the memorandum. Wardens are to begin immediately developing local procedures to reinstate social visiting.

79. Tours of facilities are suspended. All staff and inmates have been and will continue to be issued appropriate face coverings and strongly encouraged to wear the face covering when in public areas when social distancing cannot be achieved.

80. The BOP recognizes that access to legal counsel remains a paramount requirement and seeks accommodate access to the maximum extent reasonably possible under the circumstances. Specifically, legal visits are permitted on a case-by-case basis after the attorney has been screened for infection in accordance with the screening protocols in place for prison staff, contractors, and visitors. Additionally, telephone calls and video conferencing with legal counsel are accommodated to the extent possible as detailed in the BOP's Phase Nine Action Plan. *See* Exhibit D.

81. The BOP has a website dedicated to providing information on the COVID-19 pandemic. *See* <https://www.bop.gov/coronavirus/> (last visited Sep. 1, 2020). The site is updated daily. As of September 1, 2020, the BOP had 127,145 federal inmates in BOP-managed institutions and 13,878 in community-based facilities. The BOP has approximately 36,000 staff members. 1,795 federal inmates and 667 BOP staff have confirmed positive test results for COVID-19, and 10,669 inmates and 929 staff members have tested positive, been isolated, and recovered from the virus. There have been 118 inmate deaths and two staff member deaths attributable to the virus. In sum, the BOP is carefully monitoring COVID-19 and making a serious effort to prevent the virus's spread among its inmate and staff populations.

82. To support his claim that BOP is ill-prepared to handle COVID-19, Mr. Sickler relies on a district court opinion from the Southern District of New York. *See* Sickler Aff. ¶¶ 35-36 (citing *United States v. Stephens*, No. 15-cr-95 (AJN), 2020 WL 1295155 (S.D.N.Y. Mar. 19,

2020)). That case concerned the Metropolitan Correctional Center (“MCC”), a pretrial detention facility in New York. In a more recent case, a judge on the same court denied a defendant’s application for pretrial release. *See United States v. Gumora*, 20-CR-11 (VSB), 2020 WL 1862361 (S.D.N.Y. April 14, 2020). The judge in *Gumora* pointed out that BOP had “developed and implemented a plan to mitigate the impact of COVID-19 on the federal prison population.” *Id.* at *10. The court found that, at least as to the MCC, implementation of the plan “appears to have limited the spread of the virus within the institution.” *Id.* at *11.

III. Definition of National Defense Information

83. Clarification of the law in the United States regarding the definition of information relating to “the national defense”, under Section 793 of Title 18 of the United States Code, may assist the Court. Case law in the United States establishes that, to be national defense information, the documents at issue must satisfy three criteria. First, the documents must generally relate to military matters or related activities of national preparedness. *See Gorin v. United States*, 312 U.S. 19, 28 (1941); *United States v. Rosen*, 445 F. Supp. 2d 602, 620 (E.D. Va. 2006) (“[T]he phrase ‘information relating to the national defense’ has consistently been construed broadly to include information dealing with military matters and more generally with matters relating to United States foreign policy and intelligence capabilities.”). Second, the information must be “closely held” by the U.S. government. *See United States v. Squillacote*, 221 F.3d 542, 579 (4th Cir. 2000) (“[I]nformation made public by the government as well as information never protected by the government is not national defense information.”); *United States v. Morison*, 844 F.2d 1057, 1071-72 (4th Cir. 1988). Third, disclosure of the documents must be potentially damaging to the United States or potentially useful to an enemy of the United States. *See Morison*, 844 F.2d at 1071-72

(approving jury instruction that the prosecution must prove that the information “would be potentially damaging to the United States or might be useful to an enemy of the United States.”).

84. To obtain a conviction, the government must prove those elements to the jury beyond a reasonable doubt. Assange, therefore, will have the opportunity to present evidence, cross-examination, and argument that the United States has failed to prove any or all of those elements.

Conclusion

85. I, Gordon D. Kromberg, an Assistant United States Attorney, attest under penalty of perjury that, on this 3rd day of September 2020, this document is true and accurate to the best of my knowledge, information, and belief.

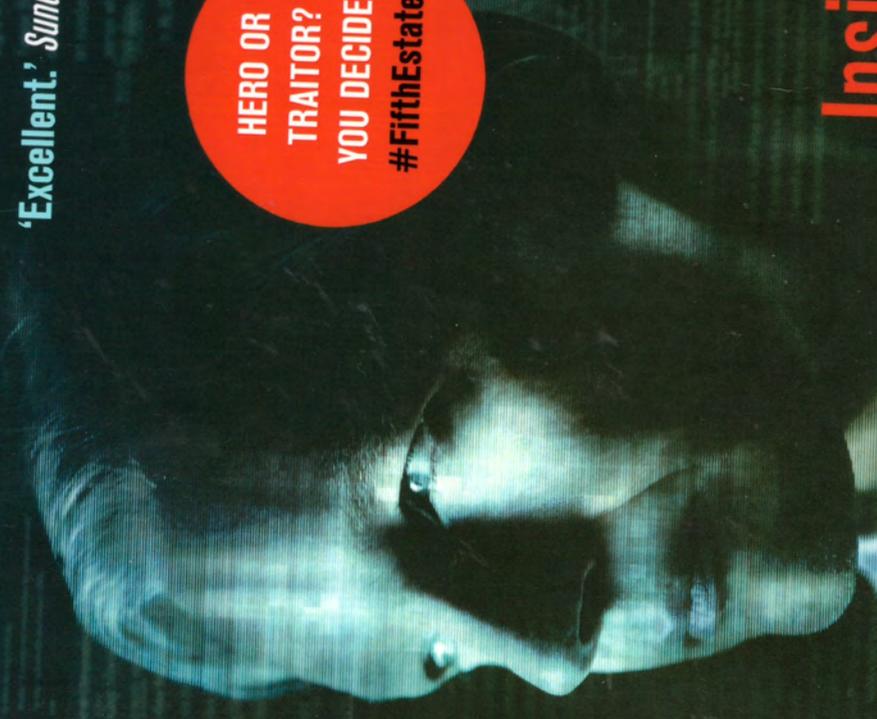

Gordon D. Kromberg
Assistant United States Attorney
Office of the United States Attorney
Alexandria, Virginia

David Leigh and Luke Harding

WIKILEAKS

'Excellent.' *Sunday Times*

HERO OR
TRAITOR?
YOU DECIDE.
#FifthEstate



**Inside
Julian Assange's
War on Secrecy**

DAVID LEIGH is one of Britain's best-known investigative journalists. He is Anthony Sampson professor of reporting at the journalism school of City University, London, and was investigations editor of the *Guardian* from 2000–2013. He is one of the founder members of the International Consortium of Investigative Journalists, a non-profit reporters' group headquartered in Washington DC.

David handled the publication in 2010 of secret US military and diplomatic data from WikiLeaks. His books include *High Time*, a biography of international cannabis smuggler Howard Marks, and *The Wilson Plot*, a study of misconduct by western intelligence agencies. He has two children and lives in London with his wife, the lawyer Jeannie Mackie.

LUKE HARDING is an award-winning foreign correspondent with the *Guardian*. He has reported from Delhi, Berlin and Moscow and covered wars in Afghanistan, Iraq and Libya. He is the author of two other books: *Mafia State: How One Reporter Became an Enemy of the Brutal New Russia*, and *The Liar: The Fall of Jonathan Aitken*, written with David Leigh and nominated for the Orwell Prize. He has also written for *Granta* magazine.

He lives in Hertfordshire with his wife, the freelance journalist Phoebe Taplin, and their two children.

I felt: 'You can't come in.'" Davies eventually agreed that while German radio was out, *Der Spiegel* could be in. Their reporters John Goetz and Marcel Rosenbach flew over to the war room.

"They fitted in very well. We liked them as people. They had lots of background expertise on Afghanistan," Davies says. Crucially, *Der Spiegel* sources had access to the German federal parliament's own investigation into the war in Afghanistan, including secret US military material. This proved vital in confirming that the details in the database the *Guardian* had been given were authentic.

The papers had another headache. Normally, with a story of this magnitude, the practical thing to do was to run it over several days. This maintained reader interest and helped sell more copies. In a previous campaign, on corporate tax avoidance, the *Guardian* had run a story a day non-stop for two weeks. This time, such a strategy was going to be impossible. For one thing, the two dailies in London and New York were now yoked to a weekly magazine in Germany. With only one shot at it, *Der Spiegel* would want to get all its stories out on Day One.

Secondly, and more gravely, none of the editors knew whether they would be allowed a Day Two at all. The US government's response might be so explosive that they sent their lawyers in with a gag order. So it was decided that, in the *Guardian's* case, the paper would run everything they had over 14 pages, on the day of launch. There was, of course, a downside to the approach although the launch of the Afghan war logs was to cause an immense uproar, it was difficult to find anyone in London the next day who had actually ploughed through all 14 pages. It was simply too much to read. For the Iraq logs, by which time it was clear the US government was not going to seek court injunctions and gag orders against the media, publication was to be more comfortably spread over a few days.

The knottiest problem surrounded redactions. The papers planned only to publish a relatively small number of significant

stories, and with them the text of the handful of relevant logs. WikiLeaks, on the other hand, intended simultaneously to unleash the lot. But many of the entries, particularly the "threat reports" derived from intelligence, mentioned the names of informants or those who had collaborated with US troops. In the vicious internecine politics of Afghanistan, such people could be in danger. Declan Walsh was among the first to realise this:

"I told David Leigh I was worried about the repercussions of publishing these names, who could easily be killed by the Taliban or other militant groups if identified. David agreed it was a concern and said he'd raised the issue with Julian, but he didn't seem concerned. That night, we went out to a Moorish restaurant, Moro, with the two German reporters. David broached the problem again with Julian. The response floored me. 'Well, they're informants,' he said. 'So, if they get killed, they've got it coming to them. They deserve it.' There was, for a moment, silence around the table. I think everyone was struck by what a callous thing that was to say.

"I thought about the American bases I'd visited, the Afghan characters I'd met in little villages and towns, the complex local politics that coloured everything, and the dilemmas faced by individuals during a bloody war. There was no way I'd like to put them at risk on the basis of a document prepared by some wet-behind-the-ears American GI, who may or may not have correctly understood the information they were receiving. The other thing that little exchange suggested to me was just how naive – or arrogant – Julian was when it came to the media. Apart from any moral considerations, he didn't seem to appreciate how the issue of naming informants was likely to rebound on the entire project."

Davies, too, was dismayed by the difficulty of persuading Assange to make redactions. "At first, he simply didn't get it, that it's not OK to publish stuff that will get people killed," Davies

By [Sari Horwitz](#)

November 25, 2013

The Justice Department has all but concluded it will not bring charges against WikiLeaks founder Julian Assange for publishing classified documents because government lawyers said they could not do so without also prosecuting U.S. news organizations and journalists, according to U.S. officials.

The officials stressed that a formal decision has not been made, and a grand jury investigating WikiLeaks remains impaneled, but they said there is little possibility of bringing a case against Assange, unless he is implicated in criminal activity other than releasing online top-secret military and diplomatic documents.

The Obama administration has charged government employees and contractors who leak classified information — such as former National Security Agency contractor [Edward Snowden](#) and former Army intelligence analyst Bradley Manning — with violations of the Espionage Act. But officials said that although Assange published classified documents, he did not leak them, something they said significantly affects their legal analysis.

