

**EXHIBIT 6**

ORIGINAL

AO 106 (SDNY Rev. 01/17) Application for a Search Warrant

## UNITED STATES DISTRICT COURT

for the  
Southern District of New YorkIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)Huawei Nexus 6P cellular telephone  
with IMEI Number 86798002059655217 MAG 1905  
Case No.

## APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Huawei Nexus 6P cellular telephone with IMEI Number 867980020596552, See Attachment A  
located in the Southern District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attached Affidavit and its Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

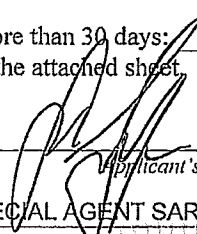
The search is related to a violation of:

Code Section(s)	Offense Description(s)
18 U.S.C. 793(d), 793(e), 1030(a)(1), 1030(a)(2)(B), 1030(a)(5)(A)	Offenses relating to unauthorized possession and distribution of national defense information

The application is based on these facts:

See Attached Affidavit and its Attachment A

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of 30 days (give exact ending date if more than 30 days: ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature  
SPECIAL AGENT SARA E. LANGENDERFER  
Printed name and title

Sworn to before me and signed in my presence.

Date:

03/15/2017

3/16/17 via telephone  
Fed.R.Crim.P.4.1

City and state: New York, NY

  
Judge's signature  
Hon. BARBARA C. MOSES  
Printed name and title

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States Of America for a Search Warrants for: (i) a Huawei Nexus 6P cellular telephone with IMEI Number 867980020596552

**TO BE FILED UNDER SEAL**

**Agent Affidavit in Support of  
Application for Search Warrant**

**Affidavit in Support of Application Pursuant to Rule 41  
For a Warrant to Search and Seize**

SARA E. LANGENDERFER, being duly sworn, deposes and states:

**I. Introduction**

**A. Affiant**

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the New York Field Office, and have been employed by the FBI since 2016. Prior to that, for four years I was Intelligence Analyst assigned to a task force with the Drug Enforcement Administration ("DEA"). I am currently assigned to a squad responsible for counterespionage matters and have worked in the field of counterintelligence from 2016 to present. In the course of my duties as a Special Agent, I am responsible for investigating offenses involving espionage and related violations of law, including unauthorized retention, gathering, transmitting or losing classified documents or materials; unauthorized removal and retention of classified documents or materials; illegally acting in the United States as a foreign agent; other national security offenses; and the making of false statements. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure or retention of classified information, as well as my training in counterintelligence operations, I am familiar with the tactics, methods, and techniques of United States persons who possess, or have possessed a United States Government security clearance and may choose to harm the United States by misusing their access to classified

information. I am also familiar, though my training and experience with the use of computers in criminal activity and the forensic analysis of electronically stored information.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the electronic device specified below (the "**Subject Device**") for the items and information described in Attachment A. This Affidavit is based upon my participation in the investigation, my examination of reports and records, and my conversations with other law enforcement agents and other individuals, as well as my training and experience. Because this Affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of this investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated. In addition, unless otherwise indicated, statements by others referenced in this Affidavit were not necessarily made to me, but may have been provided to me by someone else to whom I have spoken or whose report I have read (and who in turn may have had either direct or indirect knowledge of the statement). Similarly, unless otherwise indicated, information in this Affidavit resulting from surveillance does not necessarily set forth my personal observations, but may have been provided to me by other law enforcement agents who observed the events, and to whom I have spoken or whose reports I have read.

**B. The Subject Device**

3. The **Subject Device** is a Huawei Nexus 6P cellular telephone with IMEI Number 867980020596552. The **Subject Device**, which belongs to an individual who resides in the Southern District of New York, is believed to be located in the Southern District of New York, and will be located in the Southern District of New York at the time of the execution of the proposed warrant.

4. Based on my training, experience, and research, I know that the **Subject Device** has capabilities that allow it to serve as, among other things, a wireless telephone, a digital camera, a video recorder, a portable media player, a GPS navigation device, and a calendar. I also know that the **Subject Device** is a so-called “smartphone” in that it is Internet capable and can access the Internet through cellular and WiFi networks and that through user-installed applications, the **Subject Device** is capable of accessing and storing Internet-based content, including email, digital storage accounts, social media accounts, bank and credit card accounts, and almost any other manner of service or platform otherwise accessible through the Internet. Moreover, the **Subject Device** has an internal storage capacity that allows the **Subject Device** to store all manner of electronic data, including data obtained from the various Internet-based platforms I have identified above.

