
From: Annon1204 <Annon1204@protonmail.com>
Sent: Monday, September 24, 2018 10:40 AM
To: shanewharris@protonmail.com
Subject: Re: Search warrants
Attachments: notes.pdf; sw1.pdf

Part 1

Sent from ProtonMail mobile

----- Original Message -----

On Sep 24, 2018, 10:35 AM, Shane Harris <shanewharris@protonmail.com> wrote:

Hi. Thanks so much for getting back to me. I think you may have to send these as pdfs. I'm unable to download them from the site you sent. Chrome is blocking it and Microsoft doesn't recognize the filetype. Sorry if this is just a technical failing on my end. Is there another way for you to share this? I'm eager to see it.

Thanks.

Shane

Sent from [ProtonMail](#), encrypted email based in Switzerland.

----- Original Message -----

On Saturday, September 22, 2018 6:10 PM, Annon1204 <Annon1204@protonmail.com> wrote:

Dear Shane,

Sorry for the delay. The FBI raided Josh's parents house last week and forcibly made them delete his articles... I'm attaching the search warrants in Josh Schulte's case along with his notes. We intend to send you other documents in the coming days:

We have decided to share with you an initial expose (depending on how the first one goes with you we will share up to 9 more) involving Russian Oligarchs business ties and wire transfers involving hundreds of millions of dollars to Donald Trump's closest advisors and law firms including Giuliani and Marc Kasowitz firms. Trump's self-reported best friend plays a startling role..

Anyway, regarding Josh Schulte's case:

**GOVERNMENT
EXHIBIT
812
S2 17 Cr. 548 (PAC)**

Attached are two of the search warrant applications in Josh Schulte's case along with private notes Josh wrote regarding the first warrant. (Couldn't attach due to size limits, sent here: <https://ufile.io/qj757>)

Archive password is: zzvZyj9f

If you prefer alternative method of sending files let me know; I could attach each of the three PDFs in individual emails)

The FBI lied on their initial search warrant and then tried to cover it up. They submitted one-year-old "evidence" from when Josh lived in VA to search his NYC apartment with no specificity and no connection in the probable cause to any of Josh's electronic devices—an outrageous disregard for the 4th amendment. This case will no doubt end up in the 2nd circuit and likely the supreme court. Take a look for yourself and see the laughably miniscule probable cause that they later refute in their subsequent search warrants.

The FBI have specifically hid their malfeasance for the past 18 months. Note that they found no evidence of espionage from his apartment in March. Their investigation into espionage yielded literally NOTHING.

[REDACTED]

Let us know how much you are interested in the tech components and Josh's case. We have lots of his writings and planned pro se motions and other info on his case, but most of it is highly technical (including an expert report he did for another inmate that will rock the tech world as it unveils incredible FBI incompetence). We aren't sure how much of this is of interest to you and the Post or if it's better off in Wired or something? Let us know if that's the case and we can start to divert those aspects elsewhere.

Thanks.

9/10/18

II. Probable Cause

A. Wikileaks Publication of Classified CIA Information

This is actually very poorly written because they ramble in this section and repeat themselves in subsequent sections. I'll point out their lies in section C.) where they refer back to this section.

8.) b.) 3 of 200 people in one CIA Group had access to classified info.

In reality, two groups-- EDG AND COG and at least 400 people had access. They don't include COG who was connected to our DEVLAN through HICOC, an intermediary network that connected both COG and EDG.

--> RECKLESS DISREGARD FOR THE TRUTH: There is absolutely NO reason they shouldn't have known this connection exists. Step one is narrowing down the possible suspects and to completely disregard an ENTIRE GROUP and HALF the suspects is reckless. All they needed to do was talk to ONE person on Infrastructure branch or through ANY technical description / diagram of the network.

8.) c.) Classified Information appears to have been stolen between 3/7 and 3/8

--> RECKLESS: This is ABSURD and based on FLAWED logic that any reasonable individual could understand. I'll touch on this in later sections when they reference it again.

B. The CIA Group's LAN and Back-Up Server

9.) 3/2016, less than 200 people had access to LAN containing C.I.

--> FALSE: TWO GROUPS AND OVER 400 PEOPLE HAD ACCESS.

--> RECKLESS: Talk to staff, view network diagram. The truth is readily apparent.

C. The Publicly disclosed CI likely originated on the CIA Group's Back-Up Server

10.) CLAIM: CI copied from back-up server

--> FALSE: Subsequent search warrants say: "As set forth herein, an investigation is ongoing as to whether the stolen data was in fact backup data taken from the automated back-up." There is absolutely NO evidence that suggests a back-up server was involved.