“The problem the department has always had in investigating Julian Assange is there is no way to prosecute him for publishing information without the same theory being applied to journalists,” said former Justice Department spokesman Matthew Miller. “And if you are not going to prosecute journalists for publishing classified information, which the department is not, then there is no way to prosecute Assange.”

Justice officials said they looked hard at [Assange](#) but realized that they have what they described as a “New York Times problem.” If the Justice Department indicted Assange, it would also have to prosecute the New York Times and other news organizations and writers who published classified material, including The Washington Post and Britain’s Guardian newspaper, according to the officials, who spoke on the condition of anonymity to discuss internal deliberations.

WikiLeaks spokesman Kristinn Hrafnsson said last week that the anti-secrecy organization is skeptical “short of an open, official, formal confirmation that the U.S. government is not going to prosecute WikiLeaks.” Justice Department officials said it is unclear whether there will be a formal announcement should the grand jury investigation be formally closed.

“We have repeatedly asked the Department of Justice to tell us what the status of the investigation was with respect to Mr. Assange,” said Barry J. Pollack, a Washington attorney for Assange. “They have declined to do so. They have not informed us in any way that they are closing the investigation or have made a decision not to bring charges against Mr. Assange. While we would certainly welcome that development, it should not have taken the Department of Justice several years to come to the conclusion that it should not be investigating journalists for publishing truthful information.”

There have been persistent rumors that the grand jury investigation of Assange and WikiLeaks had secretly led to charges. Officials told The Post last week that there was no sealed indictment, and other officials have

Dealing With Assange and the WikiLeaks Secrets

By [Bill Keller](#)

Jan. 26, 2011

See how this article appeared when it was originally published on NYTimes.com.

This past June, Alan Rusbridger, the editor of The Guardian, phoned me and asked, mysteriously, whether I had any idea how to arrange a secure communication. Not really, I confessed. The Times doesn't have encrypted phone lines, or a Cone of Silence. Well then, he said, he would try to speak circumspectly. In a roundabout way, he laid out an unusual proposition: an organization called WikiLeaks, a secretive cadre of antisecrecy vigilantes, had come into possession of a substantial amount of classified United States government communications. WikiLeaks's leader, Julian Assange, an eccentric former computer hacker of Australian birth and no fixed residence, offered The Guardian half a million military dispatches from the battlefields of Afghanistan and Iraq. There might be more after that, including an immense bundle of confidential diplomatic cables. The Guardian suggested — to increase the impact as well as to share the labor of handling such a trove — that The New York Times be invited to share this exclusive bounty. The source agreed. Was I interested?

I was interested.

The adventure that ensued over the next six months combined the cloak-and-dagger intrigue of handling a vast secret archive with the more mundane feat of sorting, searching and understanding a mountain of data. As if that were not complicated enough, the project also entailed a source who was elusive, manipulative and volatile (and ultimately openly hostile to The Times and The Guardian); an international cast of journalists; company lawyers committed to keeping us within the bounds of the law; and an array of government officials who sometimes seemed as if they couldn't decide whether they wanted to engage us or arrest us. By the end of the year, the story of this wholesale security breach had outgrown the story of the actual contents of the secret documents and generated much breathless speculation that something — journalism, diplomacy, life as we know it — had profoundly changed forever.

Soon after Rusbridger's call, we sent Eric Schmitt, from our Washington bureau, to London. Schmitt has covered military affairs expertly for years, has read his share of classified military dispatches and has excellent judgment and an unflappable demeanor. His main assignment was to get a sense of the material. Was it genuine? Was it of public interest? He would also report back on the proposed mechanics of our collaboration with The Guardian and the German magazine Der Spiegel, which Assange invited as a third guest to his secret smorgasbord. Schmitt would also meet the WikiLeaks leader, who was known to a few Guardian journalists but not to us.

Schmitt's first call back to The Times was encouraging. There was no question in his mind that the Afghanistan dispatches were genuine. They were fascinating — a diary of a troubled war from the ground up. And there were intimations of more to come, especially classified cables from the entire constellation of American diplomatic outposts. WikiLeaks was holding those back for now, presumably to see how this venture with the establishment media worked out. Over the next few days, Schmitt huddled in a discreet office at The Guardian, sampling the trove of war dispatches and discussing the complexities of this project: how to organize and study such a voluminous cache of information; how to securely transport, store and share it; how journalists from three very different publications would work together without compromising their independence; and how we would all assure an appropriate distance from Julian Assange. We regarded Assange throughout as a source, not as a partner or collaborator, but he was a man who clearly had his own agenda.

By the time of the meetings in London, WikiLeaks had already acquired a measure of international fame or, depending on your point of view, notoriety. Shortly before I got the call from The Guardian, The New Yorker published a rich and colorful

profile of Assange, by Raffi Khatchadourian, who had embedded with the group. WikiLeaks's biggest coup to that point was the release, last April, of video footage taken from one of two U.S. helicopters involved in firing down on a crowd and a building in Baghdad in 2007, killing at least 18 people. While some of the people in the video were armed, others gave no indication of menace; two were in fact journalists for the news agency Reuters. The video, with its soundtrack of callous banter, was horrifying to watch and was an embarrassment to the U.S. military. But in its zeal to make the video a work of antiwar propaganda, WikiLeaks also released a version that didn't call attention to an Iraqi who was toting a rocket-propelled grenade and packaged the manipulated version under the tendentious rubric "Collateral Murder." (*See the edited and non-edited videos here.*)

Throughout our dealings, Assange was coy about where he obtained his secret cache. But the suspected source of the video, as well as the military dispatches and the diplomatic cables to come, was a disillusioned U.S. Army private first class named Bradley Manning, who had been arrested and was being kept in solitary confinement.

On the fourth day of the London meeting, Assange slouched into The Guardian office, a day late. Schmitt took his first measure of the man who would be a large presence in our lives. "He's tall — probably 6-foot-2 or 6-3 — and lanky, with pale skin, gray eyes and a shock of white hair that seizes your attention," Schmitt wrote to me later. "He was alert but disheveled, like a bag lady walking in off the street, wearing a dingy, light-colored sport coat and cargo pants, dirty white shirt, beat-up sneakers and filthy white socks that collapsed around his ankles. He smelled as if he hadn't bathed in days."

Assange shrugged a huge backpack off his shoulders and pulled out a stockpile of laptops, cords, cellphones, thumb drives and memory sticks that held the WikiLeaks secrets.

The reporters had begun preliminary work on the Afghanistan field reports, using a large Excel spreadsheet to organize the material, then plugging in search terms and combing the documents for newsworthy content. They had run into a puzzling incongruity: Assange said the data included dispatches from the beginning of 2004 through the end of 2009, but the material on the spreadsheet ended abruptly in April 2009. A considerable amount of material was missing. Assange, slipping naturally into the role of office geek, explained that they had hit the limits of Excel. Open a second spreadsheet, he instructed. They did, and the rest of the data materialized — a total of 92,000 reports from the battlefields of Afghanistan.

The reporters came to think of Assange as smart and well educated, extremely adept technologically but arrogant, thin-skinned, conspiratorial and oddly credulous. At lunch one day in The Guardian's cafeteria, Assange recounted with an air of great conviction a story about the archive in Germany that contains the files of the former Communist secret police, the Stasi. This office, Assange asserted, was thoroughly infiltrated by former Stasi agents who were quietly destroying the documents they were entrusted with protecting. The Der Spiegel reporter in the group, John Goetz, who has reported extensively on the Stasi, listened in amazement. That's utter nonsense, he said. Some former Stasi personnel were hired as security guards in the office, but the records were well protected.

Assange was openly contemptuous of the American government and certain that he was a hunted man. He told the reporters that he had prepared a kind of doomsday option. He had, he said, distributed highly encrypted copies of his entire secret archive to a multitude of supporters, and if WikiLeaks was shut down, or if he was arrested, he would disseminate the key to make the information public.

Schmitt told me that for all Assange's bombast and dark conspiracy theories, he had a bit of Peter Pan in him. One night, when they were all walking down the street after dinner, Assange suddenly started skipping ahead of the group. Schmitt and Goetz stared, speechless. Then, just as suddenly, Assange stopped, got back in step with them and returned to the conversation he had interrupted.

For the rest of the week Schmitt worked with David Leigh, The Guardian's investigations editor; Nick Davies, an investigative reporter for the paper; and Goetz, of Der Spiegel, to organize and sort the material. With help from two of The Times's best computer minds — Andrew Lehren and Aron Pilhofer — they figured out how to assemble the material into a conveniently searchable and secure database.

Journalists are characteristically competitive, but the group worked well together. They brainstormed topics to explore and

exchanged search results. Der Spiegel offered to check the logs against incident reports submitted by the German Army to its Parliament — partly as story research, partly as an additional check on authenticity.

Assange provided us the data on the condition that we not write about it before specific dates that WikiLeaks planned on posting the documents on a publicly accessible Web site. The Afghanistan documents would go first, after we had a few weeks to search the material and write our articles. The larger cache of Iraq-related documents would go later. Such embargoes — agreements not to publish information before a set date — are commonplace in journalism. Everything from studies in medical journals to the annual United States budget is released with embargoes. They are a constraint with benefits, the principal one being the chance to actually read and reflect on the material before publishing it into public view. As Assange surely knew, embargoes also tend to build suspense and amplify a story, especially when multiple news outlets broadcast it at once. The embargo was the only condition WikiLeaks would try to impose on us; what we wrote about the material was entirely up to us. Much later, some American news outlets reported that they were offered last-minute access to WikiLeaks documents if they signed contracts with financial penalties for early disclosure. The Times was never asked to sign anything or to pay anything. For WikiLeaks, at least in this first big venture, exposure was its own reward.

Back in New York we assembled a team of reporters, data experts and editors and quartered them in an out-of-the-way office. Andrew Lehren, of our computer-assisted-reporting unit, did the first cut, searching terms on his own or those suggested by other reporters, compiling batches of relevant documents and summarizing the contents. We assigned reporters to specific areas in which they had expertise and gave them password access to rummage in the data. This became the routine we would follow with subsequent archives.

An air of intrigue verging on paranoia permeated the project, perhaps understandably, given that we were dealing with a mass of classified material and a source who acted like a fugitive, changing crash pads, e-mail addresses and cellphones frequently. We used encrypted Web sites. Reporters exchanged notes via Skype, believing it to be somewhat less vulnerable to eavesdropping. On conference calls, we spoke in amateurish code. Assange was always “the source.” The latest data drop was “the package.” When I left New York for two weeks to visit bureaus in Pakistan and Afghanistan, where we assume that communications may be monitored, I was not to be copied on message traffic about the project. I never imagined that any of this would defeat a curious snoop from the National Security Agency or Pakistani intelligence. And I was never entirely sure whether that prospect made me more nervous than the cyberwiles of WikiLeaks itself. At a point when relations between the news organizations and WikiLeaks were rocky, at least three people associated with this project had inexplicable activity in their e-mail that suggested someone was hacking into their accounts.

From consultations with our lawyers, we were confident that reporting on the secret documents could be done within the law, but we speculated about what the government — or some other government — might do to impede our work or exact recriminations. And, the law aside, we felt an enormous moral and ethical obligation to use the material responsibly. While we assumed we had little or no ability to influence what WikiLeaks did, let alone what would happen once this material was loosed in the echo chamber of the blogosphere, that did not free us from the need to exercise care in our own journalism. From the beginning, we agreed that in our articles and in any documents we published from the secret archive, we would excise material that could put lives at risk.