5. Based on my training, experience, and conversations with other law enforcement officers, I know that the International Mobile Equipment Entity (“IMEI”) is an identifying number unique to a particular cellular telephone—in other words, although the call number assigned to a specific phone may change, the IMEI assigned to a specific phone does not.

### C. The Subject Offenses

6. I respectfully submit that probable cause exists to believe that the **Subject Device** contain evidence, fruits, and instrumentalities of: (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in

violation of Title 18, United States Code, Section 1030(a)(1); (iv) intentionally exceeding authorized access and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B); and (v) transmitting computer code to intentionally damage a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A) (collectively “SUBJECT OFFENSES”).

## **II. Facts Establishing Probable Cause**

### **A. WikiLeaks Publication of Classified CIA Information**

7. Based on my review of publicly available material on the Internet, including on the website wikileaks.org (“WikiLeaks”), I know that, on March 7, 2017, WikiLeaks published what it claimed were more than 8,000 documents and files that contained classified information (the “Classified Information”) belonging to the Central Intelligence Agency (“CIA”). In its press release accompanying the Classified Information, WikiLeaks further claimed that:

a. The public dissemination of the Classified Information was “the largest ever” unauthorized publication of classified CIA documents.

b. The Classified Information constituted the “first full part” of a series—thus indicating that there would be subsequent publications of additional sensitive CIA information.

c. The “collection” obtained by WikiLeaks amounted to “more than several hundred million lines of code” and revealed the “entire hacking capacity” of the CIA, including various malware, viruses, and other tools used by the CIA.

8. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that:

a. The information that WikiLeaks claimed was classified CIA information—that is, the Classified Information—was at the time of its disclosure, in fact, classified CIA information.

b. Specifically, the Classified Information was created and maintained by one specific group within the CIA which is responsible for various computer engineering activities, including the development of computer code (the "CIA Group"). That CIA Group exists within a larger CIA component (the "CIA Component"). In March 2016, less than 200 employees were assigned to the CIA Group. And only employees of the CIA Group had access to the computer network on which the Classified Information that was stolen from the CIA Group's computer network was stored. (Moreover, as described in detail below, only three of those approximately 200 people who worked for the CIA Group had access to the specific portion of the Group's computer network on which the Classified Information was likely stored.)

c. The Classified Information appears to have been stolen from the CIA Component sometime between the night of March 2, 2016 and the night of March 3, 2016.<sup>1</sup>

i. This is based on preliminary analysis of the timestamps associated with the Classified Information reflecting the latest (or most recent) creation or modification date associated with the Classified Information.

ii. Because, for the reasons described below (*see infra*), the Classified Information was apparently copied from an automated daily back-up file, it is likely that the Classified Information was copied either late on March 2, 2016 (after the March 2 nightly back-

---

<sup>1</sup> The information that the Classified Information appears to have been stolen between March 2 and March 3, 2016 was first received by the FBI on the evening of March 15, 2016. This information was provided to the FBI based on a more complete forensic analysis by analysts of the data that was stolen. In prior search warrant applications in connection with this investigation, a preliminary analysis had concluded that the Classified Information was copied between March 7 and March 8, 2016. We now understand that those dates are inaccurate, and have substituted what we understand to be the correct dates that the Classified Information was copied (*i.e.*, March 2 and 3) throughout this application where the prior applications had referenced March 7 and 8. Nevertheless, we respectfully submit that the mistaken understanding regarding the dates on which the Classified Information was stolen does not affect the probable cause underlying the prior search warrant applications.

up was completed) or on March 3, 2016 (before the March 3 nightly back-up was completed).

iii. This is so because if the Classified Information was copied before the March 2 back-up, one would *not* expect to see in the Classified Information documents dated as late as March 2. And if the Classified Information was copied after the March 3 back-up, one *would* expect to see documents dated on or after March 3 because the “back-ups” occur approximately each day.<sup>2</sup>

d. The Classified Information was publicly released by WikiLeaks approximately one year from the latest date associated with the Classified Information.

e. The duplication and removal from the CIA Group’s computer network of the Classified Information and its subsequent public dissemination via WikiLeaks was not authorized by the United States government.

f. The unauthorized disclosure of the Classified Information could—at a minimum—reasonably be expected to cause serious damage to the national security of the United States. *See* Executive Order 13526; 18 C.F.R. § 3a.11(a)(2).

g. The Classified Information is national defense information and its disclosure could reasonably be expected to be used to the injury to the United States and to the advantage of a foreign nation. *See* 18 U.S.C. § 793(d) & (e).