--> RECKLESS: SEIZE FIRST, INVESTIGATE LATER: This is ILLEGAL and has been declared as such by the courts. See subsections:

10.) a.) "Approximately" each day, automated backup

--> FALSE: They can't even get minor details correct. Each Atlassian product, Stash/Bitbucket, Confluence, Jira, Bamboo, and Crowd managed their own backup files which were backed up at differing rates from daily to monthly.

--> RECKLESS: Spent no time learning facts or investigating. The misunderstanding of one backup file versus several and daily versus daily, weekly, and monthly backups illustrates they had no idea ANYTHING about the network or backup process. Can they be said to have acted in good faith if such a fundamental claim is false? We are barely into the search warrant at all and EVERYTHING is wrong. Their failures in understanding WHEN and HOW data is backed up show they cannot possibly have acted in good faith because how can ANYTHING they claim be taken seriously when they didn't take the time to understand the backup process? How can they claim the CI was stolen from A SINGLE backup file when there were multiple?

10.) b.) Data copied en masse from server would contain numerous snapshots

--> FALSE: This is not true at all. First of all it doesn't even make sense to copy the server en masse as described in section a, each backup contains the ENTIRE data. Why would anyone copy ALL the backups of the same data? Regardless, even if that were true, the posted data by wikileaks is not backup files. Wikileaks does not provide ANY backup files. None. The only data Wikileaks provided was the actual data itself-- data that could have been taken from a SINGLE backup file. The content of the released data gives absolutely no hints as to whether it was taken from a backup or not.

--> RECKLESS: This is CRITICAL. This misunderstanding is the predicate for which the entire search warrant is based. NO technical person would ever make these claims. NONE. Thus, is it reckless to request a search warrant regarding a subject you have no knowledge? Or shouldn't a technical person be involved? The FBI's reckless disregard for the truth was their blatant disregard for the highly technical environment and reliance on insufficient knowledge that led to faulty and illogical conclusions.

10.) c.) Publicly released data does contain numerous iterations (or snapshots)

--> FALSE: The iterations in the disclosed wikileaks data is an artifact of version control, not backed-up data. The data was version controlled so you could always revert changes and the entire log of changes (changelog) of each file was maintained by the software directly and isn't a function of backing up.

--> RECKLESS: See 10.) b.). This is false and a reckless disregard for the truth because no person with technical knowledge would ever make this claim. It's as if an FBI agent commented on brain surgery--> nothing he says could ever be taken seriously and it would be utterly reckless to ever take his advice.

10.) d.) The fact that CI contains numerous snapshots therefore CI taken from backup server

--> FALSE: The version control "snapshots" seen in the released wikileaks data would exist regardless of the method in which the data was stolen. Nothing at all can be gleaned from the released data regarding a backup server or not.

--> MISLEADING: The govt puts forth a logical argument of "if a then b; a; therefore b". If "snapshots" exist in released data then data taken from backup server. Snapshots DO EXIST in released data, therefore data was taken from backup server (see 10a-d). HOWEVER, the observed "snapshots" in the leaked data indicate VERSION CONTROL, and have nothing to do with the backup process. Their premise of "if a then b" is entirely wrong and therefore the entire argument invalid.

--> RECKLESS: The FBI observe "snapshots" of data that they misidentify as indicative of backup data and so literally lie and invent that the backups are what cause the snapshots when in actuality the behavior is independent of any backup process.

10.) d.^3) impossible to copy from the data (not in the back-up server) the multiple different date-distinguished iterations of the same data

--> CONFUSING: What is this footer even mean? They seem to be conceding that it's possible the data didn't come from the back-up server, but for entirely different reasons.

--> CONTRADICTION: "In contrast, a single copy of the Back-Up Server would likely include each of the prior iterations (or snapshots) or the same data-- which is exactly what is reflected in the publicly released Classified Information". This seems to completely contradict their claims of an "en masse" copy of multiple back-up files from the server which create the multiple iteration effect. If only a SINGLE COPY of the back-up server was needed then their entire argument makes NO SENSE as it is claiming that the multiple iterations only exist BECAUSE multiple copies of the same data are present on wikileaks-- thus, MULTIPLE backups would be needed.

--> CRITICAL: This contradiction basically makes their argument that each "iteration" of data (which in reality is simply a change in version control) is a direct cause of a backup file from the associated date. In fact, each and ever "iteration" would require an entirely separate backup file... tracing back the dates and times would likely net backups years in the past. But this is IMPOSSIBLE! No backups exist together older than several months! We thus arrive at a critical contradiction whereby the FBI completely contradict themselves and PROVES in their search warrant that their claim cannot be.

--> RECKLESS: It is reckless to claim probable cause that is contradictory. They later identify this contradiction and claim it IS possible the backup server wasn't used at all.

10.) e.) Here they refer back to section II. A. 8. c. This section illustrates, illogically, why the data must have been stolen between two specific dates, presupposing the involvement of the backup server that they dont even argue until here at section C. 10. d.