Guided by reporters with extensive experience in the field, we redacted the names of ordinary citizens, local officials, activists, academics and others who had spoken to American soldiers or diplomats. We edited out any details that might reveal ongoing intelligence-gathering operations, military tactics or locations of material that could be used to fashion terrorist weapons. Three reporters with considerable experience of handling military secrets — Eric Schmitt, Michael Gordon and C. J. Chivers — went over the documents we considered posting. Chivers, an ex-Marine who has reported for us from several battlefields, brought a practiced eye and cautious judgment to the business of redaction. If a dispatch noted that Aircraft A left Location B at a certain time and arrived at Location C at a certain time, Chivers edited it out on the off chance that this could teach enemy forces something useful about the capabilities of that aircraft.

The first articles in the project, which we called the War Logs, were scheduled to go up on the Web sites of The Times, The Guardian and Der Spiegel on Sunday, July 25. We approached the White House days before that to get its reaction to the huge breach of secrecy as well as to specific articles we planned to write — including a major one about Pakistan’s

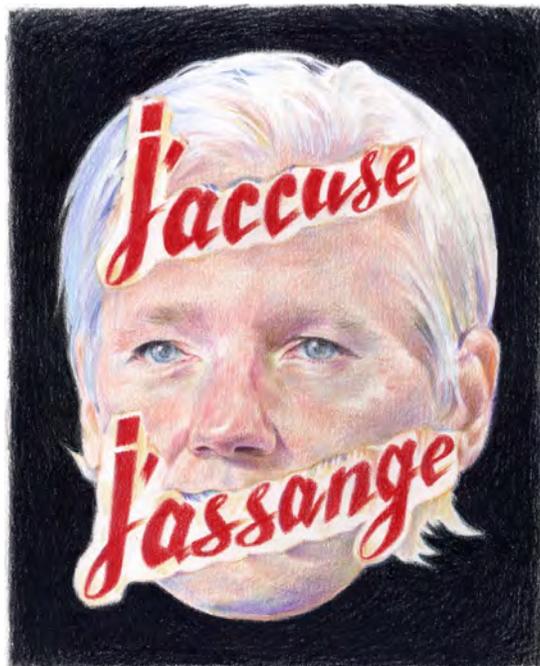
ambiguous role as an American ally. On July 24, the day before the War Logs went live, I attended a farewell party for Roger Cohen, a columnist for The Times and The International Herald Tribune, that was given by Richard Holbrooke, the Obama administration's special envoy to Afghanistan and Pakistan. A voracious consumer of inside information, Holbrooke had a decent idea of what was coming, and he pulled me away from the crowd to show me the fusillade of cabinet-level e-mail ricocheting through his BlackBerry, thus demonstrating both the frantic anxiety in the administration and, not incidentally, the fact that he was very much in the loop. The Pakistan article, in particular, would complicate his life. But one of Holbrooke's many gifts was his ability to make pretty good lemonade out of the bitterest lemons; he was already spinning the reports of Pakistani duplicity as leverage he could use to pull the Pakistanis back into closer alignment with American interests. Five months later, when Holbrooke — just 69, and seemingly indestructible — died of a torn aorta, I remembered that evening. And what I remembered best was that he was as excited to be on the cusp of a big story as I was.

We posted the articles on NYTimes.com the next day at 5 p.m. — a time picked to reconcile the different publishing schedules of the three publications. I was proud of what a crew of great journalists had done to fashion coherent and instructive reporting from a jumble of raw field reports, mostly composed in a clunky patois of military jargon and acronyms. The reporters supplied context, nuance and skepticism. There was much in that first round of articles worth reading, but my favorite single piece was one of the simplest. Chivers gathered all of the dispatches related to a single, remote, beleaguered American military outpost and stitched them together into a heartbreaking narrative. The dispatches from this outpost represent in miniature the audacious ambitions, gradual disillusionment and ultimate disappointment that Afghanistan has dealt to occupiers over the centuries.

If anyone doubted that the three publications operated independently, the articles we posted that day made it clear that we followed our separate muses. The Guardian, which is an openly left-leaning newspaper, used the first War Logs to emphasize civilian casualties in Afghanistan, claiming the documents disclosed that coalition forces killed “hundreds of civilians in unreported incidents,” underscoring the cost of what the paper called a “failing war.” Our reporters studied the same material but determined that all the major episodes of civilian deaths we found in the War Logs had been reported in The Times, many of them on the front page. (In fact, two of our journalists, Stephen Farrell and Sultan Munadi, were kidnapped by the Taliban while investigating one major episode near Kunduz. Munadi was killed during an ensuing rescue by British paratroopers.) The civilian deaths that had not been previously reported came in ones and twos and did not add up to anywhere near “hundreds.” Moreover, since several were either duplicated or missing from the reports, we concluded that an overall tally would be little better than a guess.

Another example: The Times gave prominence to the dispatches reflecting American suspicions that Pakistani intelligence was playing a double game in Afghanistan — nodding to American interests while abetting the Taliban. We buttressed the interesting anecdotal material of Pakistani double-dealing with additional reporting. The Guardian was unimpressed by those dispatches and treated them more dismissively.

Three months later, with the French daily Le Monde added to the group, we published Round 2, the Iraq War Logs, including articles on how the United States turned a blind eye to the torture of prisoners by Iraqi forces working with the U.S., how Iraq spawned an extraordinary American military reliance on private contractors and how extensively Iran had meddled in the conflict.



Artwork by Eric Yahnker

By this time, The Times's relationship with our source had gone from wary to hostile. I talked to Assange by phone a few times and heard out his complaints. He was angry that we declined to link our online coverage of the War Logs to the WikiLeaks Web site, a decision we made because we feared — rightly, as it turned out — that its trove would contain the names of low-level informants and make them Taliban targets. "Where's the respect?" he demanded. "Where's the respect?" Another time he called to tell me how much he disliked our profile of Bradley Manning, the Army private suspected of being the source of WikiLeaks's most startling revelations. The article traced Manning's childhood as an outsider and his distress as a gay man in the military. Assange complained that we "psychologicalized" Manning and gave short shrift to his "political awakening."

The final straw was a front-page profile of Assange by John Burns and Ravi Somaiya, published Oct. 24, that revealed fractures within WikiLeaks, attributed by Assange's critics to his imperious management style. Assange denounced the article to me, and in various public forums, as "a smear."

Assange was transformed by his outlaw celebrity. The derelict with the backpack and the sagging socks now wore his hair dyed and styled, and he favored fashionably skinny suits and ties. He became a kind of cult figure for the European young and leftish and was evidently a magnet for women. Two Swedish women filed police complaints claiming that Assange insisted on having sex without a condom; Sweden's strict laws on nonconsensual sex categorize such behavior as rape, and a prosecutor issued a warrant to question Assange, who initially described it as a plot concocted to silence or discredit WikiLeaks.

I came to think of Julian Assange as a character from a Stieg Larsson thriller — a man who could figure either as hero or villain in one of the megaselling Swedish novels that mix hacker counterculture, high-level conspiracy and sex as both recreation and violation.

In October, WikiLeaks gave The Guardian its third archive, a quarter of a million communications between the U.S. State Department and its outposts around the globe. This time, Assange imposed a new condition: The Guardian was not to share the material with The New York Times. Indeed, he told Guardian journalists that he opened discussions with two other American news organizations — The Washington Post and the McClatchy chain — and intended to invite them in as replacements for The Times. He also enlarged his recipient list to include El País, the leading Spanish-language newspaper.

The Guardian was uncomfortable with Assange's condition. By now the journalists from The Times and The Guardian had a good working relationship. The Times provided a large American audience for the revelations, as well as access to the U.S.

government for comment and context. And given the potential legal issues and public reaction, it was good to have company in the trenches. Besides, we had come to believe that Assange was losing control of his stockpile of secrets. An independent journalist, Heather Brooke, had obtained material from a WikiLeaks dissident and joined in a loose alliance with The Guardian. Over the coming weeks, batches of cables would pop up in newspapers in Lebanon, Australia and Norway. David Leigh, The Guardian's investigations editor, concluded that these rogue leaks released The Guardian from any pledge, and he gave us the cables.

On Nov. 1, Assange and two of his lawyers burst into Alan Rusbridger's office, furious that The Guardian was asserting greater independence and suspicious that The Times might be in possession of the embassy cables. Over the course of an eight-hour meeting, Assange intermittently raged against The Times — especially over our front-page profile — while The Guardian journalists tried to calm him. In midstorm, Rusbridger called me to report on Assange's grievances and relay his demand for a front-page apology in The Times. Rusbridger knew that this was a nonstarter, but he was buying time for the tantrum to subside. In the end, both he and Georg Mascolo, editor in chief of Der Spiegel, made clear that they intended to continue their collaboration with The Times; Assange could take it or leave it. Given that we already had all of the documents, Assange had little choice. Over the next two days, the news organizations agreed on a timetable for publication.

The following week, we sent Ian Fisher, a deputy foreign editor who was a principal coordinator on our processing of the embassy cables, to London to work out final details. The meeting went smoothly, even after Assange arrived. "Freakishly good behavior," Fisher e-mailed me afterward. "No yelling or crazy mood swings." But after dinner, as Fisher was leaving, Assange smirked and offered a parting threat: "Tell me, are you in contact with your legal counsel?" Fisher replied that he was. "You had better be," Assange said.

Fisher left London with an understanding that we would continue to have access to the material. But just in case, we took out a competitive insurance policy. We had Scott Shane, a Washington correspondent, pull together a long, just-in-case article summing up highlights of the cables, which we could quickly post on our Web site. If WikiLeaks sprang another leak, we would be ready.

Because of the range of the material and the very nature of diplomacy, the embassy cables were bound to be more explosive than the War Logs. Dean Baquet, our Washington bureau chief, gave the White House an early warning on Nov. 19. The following Tuesday, two days before Thanksgiving, Baquet and two colleagues were invited to a windowless room at the State Department, where they encountered an unsmiling crowd. Representatives from the White House, the State Department, the Office of the Director of National Intelligence, the C.I.A., the Defense Intelligence Agency, the F.B.I. and the Pentagon gathered around a conference table. Others, who never identified themselves, lined the walls. A solitary note-taker tapped away on a computer.

The meeting was off the record, but it is fair to say the mood was tense. Scott Shane, one reporter who participated in the meeting, described "an undertone of suppressed outrage and frustration."

Subsequent meetings, which soon gave way to daily conference calls, were more businesslike. Before each discussion, our Washington bureau sent over a batch of specific cables that we intended to use in the coming days. They were circulated to regional specialists, who funneled their reactions to a small group at State, who came to our daily conversations with a list of priorities and arguments to back them up. We relayed the government's concerns, and our own decisions regarding them, to the other news outlets.

The administration's concerns generally fell into three categories. First was the importance of protecting individuals who had spoken candidly to American diplomats in oppressive countries. We almost always agreed on those and were grateful to the government for pointing out some we overlooked.