---

<sup>2</sup> It is of course possible that the Classified Information was copied later than March 3, 2016. For example, the individual who copied and removed the data could have limited his or her copying to data that was modified or created on or before a specific date. (Conversely, however, the Classified Information is unlikely to have been copied before March 2, 2016, because it contains data that was created as recently as March 2, 2016.) Because the most recent timestamp on the Classified Information reflects a date of March 2, 2016, preliminary analysis indicates that the Classified Information was likely copied between the end of the day on March 2 and the end of the day on March 3, 2016.



**B. The CIA Group's Local Area Computer Network (LAN) and Back-Up Server**

9. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that the Classified Information originated in a specific isolated local area computer network ("LAN") used exclusively by the CIA Group.<sup>3</sup> As described above, in and around March 2016, in total less than 200 people had access to the CIA Group's LAN on which the Classified Information was stored.

a. An isolated network, such as the CIA Group's LAN, is a network-security structure by which the isolated network is physically separated (or "air-gapped") from unsecured networks, such as the public Internet.

b. Accordingly, such isolated networks, like the LAN, cannot be accessed from the public Internet, but rather only through those computers which are physically connected to the isolated network.

c. The CIA Group's LAN, and each of its component parts, was maintained in heavily physically secured governmental facilities, which include multiple access controls and various other security measures.

d. The isolated LAN used by the CIA Group was comprised of multiple networked computers and servers. (Each of these component computers and servers were, by definition, inside the electronically isolated LAN.)

i. In order to preserve and protect the CIA Group employees' day-to-day computer engineering work, that work was backed up, on an approximately daily basis, to another server on the CIA Group's LAN that was used to store back-up data (the "Back-Up

---

<sup>3</sup> In its press release announcing the publication of the Classified Information, WikiLeaks stated that the Classified Information originated from "an isolated, high-security network."

Server”).

ii. Back-ups of the sort stored on the Back-Up Server are designed to ensure that, should the original data be corrupted or deleted, the stored data is not lost, but rather—because of the daily back-ups—is maintained via the daily copies stored on the Back-Up Server.

**C. The Publicly Disclosed Classified Information Likely Originated on the CIA Group’s Back-Up Server**

10. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I understand that the Classified Information that was publicly released by WikiLeaks appears likely to have been copied—specifically—from the CIA Group’s Back-Up Server.

a. As described above, the Back-Up Server served as a secondary storage location for data that principally resided on the primary computer network used for CIA Group employees’ day-to-day work writing computer code. Approximately each day, an automated process would back-up that data to the Back-Up Server. Each of those daily back-ups was akin to an electronic “snapshot” of the data on that particular date. In that way, the Back-Up Server simultaneously acquired and stored, on a rolling basis, daily snapshots of the original data.

b. As such, if the data contained on the Back-Up Server was copied *en masse* directly from that Server, the copy would contain numerous iterations (or snapshots) of the similar or same data which had been backed up from the original data, distinguished by date.

c. The publicly released Classified Information does in fact contain numerous iterations (or snapshots) of the similar or same data, distinguished by date.

d. Accordingly, the fact that the Classified Information contains numerous iterations (or snapshots) of the similar or same data, distinguished by date, is strongly supportive

of the fact that the Classified Information was taken from the CIA Group's Back-Up Server.<sup>4</sup>

e. As described above, because the most recent timestamp associated with the Classified Information appears to correspond to approximately March 3, 2016, it is likely that the Classified Information was copied from the Back-Up Server after the daily back-up on March 2, 2016, and before the daily back-up on March 3, 2016.

**D. TARGET SUBJECT JOSHUA ADAM SCHULTE Was One of Only Three CIA Employees Who, in March 2016, Had Been Given System Administrator Access to the Back-Up Server**

11. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that the CIA Group's LAN was designed such that only those employees who were specifically given a particular type of systems-administrator access ("Systems Administrators") could access the Back-Up Server.

a. Systems Administrators were given a particular username and password in order to log on to and access the Back-Up Server.

b. Conversely, CIA employees who were not designated Systems Administrators were not given access to the Back-Up Server.<sup>5</sup>

---

<sup>4</sup> I understand, based on my conversations with others familiar with the CIA Group's LAN that it would be difficult, if not impossible, to copy from the data (not on the Back-Up Server) the multiple different date-distinguished iterations of the same data that are included in the publicly released Classified Information. In contrast, a single copy of the Back-Up Server would likely include each of the prior iterations (or snapshots) of the same data—which is exactly what is reflected in the publicly released Classified Information. I further understand that WikiLeaks's claims regarding the information in its possession suggest that the information would have been stored in a database (as opposed to static files which could have been "scraped" directly from the LAN), and that this fact is consistent with the information being taken from the Back-Up Server.