II. A. 8.) c.) CI stolen between 3/7 - 3/8 2016

i) preliminary timestamp analysis indicates 3/7 was most recent

ii) due to part C.10, the CI was copied from automated backup file

iii) If CI was copied before 3/7 => would not find 3/7 data. If copied after 3/7 => would find files later than 3/7.

--> FALSE: Entire argument relies on fraudulent backup file theory which was fallacious and thus, this derivative argument is also false.

--> FALSE: Even IF stolen backup file was accurate, this argument is STILL false. The timestamp sets ONLY a lower bound on when data was stolen, NOT an upper bound. Data could have been stolen and transmitted LITERALLY ANY DAY after 3/7 since backup files are retained and kept for months. So as a very simple counter-example, someone could grab the 3/7 backup file in July! In fact, this is the most probable action as it obfuscates the day the data was stolen.

--> FALSE: not only THAT, but the government fails to understand that there are, in fact, TWO backup servers: one temporary backup server on DEVLAN, and one off-site backup. The temporary backup contains backup files for up to several months until IB copies them onto a drive and uploads them to the off-site backup. This off-site backup contains ALL the backups simultaneously from all time. Why could this server not have been involved instead of the temporary backup?

--> RECKLESS: This is entirely self-evident. 3/7 was NOT the date the data was stolen. Even now the FBI recognize this. What's the difference between outright lying and presenting outrageously false information to the court? What if they knew it was all false but still presented it anyway? The FBI omit very critical pieces of information-- like the fact that data is stored for months on the temp backup before moved to the permanent, off-site backup. Once again, ALL of this information could have been rejected by members of IB or reading any documentation or even CIA internal emails about the network. If the FBI did none of this-- if the FBI did no investigation and never consulted with any experts-- is that not reckless disregard for the truth?

IF you really wanted to know the truth wouldn't a reasonable person go to the experts and consult? Isn't that EXACTLY what the FBI did AFTER the illegal search? They discovered everything they submitted was wrong after conducting an investigation.

A. 8. c.) iii^1: It IS possible the CI was copied later than 3/8. The individual who copied and removed data could have limited copying to 3/7. But, it was likely copied 3/7.

--> MISLEADING: They incorrectly claim that the breach could have only happened after 3/8 if an individual copied data directly from the Atlassian service (not from a backup file). As we have already discussed, this is false-- the data could have easily come from a backup file of 3/7 in April, May,... maybe even June or July... or worse yet, from the off-site backup in August, September, October,.... May well have been breached and stolen AFTER I LEFT THE AGENCY!

--> RECKLESS: They fail to recognize that a person can breach a server and purposefully steal an older backup. Is that reasonable? They fail to mention this possibility at all-- is that on purpose? What do the FBI actually know during this time? We need their internal emails and communications.

At this point the FBI have been wrong/lied about everything. The number of people and groups, who had access, the claim the data must have been taken from a backup server, the timeframe, literally everything. How many warrants have ever been presented to the court of law where everything in it was provably wrong, and easily provably wrong at the time of issue of the warrant? It's not like they uncovered additional information at some later point. ALL the information, the servers, the people, everyone all belonged to the USG. It's USG personnel, USG property, USG data. IF the FBI wanted to they could have easily discovered the truth. They recklessly chose to lie and omit evidence in a search warrant to SEIZE FIRST AND INVESTIGATE LATER, which the courts have deemed ILLEGAL! Then they rub the magic lamp of the good faith exception? Fuck that.

D. TARGET Joshua Adam Schulte was one of only 3 employees across the entire CIA who, in March 2016, had been given sys admin access to the backup server

--> FALSE: Backup server was just as likely not involved in the breach

--> FALSE: March 2016 is no more likely than any other date after March 2016 up until March 2017 for the breach

--> FALSE: I was never given any access to the backup server

--> RECKLESS: Permissions logs and access logs are EASILY obtainable. They could obtain what times I badged into the building but cant do a simple search through the access logs? OR maybe they did and the logs didn't turn up anything that supported their fraudulent hypothesis?

D. 11.) ONLY sys admins could access the backup server

D. 11.^4): IT is of course possible that an employee who was not a designated sys admin could access the backup server: stolen credentials or "back-doors"

--> MISLEADING: We are all exploit engineers. EDG develops malware and COG, the group they omitted, DEPLOYS the malware. It's more likely the data was stolen by someone WITHOUT official access. Also note that in addition to "stolen credentials", due to my numerous security reports that were accessible to the FBI, the system was left entirely open and vulnerable.

D. 12.) In March 2016 only 3 employees were designated sys admins with access to the backup server

--> FALSE: Where are they getting this information? I never had any access to the backup server. I never logged onto the backup server.