"We were all aware of dire stakes for some of the people named in the cables if we failed to obscure their identities," Shane wrote to me later, recalling the nature of the meetings. Like many of us, Shane has worked in countries where dissent can mean prison or worse. "That sometimes meant not just removing the name but also references to institutions that might give a clue to an identity and sometimes even the dates of conversations, which might be compared with surveillance tapes of an American Embassy to reveal who was visiting the diplomats that day"

The second category included sensitive American programs, usually related to intelligence. We agreed to withhold some of this information, like a cable describing an intelligence-sharing program that took years to arrange and might be lost if exposed. In other cases, we went away convinced that publication would cause some embarrassment but no real harm.

The third category consisted of cables that disclosed candid comments by and about foreign officials, including heads of state. The State Department feared publication would strain relations with those countries. We were mostly unconvinced.

The embassy cables were a different kind of treasure from the War Logs. For one thing, they covered the entire globe — virtually every embassy, consulate and interest section that the United States maintains. They contained the makings of many dozens of stories: candid American appraisals of foreign leaders, narratives of complicated negotiations, allegations of corruption and duplicity, countless behind-the-scenes insights. Some of the material was of narrow local interest; some of it had global implications. Some provided authoritative versions of events not previously fully understood. Some consisted of rumor and flimsy speculation.

Unlike most of the military dispatches, the embassy cables were written in clear English, sometimes with wit, color and an ear for dialogue. (“Who knew,” one of our English colleagues marveled, “that American diplomats could write?”)

Even more than the military logs, the diplomatic cables called for context and analysis. It was important to know, for example, that cables sent from an embassy are routinely dispatched over the signature of the ambassador and those from the State Department are signed by the secretary of state, regardless of whether the ambassador or secretary had actually seen the material. It was important to know that much of the communication between Washington and its outposts is given even more restrictive classification — top secret or higher — and was thus missing from this trove. We searched in vain, for example, for military or diplomatic reports on the fate of Pat Tillman, the former football star and Army Ranger who was killed by friendly fire in Afghanistan. We found no reports on how Osama bin Laden eluded American forces in the mountains of Tora Bora. (In fact, we found nothing but second- and thirdhand rumors about bin Laden.) If such cables exist, they were presumably classified top secret or higher.

And it was important to remember that diplomatic cables are versions of events. They can be speculative. They can be ambiguous. They can be wrong.

One of our first articles drawn from the diplomatic cables, for example, reported on a secret intelligence assessment that Iran had obtained a supply of advanced missiles from North Korea, missiles that could reach European capitals. Outside experts long suspected that Iran obtained missile parts but not the entire weapons, so this glimpse of the official view was revealing. The Washington Post fired back with a different take, casting doubt on whether the missile in question had been transferred to Iran or whether it was even a workable weapon. We went back to the cables — and the experts — and concluded in a subsequent article that the evidence presented “a murkier picture.”

The tension between a newspaper’s obligation to inform and the government’s responsibility to protect is hardly new. At least until this year, nothing The Times did on my watch caused nearly so much agitation as two articles we published about tactics employed by the Bush administration after the attacks of Sept. 11, 2001. The first, which was published in 2005 and won a Pulitzer Prize, revealed that the National Security Agency was eavesdropping on domestic phone conversations and e-mail without the legal courtesy of a warrant. The other, published in 2006, described a vast Treasury Department program to screen international banking records.

I have vivid memories of sitting in the Oval Office as President George W. Bush tried to persuade me and the paper’s publisher to withhold the eavesdropping story, saying that if we published it, we should share the blame for the next terrorist attack. We were unconvinced by his argument and published the story, and the reaction from the government — and conservative commentators in particular — was vociferous.

This time around, the Obama administration’s reaction was different. It was, for the most part, sober and professional. The Obama White House, while strongly condemning WikiLeaks for making the documents public, did not seek an injunction to halt publication. There was no Oval Office lecture. On the contrary, in our discussions before publication of our articles, White House officials, while challenging some of the conclusions we drew from the material, thanked us for handling the

documents with care. The secretaries of state and defense and the attorney general resisted the opportunity for a crowd-pleasing orgy of press bashing. There has been no serious official talk — unless you count an ambiguous hint by Senator Joseph Lieberman — of pursuing news organizations in the courts. Though the release of these documents was certainly embarrassing, the relevant government agencies actually engaged with us in an attempt to prevent the release of material genuinely damaging to innocent individuals or to the national interest.

The broader public reaction was mixed — more critical in the first days; more sympathetic as readers absorbed the articles and the sky did not fall; and more hostile to WikiLeaks in the U.S. than in Europe, where there is often a certain pleasure in seeing the last superpower taken down a peg.

In the days after we began our respective series based on the embassy cables, Alan Rusbridger and I went online to answer questions from readers. The Guardian, whose readership is more sympathetic to the guerrilla sensibilities of WikiLeaks, was attacked for being too fastidious about redacting the documents: How dare you censor this material? What are you hiding? Post everything now! The mail sent to The Times, at least in the first day or two, came from the opposite field. Many readers were indignant and alarmed: Who needs this? How dare you? What gives you the right?



Artwork by Barry Falls

Much of the concern reflected a genuine conviction that in perilous times the president needs extraordinary powers, unfettered by Congressional oversight, court meddling or the strictures of international law and certainly safe from nosy reporters. That is compounded by a popular sense that the elite media have become too big for their britches and by the fact that our national conversation has become more polarized and strident.

Although it is our aim to be impartial in our presentation of the news, our attitude toward these issues is far from indifferent. The journalists at The Times have a large and personal stake in the country's security. We live and work in a city that has been tragically marked as a favorite terrorist target, and in the wake of 9/11 our journalists plunged into the ruins to tell the story of what happened here. Moreover, The Times has nine staff correspondents assigned to the two wars still being waged in the wake of that attack, plus a rotating cast of photographers, visiting writers and scores of local stringers and support staff. They work in this high-risk environment because, while there are many places you can go for opinions about the war, there are few places — and fewer by the day — where you can go to find honest, on-the-scene reporting about what is happening. We take extraordinary precautions to keep them safe, but we have had two of our Iraqi journalists murdered for doing their jobs. We have had four journalists held hostage by the Taliban — two of them for seven months. We had one

Afghan journalist killed in a rescue attempt. Last October, while I was in Kabul, we got word that a photographer embedded for us with troops near Kandahar stepped on an improvised mine and lost both his legs.

We are invested in the struggle against murderous extremism in another sense. The virulent hatred espoused by terrorists, judging by their literature, is directed not just against our people and our buildings but also at our values and at our faith in the self-government of an informed electorate. If the freedom of the press makes some Americans uneasy, it is anathema to the ideologists of terror.

So we have no doubts about where our sympathies lie in this clash of values. And yet we cannot let those sympathies transform us into propagandists, even for a system we respect.

I'm the first to admit that news organizations, including this one, sometimes get things wrong. We can be overly credulous (as in some of the prewar reporting about Iraq's supposed weapons of mass destruction) or overly cynical about official claims and motives. We may err on the side of keeping secrets (President Kennedy reportedly wished, after the fact, that The Times had published what it knew about the planned Bay of Pigs invasion, which possibly would have helped avert a bloody debacle) or on the side of exposing them. We make the best judgments we can. When we get things wrong, we try to correct the record. A free press in a democracy can be messy. But the alternative is to give the government a veto over what its citizens are allowed to know. Anyone who has worked in countries where the news diet is controlled by the government can sympathize with Thomas Jefferson's oft-quoted remark that he would rather have newspapers without government than government without newspapers.

The intentions of our founders have rarely been as well articulated as they were by Justice Hugo Black 40 years ago, concurring with the Supreme Court ruling that stopped the government from suppressing the secret Vietnam War history called the Pentagon Papers: "The government's power to censor the press was abolished so that the press would remain forever free to censure the government. The press was protected so that it could bare the secrets of government and inform the people."

There is no neat formula for maintaining this balance. In practice, the tension between our obligation to inform and the government's obligation to protect plays out in a set of rituals. As one of my predecessors, Max Frankel, then the Washington bureau chief, wrote in a wise affidavit filed during the Pentagon Papers case: "For the vast majority of 'secrets,' there has developed between the government and the press (and Congress) a rather simple rule of thumb: The government hides what it can, pleading necessity as long as it can, and the press pries out what it can, pleading a need and a right to know. Each side in this 'game' regularly 'wins' and 'loses' a round or two. Each fights with the weapons at its command. When the government loses a secret or two, it simply adjusts to a new reality."

In fact, leaks of classified material — sometimes authorized — are part of the way business is conducted in Washington, as one wing of the bureaucracy tries to one-up another or officials try to shift blame or claim credit or advance or confound a particular policy. For further evidence that our government is highly selective in its approach to secrets, look no further than Bob Woodward's all-but-authorized accounts of the innermost deliberations of our government.

The government surely cheapens secrecy by deploying it so promiscuously. According to the Pentagon, about 500,000 people have clearance to use the database from which the secret cables were pilfered. Weighing in on the WikiLeaks controversy in The Guardian, Max Frankel remarked that secrets shared with such a legion of "cleared" officials, including low-level army clerks, "are not secret." Governments, he wrote, "must decide that the random rubber-stamping of millions of papers and computer files each year does not a security system make."

Beyond the basic question of whether the press should publish secrets, criticism of the WikiLeaks documents generally fell into three themes: 1. That the documents were of dubious value, because they told us nothing we didn't already know. 2. That the disclosures put lives at risk — either directly, by identifying confidential informants, or indirectly, by complicating our ability to build alliances against terror. 3. That by doing business with an organization like WikiLeaks, The Times and other news organizations compromised their impartiality and independence.

I'm a little puzzled by the complaint that most of the embassy traffic we disclosed did not profoundly change our

understanding of how the world works. Ninety-nine percent of what we read or hear on the news does not profoundly change our understanding of how the world works. News mostly advances by inches and feet, not in great leaps. The value of these documents — and I believe they have immense value — is not that they expose some deep, unsuspected perfidy in high places or that they upend your whole view of the world. For those who pay close attention to foreign policy, these documents provide texture, nuance and drama. They deepen and correct your understanding of how things unfold; they raise or lower your estimation of world leaders. For those who do not follow these subjects as closely, the stories are an opportunity to learn more. If a project like this makes readers pay attention, think harder, understand more clearly what is being done in their name, then we have performed a public service. And that does not count the impact of these revelations on the people most touched by them. WikiLeaks cables in which American diplomats recount the extravagant corruption of Tunisia's rulers helped fuel a popular uprising that has overthrown the government.

As for the risks posed by these releases, they are real. WikiLeaks's first data dump, the publication of the Afghanistan War Logs, included the names of scores of Afghans that The Times and other news organizations had carefully purged from our own coverage. Several news organizations, including ours, reported this dangerous lapse, and months later a Taliban spokesman claimed that Afghan insurgents had been perusing the WikiLeaks site and making a list. I anticipate, with dread, the day we learn that someone identified in those documents has been killed.

WikiLeaks was roundly criticized for its seeming indifference to the safety of those informants, and in its subsequent postings it has largely followed the example of the news organizations and redacted material that could get people jailed or killed. Assange described it as a "harm minimization" policy. In the case of the Iraq war documents, WikiLeaks applied a kind of robo-redaction software that stripped away names (and rendered the documents almost illegible). With the embassy cables, WikiLeaks posted mostly documents that had already been redacted by The Times and its fellow news organizations. And there were instances in which WikiLeaks volunteers suggested measures to enhance the protection of innocents. For example, someone at WikiLeaks noticed that if the redaction of a phrase revealed the exact length of the words, an alert foreign security service might match the number of letters to a name and affiliation and thus identify the source. WikiLeaks advised everyone to substitute a dozen uppercase X's for each redacted passage, no matter how long or short.