<sup>5</sup> It is, of course, possible that an employee who was not a designated Systems Administrator could find a way to gain access to the Back-Up Server. For example, such an employee could steal and use—without legitimate authorization—the username and password of a designated Systems Administrator. Or an employee lacking Systems Administrator access could,

12. I know, based on my conversations with other law enforcement agents and others, in approximately March 2016—the month when the Classified Information is assessed to have been copied—only three CIA employees were designated Systems Administrators with access to the CIA Group’s Back-Up Server.

a. TARGET SUBJECT JOSHUA ADAM SCHULTE (“SCHULTE”) was one of those three Systems Administrators.

i. SCHULTE was employed as a computer engineer by the CIA—specifically in the CIA Group—from in or about May 2010 through on or about November 10, 2016, when he resigned from the CIA.

ii. During SCHULTE’s more than six years working in the CIA Group, his responsibilities included, among other things, developing computer code for specific projects, including projects explicitly described in the Classified Information.

iii. SCHULTE had a skill set that enabled him to write computer code designed to clandestinely copy data from computers.

b. As described above, in March 2016, SCHULTE was one of only three CIA employees throughout the CIA who had authorized access to the CIA Group’s Back-Up Server from which the Classified Information was likely copied. The publicly released Classified Information published by WikiLeaks, based on a preliminary review, appears to contain the names and/or pseudonyms of, *inter alia*, multiple CIA employees—including two of the three aforementioned individuals with designated Systems Administrator privileges.

i. Names used by the other two CIA Group Systems Administrators

---

at least theoretically, gain access to the Back-Up Server by finding a “back- door” into the Back-Up Server.

were, in fact, published in the publicly released Classified Information.

ii. SCHULTE's name, on the other hand, was not apparently published in the Classified Information.

iii. Thus, SCHULTE was the only one of the three Systems Administrators with access to the Classified Information on the Back-Up Server who was not publicly identified via WikiLeaks's publication of the Classified Information.

c. The other two individuals who served in March 2016 as Systems Administrators for the CIA Group's LAN remain employed by the CIA. SCHULTE resigned from the CIA in November 2016, as described in detail below.

**E. SCHULTE Had Access to the Back-Up Server on March 2 and 3, 2016—The Likely Dates of the Copying of the Classified Information**

13. As described above, it appears likely that the Classified Information was copied between March 2 and March 3, 2016.

a. Based on my conversations with other law enforcement agents and others, and my review of documents, including access records of the CIA Component facility in which SCHULTE worked, I know that he was present at work from approximately:

- i. 10:34 a.m. until 6:29 p.m. on March 2, 2016; and
- ii. 10:37 a.m. until 7:40 p.m. on March 3, 2016.

b. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that SCHULTE's workspace (*i.e.*, his desk and computer workstation) was set up such that only three other CIA Group Employees had direct line-of-sight to SCHULTE's desk and computer—that is, only three other employees could see what he was doing at his desk. I also understand from my conversations with other law enforcement agents and others, and my review of documents, that one of those individuals was not present on

March 3, 2016, which the preliminary analysis estimates is the approximate date the stolen Classified Information was taken.<sup>6</sup>

**F. SCHULTE's Unauthorized Unilateral Reinstatement of His Own Administrative Privileges**

14. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, on or about April 4, 2016, around the time of his reassignment to another branch within the CIA Group, many of SCHULTE's administrator privileges on the LAN were revoked, and he was no longer permitted to serve as a Systems Administrator in the CIA Group's LAN.

a. At the same time, on or about April 4, 2016, SCHULTE's computer access to a specific developmental project ("Project-1") was also revoked. Until his reassignment, SCHULTE had been the CIA Group employee with principal responsibility for Project-1.

b. Upon that transfer, principal responsibility for Project-1 was transferred to another CIA Group employee, who received computer access to Project-1.<sup>7</sup>

c. I know from my review of publicly available material on the Internet, including WikiLeaks.org, that Project-1 was one of a small group of CIA projects and capabilities

---

<sup>6</sup> In prior applications, the Government had included additional information regarding a business retreat that had resulted in two of three employees being away from SCHULTE's cubicle on or about March 8. In view of the newly obtained information regarding the estimated dates of the theft of the Classified Information, that fact no longer is relevant. That said, I respectfully submit that the fact that SCHULTE was one of only three individuals with administrator access and was present at work on the date that the theft of the Classified Materials is estimated to have taken place, along with the other substantial facts surrounding SCHULTE's actions described herein, provide ample probable cause and does not alter the Court's prior determinations.

<sup>7</sup> SCHULTE retained read-only access to Project-1 (but not the ability to alter the code) and the ability to copy the computer code associated with it in order to support another project for which he had responsibility.

that WikiLeaks highlighted explicitly by name in its March 7, 2017 press release that accompanied the online publication of the Classified Information.

15. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, less than two weeks later, on or about April 11, 2016, SCHULTE unilaterally, and without authorization, logged onto the CIA Group's LAN and reinstated his own administrator privileges.

a. On or about April 14, 2016, CIA Group management discovered that SCHULTE had personally re-instituted his administrator privileges without permission.

b. On or about April 18, 2016, SCHULTE received notice regarding CIA policies against personnel restoring their own access to privileges or computer networks after those accesses have been revoked. SCHULTE signed an acknowledgment that he understood that "individuals are not permitted to personally attempt and/or renew their previous authorizations [including administrator privileges] to any particular [computer] system." That notice further instructed SCHULTE: "do not attempt to restore or provide yourself administrative rights to any project and/or system for which they have been removed."

c. A little more than one month later, on May 26, 2016, and notwithstanding the warnings described above, SCHULTE made an official request that he again be given full access to Project-1. Before receiving a response to that request, SCHULTE requested access from another employee who, apparently without proper vetting, granted SCHULTE the requested full access to Project-1.

i. On the same day, SCHULTE used that newly obtained access to, unilaterally and without authorization, revoke the computer access permissions of all other CIA Group employees to work on Project-1.



ii. Once this conduct was discovered, SCHULTE was issued a letter of warning that stated, "You were aware of the policy for access and your management's lack of support for you to retain administrative privileges, but nonetheless you took steps to deliberately violate that policy and gain those privileges." It continued by warning SCHULTE that any future violations would result in "further administrative action of a more severe nature."

iii. After receiving the letter of warning, SCHULTE disagreed with some of its conclusions and consequently refused to sign the form.

16. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that SCHULTE's accessing of information on the LAN that he had been expressly forbidden by the CIA to access, and his accessing of information which he had been electronically prevented from accessing by the CIA, using a computer network on which he was permitted to access other, distinct information, exceeded his authorized access to the government-owned and controlled computer networks of the CIA. *See* 18 U.S.C. § 1030(a)(1) & (a)(2)(B).

**G. Internal CIA Investigation of SCHULTE and a CIA Colleague**

17. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that, in or around March 2016, SCHULTE came to the attention of CIA security after SCHULTE alleged that another CIA Group co-worker had made a threat against him. SCHULTE expressed deep unhappiness about the way that CIA responded to the alleged threat. He threatened legal action against the CIA for its handling of the situation, and repeatedly stated that he felt that he was being punished by CIA management for reporting the alleged threat incident. SCHULTE informed CIA security that, if "forced into a corner" he would proceed with a lawsuit against the CIA. He also repeatedly threatened that he or his lawyer would go to the media. In addition, CIA security learned that



SCHULTE had removed an internal CIA document from CIA facilities that regarded his complaints to the CIA concerning its handling of the alleged threat, despite being told multiple times by CIA security officials not to do so.

18. In approximately August 2016, as part of a standard background reinvestigation of SCHULTE for the purpose of renewing his security clearances, the CIA conducted interviews of multiple CIA Group colleagues. Among other things:

a. Some (but not all) colleagues independently reported that SCHULTE's demeanor with his management and colleagues, and his commitment to his work, changed markedly for the worse in or around February 2016.

b. Multiple colleagues stated that SCHULTE had indicated that he felt aggrieved by the CIA in a number of respects. Some also reported that they believed SCHULTE to be untrustworthy and potentially subject to outside coercion. (Other colleagues made no such report and, indeed affirmatively reported that they believed that SCHULTE was, in fact, trustworthy.)

c. Some (but not all) colleagues also reported that SCHULTE's security practices were lax, and that SCHULTE tended not to abide by security guidelines he deemed inconvenient—particularly guidelines concerning when and what kinds of media or data (such as external drives) could be connected or uploaded to CIA computer systems.<sup>8</sup>

#### **H. SCHULTE's November 2016 Resignation from the CIA**

19. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that, in connection with and

---

<sup>8</sup> External drives can be connected to computers and files in order to allow users to move files from the computers onto the portable external drives.

preceding SCHULTE's November 2016 resignation from the CIA, he sent the following communications, among others:

a. Approximately one month prior to his resignation, on October 12, 2016, SCHULTE, using his CIA email account, sent an email to another CIA Group employee at that employee's official email account. The subject line of the email stated, "ROUGH DRAFT of Resignation Letter \*EYES ONLY\*." The email contained a letter entitled "Letter of Resignation 10/12/16" and addressed to "To whomever it may concern" ("Draft Resignation Letter"). I know from reviewing the Draft Resignation Letter, which spanned approximately three single-spaced pages, the following:

i. SCHULTE began the letter by stating, in substance and in part, that he had "always been a patriot" and would "obviously continue to support and defend this country until the day that I die," but that "from this day forward" he would "no longer do so as a public servant."