--> RECKLESS: This is a clear and obvious LIE! Only IB had access. The logs prove this. The FBI either recklessly did not review the logs OR recklessly did not include them.

D. 12. a.) JAS was one of three sys admins

--> FALSE: I never had access to the backup server. I never had login access to the backup server. I was never "given a particular username and password in order to log onto and access the Back-Up Server". I never had sys admin access on the network-- I was never even a domain admin. The only permissions I held were via Crowd where I managed the Atlassian applications along with ALL of IB. Infrastructure Branch was ultimately responsible. IB were the only people with direct access to the backup server and the only people who could even access the off-site backup.

--> RECKLESS: How hard is this to verify? Who/What is their source? If they are confusing Crowd permissions with LAN permissions then they clearly have no idea what they are doing-- which is ENTIRELY RECKLESS. It isn't logical to assume the FBI could take a two week course on brain surgery and then be able to name all the parts of the brain and perform brain surgery.

D. 12. b.) Wikileaks contains names and/or pseudos of two individuals but not Josh

--> MISLEADING: The other two employees they refer were under cover and had pseudonyms. I did not have any pseudonyms because I was overt. Wikileaks only seemed to publish pseudonyms and NOT truenames. THUS, only the other two employee's pseudos were published and NOT their truenames. In fact, there is AT LEAST one specific location with my name and Jeremy Weber names are located and BOTH-- my truename and his truename are redacted. This is a purposeful lie that the FBI puts forth.

--> RECKLESS: IT'S A LIE. It's a BOLDFACED LIE to claim only the other people's names were leaked and not mine. Regardless, the argument is idiotic; as if to presume the leaker would be dumb enough to ask for only his name to be redacted? HUH? No one would ask that and wikileaks wouldn't do that.

E. Schulte had access to backup server on 3/7 and 3/8, the likely dates of copying of classified info.

--> FALSE: This entire section assumes already-disproven details: The cause of the backup server in the leak, the dates of the leak, and Schulte's access to the server; All false.

E. 13. a.) Schulte was present at work...

--> CRITICAL: The FBI can obtain logs of when I badged into the office but not server access logs? Why? It's as if all the evidence of the crime is sitting right in front of them but they choose to ignore it or claim not to have the time to OPEN A FILE AND READ. WTF. Seriously?! How is this NOT a reckless disregard for the truth when the exculpatory evidence is SITTING RIGHT ON THE SERVER! Why can't they pull permission logs, access logs, and most critically network logs showing bandwidth of each day? This is critical to show that they did have time to do SOME investigating, but again, they other

purposefully chose not to disclose the exculpatory evidence or purposefully chose not to review it. It is reckless to not open a file and see who has sys admin permissions. It is reckless to not open access logs. It is reckless to not investigate, but rather to ASSUME based on no actual evidence.

F. Schulte's unauthorized unilateral reinstatement of his own admin privs

14.) On 4/4, Schulte reassigned and access on LAN revoked

--> FALSE: There is literally nothing as false and provably false as this statement. No. I did not have any permissions revoked because I changed branches. My administration of Atlassian was for the division, thus moving branches within the division would not involve any change of permissions. It doesn't even make any sense. Who told them this? Also, note that I never had any special LAN permissions, only Atlassian permissions; there is a HUGE difference.

--> RECKLESS: This could be confirmed in half of a second by looking at Crowd's logs and/or emails. Wouldn't emails exist explaining the loss of privileges? Wouldn't a Crowd access log show the revocation of permission? No such things exist. This lie illustrates they don't care about the truth.

14. a.) Project-1 permissions were revoked

--> MISLEADING: I am not sure if this is true. There should be logs indicating when this project was revoked, but I believe it wasn't until later.

15.) Schulte logged onto CIA group's LAN and reinstated own admin privs

--> FALSE: IT DOESN'T EVEN MAKE ANY FUCKING SENSE! SOMEONE HELP ME FOR THE LOVE OF GOD!

WTFEEEEEEEEEE. How the fuck does one "log onto the LAN"? How the fuck does one "self-grant admin privs"? Where are the logs? Is the FBI actually investigating anything? I'd imagine it's as painful for me to read this horse shit as it is to read my motions. These FBI agents are the dumbest fucks on the planet and clearly don't understand the smallest amount of tech. They take advantage of the fact that neither does the judge and then they just lie. This is literally a bold-faced, retarded lie.

15. a.) On 4/14, CIA group management discovered JAS reinstated admin privs without permission

--> FALSE: It never happened. I specifically found that ^{Jeremy Weber} was changing permissions without authorization and confronted him. He turned to the group chief with whom he had favor and told her God knows what.

--> RECKLESS: View audit logs and the truth is self-evident.