Whether WikiLeaks's "harm minimization" is adequate, and whether it will continue, is beyond my power to predict or influence. WikiLeaks does not take guidance from The New York Times. In the end, I can answer only for what my own paper has done, and I believe we have behaved responsibly.

The idea that the mere publication of such a wholesale collection of secrets will make other countries less willing to do business with our diplomats seems to me questionable. Even Defense Secretary Robert Gates called this concern "overwrought." Foreign governments cooperate with us, he pointed out, not because they necessarily love us, not because they trust us to keep their secrets, but because they need us. It may be that for a time diplomats will choose their words more carefully or circulate their views more narrowly, but WikiLeaks has not repealed the laws of self-interest. A few weeks after we began publishing articles about the embassy cables, David Sanger, our chief Washington correspondent, told me: "At least so far, the evidence that foreign leaders are no longer talking to American diplomats is scarce. I've heard about nervous jokes at the beginning of meetings, along the lines of 'When will I be reading about this conversation?' But the conversations are happening. . . . American diplomacy has hardly screeched to a halt."

As for our relationship with WikiLeaks, Julian Assange has been heard to boast that he served as a kind of puppet master, recruiting several news organizations, forcing them to work in concert and choreographing their work. This is characteristic braggadocio — or, as my Guardian colleagues would say, bollocks. Throughout this experience we have treated Assange as a source. I will not say "a source, pure and simple," because as any reporter or editor can attest, sources are rarely pure or simple, and Assange was no exception. But the relationship with sources is straightforward: you don't necessarily endorse their agenda, echo their rhetoric, take anything they say at face value, applaud their methods or, most important, allow them to shape or censor your journalism. Your obligation, as an independent news organization, is to verify the material, to supply context, to exercise responsible judgment about what to publish and what not to publish and to make sense of it. That is what we did.

But while I do not regard Assange as a partner, and I would hesitate to describe what WikiLeaks does as journalism, it is chilling to contemplate the possible government prosecution of WikiLeaks for making secrets public, let alone the passage of new laws to punish the dissemination of classified information, as some have advocated. Taking legal recourse against a government official who violates his trust by divulging secrets he is sworn to protect is one thing. But criminalizing the publication of such secrets by someone who has no official obligation seems to me to run up against the First Amendment and the best traditions of this country. As one of my colleagues asks: If Assange were an understated professorial type rather than a character from a missing Stieg Larsson novel, and if WikiLeaks were not suffused with such glib antipathy toward the United States, would the reaction to the leaks be quite so ferocious? And would more Americans be speaking up against the threat of reprisals?

Whether the arrival of WikiLeaks has fundamentally changed the way journalism is made, I will leave to others and to history. Frankly, I think the impact of WikiLeaks on the culture has probably been overblown. Long before WikiLeaks was born, the Internet transformed the landscape of journalism, creating a wide-open and global market with easier access to audiences and sources, a quicker metabolism, a new infrastructure for sharing and vetting information and a diminished respect for notions of privacy and secrecy. Assange has claimed credit on several occasions for creating something he calls “scientific journalism,” meaning that readers are given the raw material to judge for themselves whether the journalistic write-ups are trustworthy. But newspapers have been publishing texts of documents almost as long as newspapers have existed — and ever since the Internet eliminated space restrictions, we have done so copiously.

Nor is it clear to me that WikiLeaks represents some kind of cosmic triumph of transparency. If the official allegations are to be believed, most of WikiLeaks’s great revelations came from a single anguished Army private — anguished enough to risk many years in prison. It’s possible that the creation of online information brokers like WikiLeaks and OpenLeaks, a breakaway site announced in December by a former Assange colleague named Daniel Domscheit-Berg, will be a lure for whistle-blowers and malcontents who fear being caught consorting directly with a news organization like mine. But I suspect we have not reached a state of information anarchy. At least not yet.

As 2010 wound down, The Times and its news partners held a conference call to discuss where we go from here. The initial surge of articles drawn from the secret cables was over. More would trickle out but without a fixed schedule. We agreed to continue the redaction process, and we agreed we would all urge WikiLeaks to do the same. But this period of intense collaboration, and of regular contact with our source, was coming to a close.

Just before Christmas, Ian Katz, The Guardian’s deputy editor, went to see Assange, who had been arrested in London on the Swedish warrant, briefly jailed and bailed out by wealthy admirers and was living under house arrest in a country manor in East Anglia while he fought Sweden’s attempt to extradite him. The flow of donations to WikiLeaks, which he claimed hit 100,000 euros a day at its peak, was curtailed when Visa, MasterCard and PayPal refused to be conduits for contributors — prompting a concerted assault on the Web sites of those companies by Assange’s hacker sympathizers. He would soon sign a lucrative book deal to finance his legal struggles.

The Guardian seemed to have joined The Times on Assange’s enemies list, first for sharing the diplomatic cables with us, then for obtaining and reporting on the unredacted record of the Swedish police complaints against Assange. (Live by the leak. . . .) In his fury at this perceived betrayal, Assange granted an interview to The Times of London, in which he vented his displeasure with our little media consortium. If he thought this would ingratiate him with The Guardian rival, he was naïve. The paper happily splashed its exclusive interview, then followed it with an editorial calling Assange a fool and a hypocrite.

At the mansion in East Anglia, Assange seated Katz before a roaring fire in the drawing room and ruminated for four hours about the Swedish case, his financial troubles and his plan for a next phase of releases. He talked vaguely about secrets still in his quiver, including what he regards as a damning cache of e-mail from inside an American bank.

He spun out an elaborate version of a U.S. Justice Department effort to exact punishment for his assault on American secrecy. If he was somehow extradited to the United States, he said, “I would still have a high chance of being killed in the U.S. prison system, Jack Ruby style, given the continual calls for my murder by senior and influential U.S. politicians.”

While Assange mused darkly in his exile, one of his lawyers sent out a mock Christmas card that suggested at least someone on the WikiLeaks team was not lacking a sense of the absurd.

The message:

“Dear kids,

Santa is Mum & Dad.

Love,

WikiLeaks.”

The Guardian

This article is more than **9 years old**

WikiLeaks publishes full cache of unredacted cables

Former media partners condemn WikiLeaks' decision to make public documents identifying activists and whistleblowers



WikiLeaks has published its full archive, including diplomatic cables marked by the US to indicate sources could be in danger.
Photograph: Karen Bleier/AFP/Getty Images

James Ball

Fri 2 Sep 2011 12.55 BST

WikiLeaks has published its full archive of 251,000 secret US diplomatic cables, without redactions, potentially exposing thousands of individuals named in the documents to detention, harm or putting their lives in danger.

The move has been strongly condemned by the five previous media partners - the Guardian, New York Times, El Pais, Der Spiegel and Le Monde - who have worked with WikiLeaks publishing carefully selected and redacted documents.

"We deplore the decision of WikiLeaks to publish the unredacted state department cables, which may put sources at risk," the organisations said in a joint statement.

"Our previous dealings with WikiLeaks were on the clear basis that we would only publish cables which had been subjected to a thorough joint editing and clearance process. We will continue to defend our previous collaborative publishing endeavour. We cannot defend the needless publication of the complete data - indeed, we are united in condemning it.

"The decision to publish by Julian Assange was his, and his alone."

Diplomats, governments, human rights charities and media organisations had urged WikiLeaks's founder, Assange, not to publish the full cache of cables without careful source protection.

The newly published archive contains more than 1,000 cables identifying individual activists; several thousand labelled with a tag used by the US to mark sources it believes could be placed in danger; and more than 150 specifically mentioning whistleblowers.

The cables also contain references to people persecuted by their governments, victims of sex offences, and locations of sensitive government installations and infrastructure.

WikiLeaks has published its full archive in an easily accessible and searchable manner, the first time the content has been made widely available to those without sophisticated technical skills.

It conducted a poll of its Twitter followers to decide whether to publish the documents, which it initially said was running at "100 to one" in favour of publishing. WikiLeaks did not disclose the final tallies, nor how many individuals responded to its poll.

Reporters Without Borders, a press freedom group which had been maintaining a backup version of the WikiLeaks site, revoked its support for the whistleblowing site in the wake of the decision.

"Some of the new cables have reportedly not been redacted and show the names of informants in various countries, including Israel, Jordan, Iran and Afghanistan," it said in a statement. "While it has not been demonstrated that lives have so far been put in danger by these revelations, the repercussions they could have for informants, such as dismissal, physical attacks and other reprisals, cannot be neglected."

The whistleblowing website began releasing the cables in December 2010, in conjunction with five media organisations including the Guardian. The mainstream news organisations carefully selected cables and before publication removed any information which could lead to sensitive sources being identified.

WikiLeaks claimed its disclosure was prompted after conflicts between Assange and former WikiLeaks associates led to one highlighting an error made months before. When passing the documents to the Guardian, Assange created a temporary web server and placed an encrypted file containing the documents on it. The Guardian was led to believe this was a temporary file and the server would be taken offline after a period of hours.

However, former WikiLeaks staff member Daniel Domscheit-Berg, who parted acrimoniously with WikiLeaks, said instead of following standard security precautions and creating a temporary folder, Assange instead re-used WikiLeaks's "master password". This password was then unwittingly placed in the Guardian's book on the embassy cables, which was published in February 2011.

Separately, a WikiLeaks activist had placed the encrypted files on BitTorrent, a peer-to-peer file sharing network, in the hours before Julian Assange was imprisoned pending extradition proceedings in December 2010, as a form of insurance for the site. Fewer than five people knew of the existence of the site.

As former activists' disillusionment with WikiLeaks grew, one told German magazine Freitag about the link between the publicly available password and files in an attempt to highlight sloppy security at WikiLeaks. The magazine published the story with no information to identify the password or files.

WikiLeaks then published a series of increasingly detailed tweets giving clues about where the password might be found as part of its attempts to deny security failings on its own part. These are believed to have led a small group of internet users to find the files, which were published in a difficult-to-access format requiring significant technical skill, on rival leak site Cryptome.

Domscheit-Berg, often referred to as Assange's former deputy at WikiLeaks, condemned the password reuse. "The file was never supposed to be shared with anyone at all," he said. "To get a copy you would usually make a new copy with a new password. He [Assange] was too lazy to create something new."

Since you're here ...

... we have a small favour to ask. Millions are flocking to the Guardian for open, independent, quality news every day, and readers in 180 countries around the world now support us financially.

We believe everyone deserves access to information that's grounded in science and truth, and analysis rooted in authority and integrity. That's why we made a different choice: to keep our reporting open for all readers, regardless of where they live or what they can afford to pay.

The Guardian has no shareholders or billionaire owner, meaning our journalism is free from bias and vested interests - this makes us different. Our editorial independence and autonomy allows us to provide fearless investigations and analysis of those with political and commercial power. We can give a voice to the oppressed and neglected, and help bring about a brighter, fairer future. Your support protects this.

Supporting us means investing in Guardian journalism for tomorrow and the years ahead. The more readers funding our work, the more questions we can ask, the deeper we can dig, and the greater the impact we can have. We're determined to provide reporting that helps each of us better understand the world, and take actions that challenge, unite, and inspire change.

Your support means we can keep our journalism open, so millions more have free access to the high-quality, trustworthy news they deserve. So we seek your support not simply to survive, but to grow our journalistic ambitions and sustain our model for open, independent reporting.