ii. SCHULTE claimed that he believed that the CIA Group management had unfairly "veiled" CIA leadership from various of SCHULTE's previously expressed concerns, including concerns about the network security of the CIA Group's LAN. SCHULTE continued: "That ends now. From this moment forward you can no longer claim ignorance; you can no longer pretend that you were not involved."

iii. SCHULTE explained that he was resigning from the CIA because CIA Group management had, among other things, "ignored" issues he had raised about "security concerns" and had attempted to "conceal these practices from senior leadership," including that the CIA Group's LAN was "incredibly vulnerable" to the theft of sensitive data. He claimed that one named CIA Group manager had ignored his security concerns and "later attempt[ed] to evade

responsibility and blame the decentralized and insecure [CIA Group computing] environment entirely on me.”<sup>9</sup>

iv. Specifically, SCHULTE wrote that inadequate CIA security measures had “left [the CIA Group’s LAN] open and easy for anyone to gain access and easily download [from the LAN] and upload [sensitive CIA Group computer code] in its entirety to the [public] internet.”

b. It appears that SCHULTE did not, in fact, submit the Draft Resignation Letter.

c. On his last day with the CIA (November 10, 2016), SCHULTE did, however, send an internal email to the CIA Office of the Inspector General (OIG) advising that office that he had been in contact with the United States House of Representatives’ Permanent Select Committee on Intelligence regarding his complaints about the CIA (“OIG Email”).

i. In the OIG Email, which SCHULTE labeled “Unclassified,” SCHULTE raised many of the same complaints included in the draft “Letter of Resignation 10/12/16,” described above, including the CIA’s treatment of him and its failure to address the “security concerns” he had repeatedly raised in the past.

ii. Shortly thereafter, CIA security learned that one of SCHULTE’s colleagues had witnessed SCHULTE printing the OIG Email, placing it in a folder, and exiting the CIA Component facility where SCHULTE worked.

iii. Notwithstanding SCHULTE’s labeling of the email as “Unclassified,” the CIA subsequently determined that the OIG Email which SCHULTE removed

---

<sup>9</sup> SCHULTE went on to describe other complaints he had about managers at the CIA. Among other things, SCHULTE described his complaints about the way in which CIA Group management had handled various personnel and disciplinary issues (*see supra* at Part II.G.16).

from the CIA without authorization did, in fact, contain classified information.

**I. Events on March 15, 2017**

20. On or about March 15, 2017, agents from the FBI executed a search warrant for SCHULTE's residence in Manhattan, New York. I know from speaking to individuals involved in the search, which is still ongoing, agents have in the initial stages of the search found, among other things:

- a. The November 10, 2016 email that SCHULTE had sent to the Office of Inspector General (OIG) (referenced above in paragraph 20), which contained classified information and which SCHULTE labeled "Unclassified" and removed from a CIA facility.
- b. Multiple terabytes (at least 13 terabytes) of computer storage devices, including at least one server, desktop computers, and various hard drives. Some of these devices appear to be encrypted.
- c. Multiple internal correspondence from the CIA that includes, *inter alia*, the names of CIA employees and what appear to be classified information (e.g., code words for specific CIA programs).
- d. A computer coding manual that is labeled "FOUO" (For Official Use Only).
- e. Handwritten notes that appear to reference former CIA employees and past grievances. For example, there is one note referencing an incident that occurred with another employee on March 1, 2016, days before the download of the Classified Information is estimated to have occurred.

21. On or about March 15, 2017, two agents of the FBI also approached SCHULTE as he exited from his place of employment, identified themselves as law enforcement, and asked him whether he would be willing to speak with them. Based on my conversations with those law enforcement officers, I understand the following, in substance and in part:

- a. SCHULTE agreed to speak with the FBI agents, and accompanied them to a nearby café where they talked over coffee.
- b. Among other things, SCHULTE described to the FBI agents concerns and issues he had with respect to his former employer's handling of the Classified

Information, its security protocols, and how they handled a complaint that he had filed.

- c. SCHULTE denied any involvement in the transmission of the Classified Information to WikiLeaks.
- d. SCHULTE also denied having a copy of the November 10, 2016 email to OIG referenced above in paragraph 30(a), which contained classified information and which was found in SCHULTE's residence.