15. b.) Memo of Warning received

--> MISLEADING: I only acknowledged the policy but I refuted the event. I was furious. I told my division chief, who works under the group chief, that it was not true and made no sense. He did not care. So I signed and acknowledged that I received the memo. At this point, on 4/18 my access to Atlassian through Crowd was revoked.

15. c.) SCHULTE made an official request that he again be given full access to Project-1

--> MISLEADING: It makes it sound as if the previous incident had something to do with Project-1. It did not. No permissions to Project-1 were ever changed by me. In fact, I was told by my division chief that I was still the primary person for Project-1 and it would carry with me to my new branch. The reason for the delay from 4/18 to 5/26 is my current project, Nader. Once I completed that project in late May then I turned back to Project-1 AKA Brutal Kangaroo.

--> RECKLESS: This is all very easily discernable from the LOGS!

15. c. i.) Schulte removed access from all CIA Group employees

--> FALSE!!!! A fucking straight lie. They LIE and make it seem as if I'm doing something nefarious. IN REALITY, ALL I DID WAS CHANGE THE PROJECT PERMISSIONS FROM MY FORMER BRANCH TO MY NEW BRANCH; From OSB to RDB.

--> RECKLESS: What excuse do they have for this lie? They can't read the logs? FUCKING LIARS.

15. c. iii.) Schulte disagreed with some of the letter of warning

--> FALSE: I disagreed with everything. It was a disgusting retaliatory measure by my worthless group chief.

--> RECKLESS: I was the one who fucking NOTIFIED my group management of this entire situation. I seriously sent an email to HR and my group chief as soon as I saw my permissions had been revoked from this project. I told them that ^{Jeremy Weber} again, had revoked my permissions without authorization and that this was a major security breach because he was doing as he pleased on the system. The FBI PURPOSEFULLY left out that it was ME who notified my management of this issue. There is literally an email that exists where I specify ALL of this. Where is this email? Did the FBI not review it? This is so critical because it shows my group chief's complacency regarding ^{Jeremy Weber}'s illegal behavior and her retaliatory nature against me.

18. a.) Some (but not all) colleagues...

b.) Multiple colleagues...

c.) Some (but not all) colleagues...

--> RECKLESS: It's reckless not to disclose the exact number and/or if these colleagues were directly involved in the alleged threat and/or memo/letter of warning— because obviously THEY would be extremely biased. Not disclosing that ONLY these individuals were the particular colleagues would be entirely reckless.

18. c.) "SCHULTE tended not to abide by security guidelines he deemed inconvenient..."

--> FALSE: EDG allowed anything to be plugged in and ICE allowed nothing, thus this allegation is FALSE. It was ME who was reporting the security issues!!!

--> RECKLESS: If I wasn't abiding with policy then automated systems would flag my usage. Did it? Did management or security complain? No. (Besides the bogus memo/letter of warning).

H. 19. a.) i-iv.) ... claims EDG poorly handled situation

--> RECKLESS: My claims of poor EDG management and retaliation are known RIGHT HERE and stated as such. It would be reckless if the FBI went to the very people I claimed were retaliatory and trusted them without ever investigating their claims or literally obtaining access/security logs. To solely rely on ANYTHING EDG management claimed would be entirely reckless.

H. 19. c.) i-iii.) Schulte labeled email unclassified and removed it without authorization

--> MISLEADING: It's not unauthorized to remove unclassified, so, to remove the email was NOT unauthorized. Claiming that it is classified would make the miss-classification a simple MISTAKE, but not a purposeful, unauthorized disclosure. Classification is left to OUR discretion; The same information is classified differently by different people. This misclassification is simply harmless error.

I. Schulte's recent inquiries about status of investigation

20.) I initiated contact

--> FALSE: Contact was initiated by Tandeep who CALLED ME and told me people were mentioning my name regarding the leak.

I. 20. a.) Schulte inquired into status of investigation

--> FALSE: NEVER asked the status. EVER.

--> RECKLESS: Where is the proof of this?

I. 20. e.) Schulte believes he is a suspect in investigation

--> MISLEADING: Tandeep TOLD ME I was, hence my concern.

K. Probable cause justifying search of the subject premises

22."Based on my training and experience, I know that individuals who are involved in the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials use computers and other electronic devices in furtherance of their criminal activities. Based on my training and experience, I also know that individuals typically keep their computers and other electronics in their homes..."

--> UNBELIEVABLE ----- THIS is the entire basis for searching my apartment ?!?! They have NO evidence any tech was used to exfiltrate data. They have no reason to believe I possess any electronic devices or electronic data at my home in Virginia much less my apartment in New York. They have ZERO theories of how the data was transmitted to Wikileaks, assuming it wasn't mailed and/or deaddropped. There are so many possibilities that don't include use of my own electronics (if we even ASSUME their probable cause is true which we KNOW it to be ENTIRELY FABRICATED). The FBI rely on contemporaneous, 1+ year old "evidence" to search my new residence in a new city based on NOTHING!!!