Pakistani-Taliban Link Is Suspected

A Close-Up View of the War

Attack at a Gritty Outpost

A Note to Readers

Origin of the Documents

Read Selected Documents

More About These Articles >

A NOTE TO READERS

Piecing Together the Reports, and Deciding What to Publish

Published: July 25, 2010

The articles published today are based on thousands of United States military incident and intelligence reports — records of engagements, mishaps, intelligence on enemy activity and other events from the war in Afghanistan — that were made public on Sunday on the Internet. The New York Times, [The Guardian newspaper](#) in London, and the German magazine [Der Spiegel](#) were given access to the material several weeks ago. These reports are used by desk officers in the Pentagon and troops in the field when they make operational plans and prepare briefings on the situation in the war zone. Most of the reports are routine, even mundane, but many add insights, texture and context to a war that has been waged for nearly nine years.

LINKEDIN

PRINT

REPRINTS

SHARE

Readers'



Comments and Reaction

Share your thoughts about the classified documents on the At War blog, which is following the reaction to the War Logs report.

Post a Comment | Read Comments

Talk to the Newsroom

Editors and reporters who worked on these articles will be answering questions about the coverage of the material.

E-Mail Your Questions to askthetimes@nytimes.com

Over all [these documents](#) amount to a real-time history of the war reported from one important vantage point — that of the soldiers and officers actually doing the fighting and reconstruction.

The Source of the Material

The documents — some 92,000 individual reports in all — were made available to The Times and the European news organizations by WikiLeaks, an organization devoted to exposing secrets of all kinds, on the condition that the papers not report on the data until July 25, when WikiLeaks said it intended to post the material on the Internet. WikiLeaks did not reveal where it obtained the material. WikiLeaks was not

involved in the news organizations' research, reporting, analysis and writing. The Times spent about a month mining the data for disclosures and patterns, verifying and cross-checking with other information sources, and preparing the articles that are published today. The three news organizations agreed to publish their articles simultaneously, but each prepared its own articles.

Classified Information

Deciding whether to publish secret information is always difficult, and after weighing the risks and public interest, we sometimes chose not to publish. But there are times when the information is of significant public interest, and this is one of those times. The documents illuminate the extraordinary difficulty of what the United States and its allies have undertaken in a way that other accounts have not.

Most of the incident reports are marked "secret," a relatively low level of classification. The Times has taken care not to publish information that would harm national security interests. The Times and the other news organizations agreed at the outset that we would not disclose — either in our articles or any of our online supplementary material — anything that was likely to put lives at risk or jeopardize military or antiterrorist operations. We have, for example, withheld any names of operatives in the field and informants cited in the reports. We have avoided anything that might compromise American or allied intelligence-gathering methods such as communications intercepts. We have not linked to the archives of raw material. At the request of the White House, The Times also urged WikiLeaks to withhold any harmful material from its Web site.

Verification

To establish confidence in the information, The Times checked a number of the reports against incidents that had been publicly reported or witnessed by our own journalists. Government officials did not dispute that the information was authentic.

It is sometimes unclear whether a particular incident report is based on firsthand observation, on the account of an intelligence source regarded as reliable, on less trustworthy sources or on speculation by the writer. It is also not known what may be missing from the material, either because it is in a more restrictive category of classification or for some other reason.

A version of this article appeared in print on July 26, 2010, on page A8 of the New York edition.

Related Searches

[Afghanistan War \(2001- \)](#)

[Get E-Mail](#)

PRINT



TÉLÉCOPIE • FACSIMILE TRANSMISSION

DATE: 27 May 2019

A/TO: His Excellency
Mr. Julian Braithwaite
Ambassador
Permanent Representative
Permanent Mission of the United Kingdom of Great Britain and Northern Ireland to the
United Nations Office and other international organizations in Geneva

FAX: +41 22 918 23 10

EMAIL: Geneva.UN@fco.gov.uk ; Niamh.clarke@fco.gov.uk ; Teresa.levigne@fco.gov.uk

DE/FROM: Beatriz Balbin
Chief
Special Procedures Branch
OHCHR

FAX: +41 22 917 9008

TEL: +41 22 917 9543 / +41 22 917 9738

E-MAIL: registry@ohchr.org

REF: UA GBR 3/2019

PAGES: 15 (Y COMPRIS CETTE PAGE/INCLUDING THIS PAGE)

OBJET/SUBJECT: **URGENT APPEAL FROM SPECIAL PROCEDURES**

Please find attached an urgent appeal sent by the Special Rapporteur on torture and other
cruel, inhuman or degrading treatment or punishment.

I would be grateful if this letter could be transmitted at your earliest convenience to
His Excellency Mr. Jeremy Hunt, MP, Secretary of State for Foreign and Commonwealth
Affairs.



PALAIS DES NATIONS • 1211 GENEVA 10, SWITZERLAND
www.ohchr.org • TEL: +41 22 917 9543 / +41 22 917 9738 • FAX: +41 22 917 9008 • E-MAIL: registry@ohchr.org

Mandate of the Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment

REFERENCE:
UA GBR 3/2019

27 May 2019

Excellency,

I write in my capacity as UN Special Rapporteur on Torture and other Cruel, Inhuman or Degrading Treatment or Punishment, pursuant to Human Rights Council resolutions 34/19, and in connection with my visit on 9 May 2019 to Mr. Julian Assange, detained since 11 April 2019 in HMP Belmarsh prison.

The primary purpose of my visit was to examine Mr. Assange's current state of health – physical and psychological – in order to assess whether the circumstances and treatment he has been exposed and subjected to since his confinement at the Ecuadorian Embassy in 2012 or, respectively, his potential extradition or transfer to another country, amount to torture or other cruel, inhuman or degrading treatment or punishment, as absolutely prohibited in universally applicable human rights law including, most notably, the UN Convention against Torture (UNCAT) and the Covenant on Civil and Political Rights (CCPR).

During my visit, I was assisted by Prof. Duarte Vieira Nuno (medical forensic expert) and Dr. Pau Perez-Sales (psychiatrist). Both experts are specialized in examining, identifying and documenting the medical effects of physical and psychological torture and other cruel, inhuman or degrading treatment or punishment.

Based on direct, verified information collected prior, during and after my visit, I am summarizing below my initial observations and recommendations. Similar letters will be sent to the Governments of Ecuador, Sweden, and the United States of America.

According to the information received:

On 11 April 2019, the Metropolitan Police Service (MPS), at the invitation of the Government of Ecuador, entered the Embassy of Ecuador in London to apprehend

.../2

His Excellency
Mr. Jeremy Hunt, MP,
Secretary of State for Foreign and Commonwealth Affairs

Mr. Julian Assange. He was forcibly taken into police custody and arrested for breaching the 1976 Bail Act in connection with his failure to surrender to the court in June 2012 for extradition to Sweden, and in connection with an extradition request by the United States of America. That same day, Mr. Assange was taken to Westminster Magistrates' Court where a judge convicted Mr. Assange for bail violation almost seven years earlier, without allowing him sufficient time for the preparation of his defense, refusing to consider important evidence suggesting a conflict of interest of another judge involved in that proceeding, and personally insulting Mr. Assange as a "narcissist, who cannot go beyond his own self-interest".

On 1 May 2019, Mr. Assange was sentenced at Southwark Crown Court to 50 weeks imprisonment – nearly the maximum provided by law - which the UN Working Group on Arbitrary Detention in a press statement of 3 May 2019 described as disproportionate to the minor gravity of his offence. The sentencing judge reportedly read from a pre-typed judgment, without even considering the detailed mitigating evidence presented by Mr. Assange's defense counsel as to the real risk of serious harm which his compliance with the terms of his bail would have exposed him to.

On 2 May 2019 an initial hearing took place at the same court relating to an extradition request made by the United States for Mr. Assange. On 13 May 2019, the Swedish prosecuting authorities announced that they were re-opening a preliminary criminal investigation for sexual offences against Mr. Assange, an investigation which had already been formally closed twice in 2010 and 2017, and which had never produced tangible evidence or led to formal charges.

On 23 May, the US justice department extended the basis for its extradition request by filing 17 new charges against Mr. Assange, including under the Espionage Act.

Mr. Assange is currently serving his sentence and awaiting the continuation of his extradition proceedings to the United States, and possibly to Sweden, at HMP Belmarsh, a high-security prison in south-east London.

1. Concerns regarding current conditions of detention

At the time of my visit, Mr. Assange was held in cell 37 of Block 2 and, like other inmates in this block, had access to an outside yard for between 30 and 60 minutes per day, depending on the weather conditions. According to the prison staff, he was also entitled to apply for access to the library and the gym, and to interact with other inmates in the shared areas of the Block 2 during the so-called "association" time, which was said to last between 3 and 4 hours per day, either in the morning or the afternoon. The prison

staff acknowledged, however, that Mr. Assange had not yet been able to access the gym or the library since his arrival at HMP Belmarsh, primarily due to his frequent absences from the block for court appearances, medical care, and meetings with lawyers and other external visitors. During “association” time, like other inmates, Mr. Assange was permitted to use one of the telephones installed in the shared area of the block to call authorized numbers including, most notably, his legal team. Expenses for such calls and other purchasable items, such as pens and paper, were limited to GBP 15 per week. This budget could be increased once Mr. Assange started to work, which was not yet the case at the time of my visit. According to the prison staff, after an initial induction period, the normal daily routine for convicted inmates, such as Mr. Assange, was to work for between 3 and 4 hours in the morning or the afternoon, and to spend the other half of the day in “association” time as described above. All three meals were said to be taken by inmates in their cells, in the case of Mr. Assange in a freshly painted single occupancy cell measuring approximately 2 meters (width) by 3 meters (length) by 2,3 meters (height), equipped with a bed and bedding, a cupboard, a note-board, basic sanitary installations, a plastic chair and a medium sized window. Mr. Assange had received numerous letters, which he was allowed to keep in his cell.

In general terms, at the time of my visit, the conditions of detention, as well as the daily routine and disciplinary regime applied to Mr. Assange appeared to meet the requirements of the Standard Minimum Rules for the Treatment of Prisoners (also known as the “Mandela Rules”, updated and adopted by the UN General Assembly on 5 November 2015). Contrary to prior reports received, at the time of my visit, Mr. Assange was not being held in solitary confinement, but was confined to his cell for approximately 20 hours per day. While this may be acceptable for an induction period of a few days, Mr. Assange now should be granted regular access to the library, the gym and opportunities for meaningful work and social engagement. More importantly, however, I am seriously concerned that the restrictive “B-type” security regime applied to Mr. Assange, including the limited frequency and duration of lawyers’ visits and the lack of access to a computer (even without internet), severely hampers his ability to adequately prepare for the multiple and complex legal proceedings that are pending against him. It must be emphasized that, in contrast to most other convicts, Mr. Assange’s legal cases are still pending and require not only frequent and extensive exchange with lawyers covering various jurisdictions, but also the facilities to draft written statements and correspondence.

2. Concerns regarding current state of health

Prior to my visit, I received consistent reports that Mr. Assange’s physical and mental health had seriously deteriorated in the course of his confinement at the Ecuadorian Embassy and had reached a critical state in the course of the past year. On 9 May 2019, I was able to conduct confidential interviews with Mr. Assange and a thorough physical and psychiatric examination in line with specialized medical protocols,

most notably the universally recognized “Manual on the Effective Investigation and Documentation of Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment” (also known as the “Istanbul Protocol”). In order to triangulate and consolidate the collected information, numerous additional sources have also been consulted including, most notably, several medical experts who have had the opportunity to examine Mr. Assange on one or several occasions during his confinement at the Ecuadorian Embassy.