**J. Probable Cause Justifying Search of the Subject Device**

22. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, since the March 7, 2017 publication of the Classified Information on WikiLeaks, SCHULTE has repeatedly initiated contact, via telephone and text messages, with multiple of his former CIA Group colleagues. Those colleagues have reported that contact to government and law enforcement officials.

a. In those communications with his former colleagues, SCHULTE has repeatedly asked about the status of the investigation into the disclosure of the Classified Information.

b. SCHULTE has requested more details on the information that was disclosed.

c. SCHULTE has inquired of his interlocutors' personal opinions regarding who, within the CIA Group, each believes is responsible for the disclosure of the Classified Information. SCHULTE has also asked what other former CIA Group colleagues are saying about the disclosure.

d. SCHULTE has repeatedly denied any involvement in the disclosure of the Classified Information.

e. SCHULTE has indicated the he believes that he is a suspect in the investigation of the leak of Classified Information.

f. I am not aware of any other former CIA employee who has initiated any contact with former colleagues regarding the disclosure of the Classified Information.

23. Furthermore, I know that SCHULTE has made at least some of the communications above using the so-called Google Voice feature associated with a particular Google account with the email address joshschulte1@gmail.com (the SCHULTE Gmail Address). I know from my training and experience, and my participation in this investigation, that Google Voice is a service which provides users the ability to, among other things, make voice calls, send text messages, forward calls, and receive voicemails via their Google account. In this case, the Google account in question is the account associated with the SCHULTE Gmail address and which has the subscriber name "Josh Schulte" (the "SCHULTE Google Account"). Specifically, for example:

a. Records show that, on or about March 7, 2017, when WikiLeaks released the Classified Information, SCHULTE used the Google Voice feature associated with the SCHULTE Google Account to send approximately 149 texts to multiple of his former colleagues at the CIA.

b. SCHULTE, using the Google Voice feature associated with the SCHULTE Google Account, also had phone calls with former CIA colleagues, including one telephone call with a former colleague in which he, among other things, inquired of the former colleague's personal opinions regarding who was responsible for the disclosure of the Classified Information and what the person's motivation might be. SCHULTE indicated that he believed that the person responsible was a contractor who disclosed the Classified Information for fame.

c. In a call on March 8, 2017 using the telephone number associated with the

SCHULTE Google Account with the same former colleague,<sup>10</sup> SCHULTE denied his involvement in the disclosure of the Classified Information, indicated his belief that many people suspected him of the disclosure, and relayed a conversation with another acquaintance in which SCHULTE had denied involvement in the disclosure of the Classified Information, but was dissatisfied with the acquaintance's reaction to SCHULTE's denial.

24. I know from a review of records that that the **Subject Device** is the mobile telephone that is assigned to the SCHULTE Google Account via Google's Android feature.<sup>11</sup> That is, the **Subject Device's** unique IMEI number (as well as other identifiers, such as the Subject Device's device ID, MEID, and serial number) is listed among the identifying features of the telephone associated with the SCHULTE Google Account. I also know that the same subscription information lists the SCHULTE Gmail address as the user of the **Subject Device**. I therefore believe that there is probable cause to believe that the **Subject Device** was used in some of the aforementioned conversations and that it contains evidence, fruits, and instrumentalities of the Subject Offenses.

25. Specifically, there is probable cause to believe that the **Subject Device** contains some or all of the following:

- a. The phone number associated with the **Subject Device**, as well as call log

---

<sup>10</sup> The telephone number associated with the SCHULTE Google Account is listed in the subscriber information for the account under the category "SMS."

<sup>11</sup> Based on my conversations with other law enforcement agents and others, and my review of documents, I know that Android is a mobile operating system developed by Google, and it is used on a variety of touchscreen mobile devices, such as smartphones and tablet computers. Google retains information related to the Android device associated with an account, including the IMEI (the International Mobile Station Equipment Identifier), MEID (the Mobile Equipment Identifier), device ID, and/or serial number of the devices. Each of those identifiers uniquely identifies the device used. One device may be associated with multiple different Google and Android accounts, and one Google or Android account may be associated with multiple devices.

information of phone numbers of incoming and outgoing, and missed or unanswered calls to and from the Subject Device;

b. Address books and contact lists stored on the **Subject Device** or its memory card(s);

c. Voicemail messages, opened or unopened, related to the Subject Offenses;

d. Evidence concerning the identity or location of the owner(s) or user(s) of the Subject Device;

e. Evidence concerning the identity and/or location of the individual(s) involved in the commission of the Subject Offenses;

f. Evidence of communications among, or concerning, participants in or witnesses to the commission of the Subject Offenses;

g. Contact information of co-conspirators and witnesses to the commission of the Subject Offenses, including telephone numbers, email addresses, and identifiers for instant messaging and social media accounts;

h. Text, data, "chats," MMS ("Multimedia Messaging Service") messages, SMS ("Short Message Service") messages, FaceTime messages, and e-mail messages, any attachments to those messages, such as digital photographs and videos, and any associated information, such as the phone number or e-mail address from which the message was sent, pertaining to the Subject Offenses;

i. Digital photographs and videos related to the commission of the Subject Offenses;

j. Browsing history, websites visited, and internet searches conducted on the Subject Device; and

k. Any Global Positioning Satellite ("GPS") entries, Internet Protocol



connections, and location entries to include Cell Tower and WiFi entries.