.... To be continued

L. Probable Cause Justifying Search of ESI

24.) "As noted above, individuals who engage in the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials often use computers and other electronic devices to store documents and records relating to their illegal activity. Individuals engaged in these activities use electronic devices to, among other things, store copies of classified documents or materials; engage in email correspondence relating to their illegal activity; store contact info of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social media accounts; and/or store records of illegal transactions involving classified documents"

--> UN. BELIEVABLE. These are all STATEMENTS. Not a single fact. Not a single piece of evidence. They request a search warrant for ESI without any legal basis. Literally they just claim "because we say so".

V. Execution of the SW: Necessity of covert search and delayed notification

37.) b.) Schulte likely engaged in these activities by using sophisticated computer skills to exfiltrate a substantial amount of data onto a removable drive and then covertly removed that drive from the CIA.

--> FALSE: BASED ON WHAT?! This is the first time they claim anything about a removable drive or removing anything from the CIA. How is this even valid?

37.) c.) If SCHULTE is provided advances or contemporaneous notice of the execution of the search warrant, it may allow him to destroy evidence of his crimes on electronic devices by, for example, deleting drives or activating encryption programs that would make his devices virtually impossible to access.

--> ABSURD: Contemporaneous notice? Crime allegedly took place A YEAR AGO and wikileaks ALREADY PUBLISHED so wouldn't the subject know?! Furthermore, why would someone keep classified info stolen from the CIA AFTER giving it to wikileaks?!

--> RECKLESS: What reasonable person would suspect devices used to transmit classified would even STILL EXIST let alone be moved with the target to a new city? No chance.

=====

List of LIES:

B. 9. In March 2016 less than 200 people and only one CIA group had access to classified information later disclosed by wikileaks

--> TRUTH: 2 groups, EDG AND COG, and over 400 people across the WORLD had access.

C. 10. EDG backed up data daily on one backup, on one backup server

--> TRUTH: Each separate Atlassian product had its own backup file and frequency of backup; Backup server was really EDG storage server that was used for a multitude of things across the network including sharing and storing files and as a repository for tool deliverables. Additionally, backups stored on this server for an indeterminable amount of time before transfer to an offsite backup server-- which could have been the attack vector.

C. 10. b. IF data was taken from back-up server, data would contain numerous iterations (or snapshots) of the same or similar data

--> TRUTH: Since backups copied data from the server, there would be no distinction between data stolen from a server hosting the data or from a backup. The "iterations" are nothing more than a changelog, tracked changes that make it easy to revert and control versions of the files. The "iterations" literally have nothing to do with the backup process but are instead inherent in the software and accessible to all users.

A. 8. CI had to be stolen between 3/7 and 3/8 because latest data is from 3/8

--> TRUTH: 3/7 and 3/8 establish only the lower bound from the first possible date the data could have been stolen. Since data existed from 3/7 and 3/8, it could not be that the data was stolen before this date (although it is within reason that data was continuously stolen in which case this date would be the last date that data was stolen). However, since the backups are stored from the time of the backup, indefinitely, any date after 3/7 and 3/8 is a reasonable date that data could have been stolen up until the wikileaks release. As an easy counter-example, on 7/9 someone could have copied the 3/7 backup and gave it to

wikileaks. In fact, in all actuality the date of the backup is almost certainly NOT the date the data was stolen as any intelligent person would try to obfuscate the day the data was stolen.

D. 11. Only system administrators could access the backup server
--> TRUTH: Only domain admins, who were limited to IB could access the backup server

D. 11. a. System admins were given a particular username and pw to log onto the backup server
--> TRUTH: No, DEVLAN used active directory such that everyone only had one account to all network resources. The domain admin group was restricted to IB.

D. 12. In March 2016 only 3 employees had access to the backup server
--> TRUTH: Only IB had access

D. 12. a. JAS was one of 3 sys admins who had access to the backup server
--> TRUTH: False.

D. 12. b. Wikileaks revealed truenames of other 2 sys admins
--> TRUTH: Wikileaks only revealed pseudonyms, no truenames.

E. Schulte had access to backup server on 3/7 and 3/8
--> TRUTH: I never had access nor was I a sys admin

INCONVENIENT TRUTH: Only IB had access to backup server. The "three sys admins" managed the Atlassian tool suite where the data was stolen, but this access has nothing to do with any servers or backups-- it is managed through Crowd and simply allows for configuration and granting of permissions to other.

The servers themselves only had one login, root, which the credentials were stored online where everyone had access. Thus, all 400 people knew the login credentials and could access these servers.