While the precise medical data collected, including the exact diagnoses produced by the medical examinations conducted during my assessment of Mr. Assange remain subject to source and patient confidentiality, the resulting medical conclusions, as far as they are relevant for the observations of my mandate, can be summarized as follows:

From a strictly physical point of view, several aspects of Mr. Assange’s health condition and cognitive and sensory capacity have been, and still are, significantly impaired as a direct consequence of his long-term confinement in the Ecuadorian Embassy, without access to natural sunlight and adequate medical and dental care. At the time of the physical examination, the most urgent physical conditions had been adequately attended to by the health care unit at HMP Belmarsh, and no immediate life-threatening condition or imminent risk of serious and irreparable harm was observed.

From a psychological perspective, Mr. Assange showed all symptoms typical for prolonged and sustained exposure to severe psychological stress, anxiety and related mental and emotional suffering in an environment highly conducive to major depressive and post-traumatic stress disorders (PTSD). Both medical experts accompanying my visit agreed that Mr. Assange is in urgent need of treatment by a psychiatrist of his own choice and confidence, whom he does not associate with the detaining authorities, and that his current condition is likely to deteriorate dramatically, with severe and long-term psychological and social sequels, in the event of prolonged exposure to significant additional stressors, such as those expected to arise in the event of his extradition to the United States or any other country refusing to provide guarantees against refoulement to the United States.

In this regard, I am alarmed at information received after my visit, that on or about 18 May 2019, Mr. Assange was moved to the health care unit within HMP Belmarsh. The reason for this transfer appears to be a serious deterioration of the medical symptoms observed during my visit, now also involving a significant loss of weight, thus confirming Mr. Assange’s continued exposure to progressively severe psychological suffering and the ongoing exacerbation of his pre-existing trauma.

3. Causal relation between current medical symptoms and previous treatment and conditions

For almost seven years, from June 2012 to April 2019, Mr. Assange was physically confined to the Embassy of Ecuador, where he was exposed to a progressively controlled, restricted and closely monitored environment with increasingly limited contact to the outside world. In these circumstances, significant extraneous interfering factors can be excluded, and the primary causes for the physical and psychological symptoms observed during the visit can be identified and assigned with a high degree of certainty. More specifically, based on the known evolution of the factual circumstances impacting Mr. Assange's daily life during the past seven years, a clear and direct causal relation can be established between the serious psychological trauma and other medical symptoms observed and his well-documented, prolonged exposure to the following factors:

- a) **Prolonged arbitrary confinement by the United Kingdom and Sweden:** All records available to me show that Mr. Assange voluntarily and consistently cooperated with the Swedish police and prosecutors, both during his presence in Sweden in 2010 and after he sought refuge at the Ecuadorian Embassy in June 2012, in relation to the allegations of sexual offences which had been made against him. However, there is compelling evidence that Swedish and British prosecuting authorities, through concerted actions and omissions, have deliberately created and maintained a long-term situation rendering Mr. Assange unable to travel to Sweden for additional questioning, and to comply with British bail conditions, without simultaneously having to expose himself to the materially unrelated risk of onward extradition or surrender to the United States and, thereby, to a real risk of serious violations of his human rights.

As has been accurately determined by the UN WGAD in its decision of 4 December 2015, this situation effectively exposed Mr. Assange to prolonged, involuntary and arbitrary confinement in the Ecuadorian Embassy, and also deprived him of adequate dental and medical care for a period of almost seven years. As my mandate has previously observed, the longer a situation of arbitrary confinement lasts, and the less the affected person can do to influence their own situation, the more intense their mental and emotional suffering will become, and the higher the likelihood that the prohibition of torture and other cruel, inhuman or degrading treatment or punishment has been breached (A/HRC/37/50, §27).

- b) **Public shaming and judicial harassment by Sweden:** Records made available to me show that, in 2010, after Mr. Assange had fully cooperated with Swedish police and prosecution concerning allegations of sexual misconduct made against him, the Chief Prosecutor of Stockholm stated that "I don't think there is reason to suspect that he has committed rape" and closed the investigation, determining that

the “conduct alleged by (the complainant) disclosed no crime at all”. Upon appeal, the investigation was re-opened by a different prosecutor shortly thereafter, reportedly after the statement of the complainant had been modified to include more prejudicial language. The mass media were informed, resulting in widespread dissemination of a distorted and misleading narrative portraying Mr. Assange as a “rape” suspect, thus suggesting a violent offence far more serious than the facts alleged by the complainants themselves. In reality, the most serious allegation made against Mr. Assange seems to involve the predictably unresolvable question of whether, during consensual intercourse with the complainant, and unbeknownst to her, Mr. Assange had ripped his condom intentionally, or merely accidentally.

For almost nine years, the Swedish authorities have consistently maintained, revived and fueled the “rape”-suspect narrative against Mr. Assange, despite the legal requirement of anonymity, despite the mandatory presumption of innocence, despite the objectively unrealistic prospect of a conviction, and despite contradicting evidence suggesting that, in reality, the complainants never intended to report a sexual offence against Mr. Assange, but that they had been pressured (“railroaded”) into doing so by the Swedish police and had subsequently decided to “sell” their story to the tabloid press.

The resulting reputational harm to Mr. Assange was perpetuated and exacerbated by the Swedish prosecutor’s persistent rejection, contrary to standard practice in many other cases, of all possibilities which would have enabled Mr. Assange to respond to questions of Swedish prosecution without simultaneously having to expose himself to the risk of refoulement to the United States. At no point did the Swedish prosecuting authorities make any attempt to prevent, contain or redress reputational harm to Mr. Assange, or to protect his human dignity by publicly rejecting and rectifying obvious exaggerations and misrepresentations of the allegations made against him.

The announcement of 13 May 2019 that the Swedish prosecuting authorities had re-opened the preliminary investigation into the same allegations made already in 2010 against Mr. Assange compounds my serious concern that, in this case, the “rape” suspect narrative appears to be misused to deliberately undermine his reputation and credibility and, ultimately, to facilitate his indirect refoulement from the United Kingdom to the United States.

- c) **Coercive harassment and defamation by Ecuador:** Several first-hand witnesses confirmed that the initial five years of co-existence between Mr. Assange and the staff at the Ecuadorian Embassy from June 2012 to May 2017 were marked by respectful and friendly relations. After the election of the new Ecuadorian Government in 2017, the Ecuadorian authorities reportedly began to deliberately

create and maintain circumstances rendering Mr. Assange's living conditions increasingly difficult and oppressive, with the apparent aim of coercing him to voluntarily leave the Embassy, or to trigger a health crisis which would justify his involuntary transfer to a hospital under British jurisdiction, where he could be arrested. Between March 2018 and April 2019, the progressively severe harassment of Mr. Assange by the Ecuadorian authorities reportedly culminated in a situation marked by **excessive regulation, restriction and surveillance** of Mr. Assange's communications, meetings with external visitors (including lawyers and medical doctors) and his private life; by **various degrees of harassment** by security guards and certain diplomatic staff; and by the **public dissemination** of distorted half-truths, defamations and deliberately debasing statements, including by the State leadership. On 11 April 2019, the Ecuadorian authorities 'suspended' Mr. Assange's Ecuadorian citizenship, terminated his diplomatic asylum, and invited British police to arrest him inside the Embassy, without any form of due process, without adequate advance notification and without any apparent medical necessity or other material urgency. His sudden expulsion from the Embassy in the hands of the British police did not allow Mr. Assange to collect and take his belongings with him, including his documents which may contain confidential information related to his sources as a journalist and publisher. The risk that this sensitive information may fall in the wrong hands would be an additional source of extreme anxiety for any journalist.

- d) Sustained and unrestrained public mobbing, intimidation and defamation in the United States, United Kingdom, Sweden and Ecuador:** There is abundant evidence that, since August 2010, the Governments of the United States, the United Kingdom, Sweden, and (since May 2017) Ecuador have progressively either acquiesced in, consented to, instigated, or even initiated or actively contributed to a sustained and unrestrained campaign of public mobbing, intimidation and defamation against Mr. Assange, consisting of a constant stream of public statements not only by the mass media and influential private individuals, but also by current or former political figures and senior officials of various branches of government, including judicial magistrates personally involved in proceedings against Mr. Assange. These statements have ranged from deliberate ridicule, insult and humiliation, to distorted reporting and misleading criminal accusations, and from open threats and instigation of violence, to repeated calls for his assassination or murder. Despite the grave, repeated and deliberately degrading and intimidating nature of these acts, none of the mentioned Governments have expressed public disapproval or taken appropriate measures of prevention, protection and redress, thus displaying an attitude of complacency (at best) and complicity (at worst), and creating an atmosphere of impunity encouraging further abuse and vilification.

Mr. Assange's exposure to these cumulative factors over a prolonged period of time, with the active participation of several Governments, or at their instigation, or with their consent or acquiescence, has resulted in patterns of severe and traumatic pain and suffering, including chronic anxiety, stress and depression, and an intense sense of humiliation, isolation, vulnerability and powerlessness.

I am therefore gravely concerned that, starting from August 2010, Mr. Assange has been, and currently still is, exposed to progressively severe pain and suffering, inflicted through various forms and degrees of cruel, inhuman or degrading treatment or punishment, the cumulative effects of which clearly amount to psychological torture.

I condemn, in the strongest terms, the deliberate, concerted and sustained nature of the abuse intentionally inflicted on Mr. Assange and seriously deplore the consistent failure of all involved Governments to take measures for his protection against sustained patterns of public mobbing, intimidation and defamation.

The evidence made available to me strongly suggests that the primary international responsibility for the described patterns of cruel, inhuman or degrading treatment or punishment, and the resulting exposure of Mr. Assange to psychological torture, rests with the Governments of the United Kingdom, Sweden, Ecuador, and the United States, both jointly for the foreseeable cumulative effect, and separately for their respective contributions through direct perpetration or, as the case may be, through instigation, consent, or acquiescence, as well as through failure to prevent such abuse being perpetrated against Mr. Assange by persons acting within their jurisdiction.

4. Risks in the event of direct or indirect extradition or transfer to the United States:

In light of the extradition request made by the United States and the re-opening of the preliminary criminal investigation against Mr. Assange in Sweden, I am also gravely concerned about the risks arising for Mr. Assange in the event of his extradition or surrender to the United States, whether directly from the United Kingdom (direct refoulement) or indirectly via Sweden or any other intermediary third country (indirect refoulement).

- a) **Concerns related to the impunity for torture in the United States:** In the recent past, the United States Government has repeatedly refused to investigate and prosecute torture and other cruel, inhuman or degrading treatment or punishment perpetrated by its officials, despite compelling and undisputed evidence, particularly in cases involving national security. The Government has also exercised strong pressure on other States, the United Nations or the International Criminal Court to prevent non-US criminal investigations against

US officials on such charges. While the United States of America formally recognizes the prohibition of torture and other cruel, inhuman or degrading treatment or punishment, its reluctance to implement and enforce this formal commitment in cases involving national security and its own officials has been and continues to be a matter of serious concern to my mandate.