26. Like individuals engaged in any other kind of activity, individuals who engage in the Subject Offenses store records relating to their illegal activity and to persons involved with them in that activity on electronic devices such as the **Subject Device**. Such records can include, for example logs of online “chats” with co-conspirators; email correspondence; contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and/or records of illegal transactions using stolen financial and personal identification data. Individuals engaged in criminal activity often store such records in order to, among other things, (1) keep track of co-conspirator’s contact information; (2) keep a record of illegal transactions for future reference; (3) keep an accounting of illegal proceeds for purposes of, among other things, dividing those proceeds with co-conspirators; and (4) store stolen data for future exploitation.

27. Computer files or remnants of such files can be recovered months or even years after they have been created or saved on an electronic device such as the **Subject Device**. Even when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. The ability to retrieve from information from the **Subject Device** depends less on when the information was first created or saved than on a particular user's device configuration, storage capacity, and computer habits.

28. Accordingly, in light of the foregoing, I respectfully submit that there is probable cause to believe that the **Subject Device** contains evidence, fruits, and contraband relating to the Subject Offenses.

### III. Procedures for Searching ESI

#### A. Review of ESI

29. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained on the **Subject Device** for information responsive to the warrant.

30. In conducting this review, law enforcement may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

31. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement may need to conduct a complete review of all the ESI from the **Subject Device** to locate all data responsive to the warrant.


**B. Return of the Subject Device**

32. If the Government determines that the **Subject Device** is no longer necessary to retrieve and preserve the data on the device, and that the **Subject Device** is not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return the **Subject Device**, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.


**IV. Conclusion and Ancillary Provisions**

33. Based on the foregoing, I respectfully request the court to issue a warrant to seize and search the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

34. In light of the confidential nature of the continuing investigation, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.

  
SARA E. LANGENDERFER  
Special Agent  
Federal Bureau of Investigation

Sworn to before me on  
March 16, 2017 in a telephone, Fed. R. Crim P. 4.1

  
HONORABLE BARBARA MOSES  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF NEW YORK

## **Attachment A**

### **I. Device to be Seized and Searched**

The device to be seized and searched (the “**Subject Device**”) is a Huawei Nexus 6P cellular telephone with IMEI Number 867980020596552.

### **II. Execution of the Warrant**

Law enforcement agents are permitted to execute the search warrant at any time in the day or night. Upon the execution of this warrant, notice will be provided at or as soon as possible after the execution of the search.

### **III. Review of ESI on the Subject Device**

Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the **Subject Device** for the following evidence, fruits, and instrumentalities of violations of (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); (iv) intentionally exceeding authorized access and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B); and (v) transmitting computer code to

---

intentionally damage a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A) (collectively, the "Subject Offenses"):

1. The phone number associated with the **Subject Device**, as well as call log information of phone numbers of incoming and outgoing, and missed or unanswered calls to and from the **Subject Device**;

2. Address books and contact lists stored on the **Subject Device** or its memory card(s);

3. Voicemail messages, opened or unopened, related to the Subject Offenses;

4. Evidence concerning the identity or location of the owner(s) or user(s) of the **Subject Device**;

5. Evidence concerning the identity and/or location of the individual(s) involved in the commission of the Subject Offenses;

6. Evidence of communications among, or concerning, participants in or witnesses to the commission of the Subject Offenses;

7. Contact information of co-conspirators and witnesses to the commission of the Subject Offenses, including telephone numbers, email addresses, and identifiers for instant messaging and social media accounts;

8. Text, data, "chats," MMS ("Multimedia Messaging Service") messages, SMS ("Short Message Service") messages, FaceTime messages, and e-mail messages, any attachments to those messages, such as digital photographs and videos, and any associated information, such as the phone number or e-mail address from which the message was sent, pertaining to the Subject Offenses;

9. Digital photographs and videos related to the commission of the Subject Offenses;

10. Browsing history, websites visited, and internet searches conducted on the **Subject Device**; and

11. Any Global Positioning Satellite ("GPS") entries, Internet Protocol connections, and location entries to include Cell Tower and WiFi entries.