F. 14. Schulte's LAN admin privs were revoked on 4/4/16
--> TRUTH: Schulte never had LAN privs, but his Atlassian privs were NOT taken on 4/4.

F. 15. Schulte logged onto LAN and reinstated his own admin privs on 4/11
--> TRUTH: Schulte NEVER had privs revoked so never reinstated them. In REALITY, Schulte noticed that another employee named [redacted] had changed permissions through Crowd and Schulte merely REVERTED these changes and informed him any additional unauthorized, unilateral changes would be sent to management.

F. 15. c. On 5/26 Schulte made official request that he be given full access to Project-1 again
--> TRUTH: Schulte never reverted his access to Project-1 on 4/11 and in actuality only discovered his removal on 5/26 when he emailed HR and his group chief Karen to inform her of this 2nd illegal change by [redacted]

F. 15. c. On 5/26 Schulte made an official request for access to Project-1. Before receiving a response to that request, Schulte requested access from another employee.
--> TRUTH: Schulte sent a branch-all email to IB for access and never sent multiple requests. An employee responded and gave Schulte access.

F. 15. c. On 5/26 an employee granted Schulte's request for access without proper vetting
--> TRUTH: The vetting procedure for access wasn't established and emailed to the division until AFTER this incident.

F. 15. c. i. On 5/26, Schulte revoked computer access permissions of all other CIA group employees to work on Project-1
--> TRUTH: Schulte was told his new branch would retain his old project so he changed permissions from his old branch to new branch. His entire branch still had access.

F. 15. c. ii. Once his conduct was discovered Schulte was issued a letter of warning
--> TRUTH: Schulte directly emailed HR and his group chief. They knew only because of this email. Schulte had been told was his project so when he saw his access was revoked again by [redacted] he notified management.

F. 15. c. iii. Schulte disagreed with some of the letter's conclusions
--> TRUTH: Schulte very clearly disagreed with ALL conclusions.

I 20 Schulte repeatedly initiated contact

--> TRUTH Schulte was contacted by Tandeep who panicked him by saying everyone thinks it was him

I 20 a Schulte repeatedly asked about the status of the investigation

--> TRUTH He never asked about status

Paragraph form:

The FBI wrongly assume that 200 people within one CIA group had access to the stolen data when in reality it was double this; The FBI then wrongly assume the data was taken from the backup server based solely on observed behavior from the released documents showing "iterations" which they wrongly attribute to a backup when in reality this is a function of the data and would exist if the data was taken from a backup or not;

The FBI then use their wrong assumptions that the data was a backup to assume the data was stolen from a backup on a certain date because they see no data after this date when in reality, even assuming their faulty assumption of the involvement of a backup is true, the only conclusion that can be drawn is a lower bound of the first possible date the data could have been stolen and not an exact date.

The FBI then use their wrong assumptions of the date format of theft of data to point blame at Joshua Schulte, claiming he had logon access to the backup server when in actuality he had no domain credentials and could not directly access the backup server.

The FBI then incredulously confuse permissions of the administration of "web-based services" with LAN permissions and omit an entire branch of people (10-12) who also possessed these administration abilities and attribute this Access Control List to servers when in reality they are TWO separate ACLs.

The FBI then mislead the judge and claim Josh was the only person of the three people from this separate access control list, excluding the other 12 from IB, whose truename wasn't exposed in the leak when in reality only pseudonyms were exposed.

The FBI then string their incorrect assumptions together and claim Schulte was the only person of the wrong access control list who had access to the backup server (which he didn't), the wrongly assumed location of the stolen data, on 3/7, the wrongly assumed date of the theft.

Not to be outdone, the FBI then seek to find confirmation bias in the incredulous events that led to his resignation, which clearly point to mischief and illegal behavior of others. Namely:

The FBI claim Schulte's LAN admin privs (which he never possessed) were revoked on 4/4, but even his administration of the "web-based services" were not revoked.

The FBI then claim that on 4/11 Schulte logged onto the LAN and reinstated his admin privs which makes no sense and severely undermines the notion of privileges and system administration.

In reality on 4/11 Josh confronted one of the other admins ^{Jeremy Weber} for unauthorized changes which Josh promptly reverted, and which had absolutely nothing to do with Project-1.

On 4/18, Josh was issued a memo of warning and had his access to the "web-based services" revoked after the employee contacted the group chief that he was having an affair and told her to revoke Josh's permissions.

The FBI then claim on 5/26 Josh again requested full access to Project-1, when in reality he had never requested access nor changed access to this project before, but rather, requested permission after finishing his previous project and discovering, to his surprise, that the project he was assigned to work on next, Project-1, was inaccessible.

The FBI claim that before receiving a response to his initial request, Josh requested access from another employee when in reality Josh had simply and without any deceitful intent, emailed ALL of IB to request permissions in a group-all email.