- b) **Concerns related to conditions of detention:** If extradited to the United States, I fear that Mr. Assange may be detained in a high security prison (“Supermax”) or in an institution with comparable conditions of detention and treatment, both during his trial and after his conviction. In the past, my mandate has repeatedly requested to carry out an official country visit to the United States to examine the prison system and treatment of inmates from the perspective of the prohibition of torture and other cruel, inhuman or degrading treatment or punishment. The Government of the United States never agreed to facilitate such a visit in compliance with the terms of reference of my mandate, thus preventing an independent on-site assessment by the Special Rapporteur.

However, there are numerous consistent reports, based on first-hand accounts, indicating that both Federal and State level detention centres routinely practice measures of control and discipline, without recourse to judicial review, which in the view of my mandate amount to torture or other cruel, inhuman or degrading treatment or punishment. These measures include, most notably, the practice of prolonged or indefinite solitary confinement and other forms of social and sensory deprivation, in-cell restraints, shackling in stress positions, and excessively intrusive strip-searches. Persons with physical or mental disabilities and other vulnerabilities have been reported not to receive the medical care required by their condition. In 2016, my predecessor on the mandate determined that Ms. Chelsea Manning, whose case is related to that of Mr. Assange, was detained in conditions amounting to cruel, inhuman or degrading treatment, or even torture (A/HRC/19/61/Add.4., pp. 74/75).

- c) **Concerns related to psychological ill-treatment:** Severely intimidating and debasing public statements made by current and former state officials, media representatives and other influential persons in the United States suggest that, if extradited or otherwise surrendered to the United States, Mr. Assange will be exposed to an environment of public vilification, arbitrariness and judicial bias, which will be even more intense than has been the case so far. Given the strongly perceptible public and official prejudice held against Mr. Assange in the United States, there are serious reasons to doubt that he would receive a fair trial before an impartial judicial body as required under human rights law. This prospect, in conjunction with the effects of the traumatic abuse and degradation he already has been subjected to, would almost certainly result in aggravated, profound and prolonged psychological, social and physical distress and suffering incompatible

with the prohibition of torture and other cruel, inhuman or degrading treatment or punishment.

- d) **Concerns regarding cruel, inhuman or degrading punishment:** In light of the public prejudice prevailing in the United States against Mr. Assange, and the threat which the publishing activities of Wikileaks are perceived to present to US national security I am gravely concerned that US authorities intend to make an “example” of him, in order to punish him personally, but also to deter others who may be tempted to engage in similar activities as Wikileaks or Mr. Assange. I therefore fear that, irrespective of his personal criminal culpability, and whatever offence he may in reality have committed or contributed to, Mr. Assange will be confronted with overly expansive charges and subjected to excessively severe criminal sanctions.

This concern has been significantly exacerbated by reports that, on 23 May 2019, the US Department of Justice has added 17 new charges to their extradition request for Mr. Assange, including under the Espionage Act and each of them carrying a potential sanction of 10 years of imprisonment, which currently results in a possible maximum penalty of 175 years of imprisonment. It is my understanding that, in principle, the US can add further charges to their extradition request until 11 June 2019. Further, I am currently examining concerns that, after a potential extradition of Mr. Assange to the United States, the broad description of facts in the US extradition request might subsequently be used as a basis for adding even more serious charges, as appears to be permissible under the current UK/US extradition treaty, potentially carrying the death penalty or a life sentence without parole, both of which would constitute absolute barriers to refoulement under human rights law. Finally, I am currently examining concerns that the mechanism of temporary surrender, or any other form of informal transfer without full judicial review, might potentially be used by the United Kingdom or by Sweden to circumvent the due process requirements of a full extradition proceeding in line with the absolute and non-derogable prohibition of refoulement towards a real risk of torture or other cruel, inhuman or degrading treatment or punishment.

In light of these concerns, and taking into full consideration the serious deterioration of Mr. Assange’s physical and psychological health resulting from the combination of factors described in this letter, I underscore my most serious concern that, if Mr. Assange were to be extradited or otherwise surrendered to the United States, or to Sweden or any other State refusing to provide full guarantees against onward extradition or surrender to the United States, he would be exposed to a real risk of torture or other cruel, inhuman or degrading treatment or punishment. It must be emphasized that, in circumstances such as these, the instrument of diplomatic assurances, even in conjunction with post-extradition monitoring

mechanisms, is inherently incapable of providing the required safeguards and, for this reason, has been widely criticized for being used as a loophole undermining the principle of non-refoulement (A/HRC/37/50, para. 45-48; A/70/303, para. 69).

In view of the urgency of the matter, I would appreciate a response on the initial steps taken by your Excellency's Government to safeguard the rights of the above-mentioned person(s) in compliance with international instruments.

As it is my responsibility, under the mandate provided to me by the Human Rights Council, to seek to clarify all cases brought to my attention, I would be grateful for your observations on the following matters:

1. Please provide any additional information and any comment you may have on the above-mentioned allegations.
2. Please provide the details and, where available, the results of any investigation, medical examinations, and judicial or other inquiries which may have been carried out, or which are foreseen, in relation to the allegations of psychological torture and other cruel, inhuman or degrading treatment or punishment, and the serious health concerns. If no such measures have been taken, please explain how this is compatible with the human rights obligations of the United Kingdom.
3. Please provide the details of any measures which have been taken, or which are foreseen, for the purpose of protecting Mr. Assange from further infliction of torture and other cruel, inhuman or degrading treatment or punishment. If no such measures have been taken, please explain how this is compatible with the human rights obligations of the United Kingdom.
4. Please provide the details of any measures which have been taken, or which are foreseen, for the purpose of ensuring that Mr. Assange obtains redress for the harm inflicted on him, including fair and adequate compensation and the means for full physical, psychological and reputational rehabilitation. If no such measures have been taken, please explain how this is compatible with the human rights obligations of the United Kingdom.

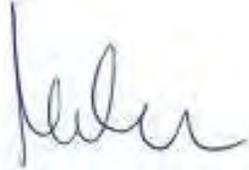
In the meantime, for the reasons stated above, I urgently appeal to Your Excellency's Government not to extradite or otherwise surrender Mr. Assange to the United States, whether directly or indirectly via another State failing to provide reliable guarantees against his onward transfer to the United States. I also respectfully recommend to Your Excellency's Government to commute the sentence imposed for bail violation or, should that prove not possible, to review and significantly adjust its

implementation so as to allow Mr. Assange to regain his physical and mental health, which is acutely endangered, most notably through urgent access to a psychiatrist of his choice and confidence, and through urgent relief from his constant exposure to traumatizing psychological stress, anxiety and depression. Moreover, Mr. Assange must be enabled to adequately prepare, with the unrestricted support of his legal team, for any judicial or administrative proceeding which may be pending against him personally, or that may otherwise require his attention.

I intend to publicly express my concerns in this case in the near future, given that, in my view, the evidence supporting my concerns is sufficiently consistent and reliable to indicate a matter warranting urgent public attention. Any public expression of concern on my part will indicate that I have been in contact with your Excellency's Government, as well as the other concerned Governments, to share my views, concerns and recommendations, and to clarify the issue in question.

This communication and any response received from your Excellency's Government will be made public via the communications reporting [website](#) within 60 days. They will also subsequently be made available in the usual report to be presented to the Human Rights Council.

Please accept, Excellency, the assurances of my highest consideration.

A handwritten signature in blue ink, appearing to read 'Nils Melzer', is centered on the page.

Nils Melzer
Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment

Annex

Reference to international human rights law

Under universally applicable human rights law, States have the obligation to protect the physical and mental integrity of all persons within their jurisdiction and, most notably, to prevent acts or omissions amounting to torture and other cruel, inhuman or degrading treatment or punishment. These fundamentally important obligations are reflected in the Universal Declaration of Human Rights (UDHR) and codified, inter alia, the International Covenant on Civil and Political Rights (ICCPR), to which the United Kingdom ratified on 20 May 1976, and the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, to which the United Kingdom ratified on 8 December 1988.

Definition of torture

Article 1 of the Convention against Torture defines ‘torture’ as “any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person for such purposes as obtaining from him or a third person information or a confession, punishing him for an act he or a third person has committed or is suspected of having committed, or intimidating or coercing him or a third person, or for any reason based on discrimination of any kind, when such pain or suffering is inflicted by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity.” The concept of ‘other cruel, inhuman or degrading treatment or punishment’, within the meaning of Article 16 of the Convention against Torture, does not necessarily require the elements of severity, intentionality or purposefulness but implies the absence of a valid legal justification for the resulting pain, suffering or humiliation, namely its necessity and proportionality for a lawful purpose (A/72/178, para. 31, and E/CN.4/2006/6, paras. 38–41).

Paragraph 8a of Human Rights Council Resolution 16/23, reminds States that “Intimidation and coercion, as described in **article 1 of the Convention against Torture**, including serious and credible threats, as well as death threats, to the physical integrity of the victim or of a third person can amount to cruel, inhuman or degrading treatment or to torture.”

Risk of torture or ill-treatment if extradited

Article 3 of the CAT provides that, “[n]o State Party shall expel, return (“refouler”) or extradite a person to another State where there are substantial grounds for believing that he would be in danger of being subjected to torture”.

I would also like to refer to **paragraph 9 of the General Comment No. 20 of the Human Rights Committee** in which it states that State parties “must not expose

individuals to the danger of torture or cruel, inhuman or degrading treatment or punishment upon return to another country by way of extradition, expulsion or refoulement.”

Diplomatic assurances are insufficient as a procedural safeguard

This principle has been consistently affirmed by the Human Rights Council and the General Assembly, for instance in **paragraph 7 of the Resolution A/RES/70/146 of the UN General Assembly** which urges States “not to expel, return (“refouler”), extradite or in any other way transfer a person to another State where there are substantial grounds for believing that the person would be in danger of being subjected to torture, and recognizes that *diplomatic assurances*, where used, do not release States from their obligations under international human rights, humanitarian and refugee law, in particular the principle of non-refoulement.”

The former **Special Rapporteur on Torture, in his report A/60/316**, concluded after a thorough review of the practice that “*diplomatic assurances* are unreliable and ineffective in the protection against torture and ill-treatment upon return as diplomatic assurances are not legally binding, therefore they carry no legal effect and no accountability if breached; and the person whom the assurances aim to protect has no recourse if the assurances are violated” (para 51). This assessment was confirmed and expanded on by the current Special Rapporteur in his report A/HRC/37/50, para. 45-48.

Minimum Standards regarding adequate health care

Moreover, as outlined by **the UN Standard Minimum Rules for the Treatment of Prisoners (see the revised version adopted on 5 November 2015 and renamed “Mandela Rules”)**, the provision of health care is the responsibility of the state authorities. **Rule 27(1)** furthermore provides that all prisons shall ensure prompt access to medical attention in urgent cases. Prisoners who require specialized treatment or surgery shall be transferred to specialized institutions or to civil hospitals. Where a prison service has its own hospital facilities, they shall be adequately staffed and equipped to provide prisoners referred to them with appropriate treatment and care.

Further, to take note, in this respect, of the Principles on the Effective Investigation and Documentation of Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment and the updated set of principles for the protection of human rights through action to combat impunity as a useful tool in efforts to prevent and combat torture” and “(t)o ensure that victims of torture or other cruel, inhuman or degrading treatment or punishment obtain redress, are awarded fair and adequate compensation and receive appropriate social, psychological, medical and other relevant specialized rehabilitation.