The FBI claim the individual who responded and gave Josh access did so without properly vetting the request when in reality these vetting procedures were not created nor disseminated to the division until several weeks later.

The FBI claim Josh revoked computer access permissions of all CIA group employees on Project-1 when in reality, and

consistent with Josh's belief that the project belonged to him and his branch, changed the project's permissions from the previous branch to his new branch.

The FBI then omit how Josh sent an email to HR and his group chief specifically stating that this abuse of permissions was further evidence of the employee that Josh previously reprimanded's wrongdoing and unauthorized manipulation of permissions. This group chief, still in an active affair with the employee, then sought to conceal the employee's behavior and issue Josh a letter of warning for self-granting admin privileges by overtly emailing an entire branch for request and then emailing her when he discovered what he determined to be a security breach. Wouldn't you resign after all this bullshit too?

Fuck the government,
Josh Schulte

UNITED STATES DISTRICT COURT

for the Southern District of New York

17 MAR 18 56

In the Matter of the Search of (Briefly describe the property to be searched or identify the person by name and address) 200 East 39th Street, Apartment 8C, New York, New York 10016, as well as Any Closed Containers/Items

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):

200 East 39th Street, Apartment 8C, New York, New York 10016 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):

- [x] evidence of a crime; [x] contraband, fruits of crime, or other items illegally possessed; [x] 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) 18 U.S.C. 793(d), 793(e), 1030(a)(1), 1030(a)(2)(B). Offense Description(s) 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

- [x] Continued on the attached sheet. [x] 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 Jeff D. Donaldson, FBI Printed name and title

Sworn to before me and signed in my presence.

Date: 03/13/2017

City and state: New York, NY

S/Barbara Moses Judge's signature Honorable 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 Warrant for the Premises Known and Described as 200 East 39th Street, Apartment 8C, New York, New York 10016, as well as Any Closed Containers/Items Contained in the Premises

TO BE FILED UNDER SEAL

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

SOUTHERN DISTRICT OF NEW YORK) ss.:

JEFF D. DONALDSON, being duly sworn, deposes and says:

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 2010. I am currently assigned to a squad responsible for counterespionage matters and have worked in the field of counterintelligence from 2010 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 a warrant to search the premises specified below ("Subject Premises") for the items and information described in Attachment A. This Affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). 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 my 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.

B. The Subject Premises

3. The Subject Premises is particularly described as apartment 8C in a residential apartment building located at 200 East 39th Street, New York, New York 10016 (the "Building"). The Building is located near the corner of 39th Street and Third Avenue in Manhattan. The Building is nineteen stories high and contains approximately ninety-one apartment units. The Subject Premises is a one-bedroom apartment located on the eighth floor of the Building, and it is clearly identifiable as Apartment 8C from the outside of the Subject Premises.

C. The Subject Offenses

4. For the reasons detailed below, I believe that there is probable cause to believe that the Subject Premises 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); and (iv) intentionally exceeding authorized access to a computer 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) (collectively the "Subject Offenses").

D. Terminology

5. The term "computer," as used herein, is defined as set forth in 18 U.S.C. § 1030(e)(1).

6. The terms "records," "documents," and "materials" include all information recorded in any form, visual or oral, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device), as well as the equipment needed to record such information (including but not limited to cameras and video recording and storage devices).

II. 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 7, 2016 and the night of March 8, 2016.

i. This is based on preliminary analysis of the timestamps associated with the Classified Information which indicates that March 7, 2016 was the latest (or most recent) creation or modification date associated with the Classified Information.

ii. Because, for the reasons described below (*see infra* Part C.10), 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 7, 2016 (after the March 7 nightly back-up was completed) or on March 8, 2016 (before the March 8 nightly back-up was completed).

iii. This is so because if the Classified Information was copied before the March 7 back-up, one would *not* expect to see in the Classified Information documents dated as late as March 7. And if the Classified Information was copied after the March 8 back-up, one *would* expect to see documents dated on or after March 8 because the "back-ups" occur approximately each day.¹

¹ It is of course possible that the Classified Information was copied later than March 8, 2016 even though the creation/modification dates associated with it appear to end on March 7, 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 March 7, 2016. (Conversely, however, the Classified Information is unlikely to have been copied before March 7, 2016, because it contains data that was created as recently as March 7, 2016.) Because the most recent timestamp on the Classified Information reflects a date of March 7, 2016, preliminary analysis indicates that the Classified Information was likely copied between the end of the day on March 7 and the end of the day on March 8.

d. The Classified Information was publicly released by WikiLeaks exactly one year to the day (March 7, 2017) from the latest date associated with the Classified Information (March 7, 2016).

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).

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.² 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.

² In its press release announcing the publication of the Classified Information, WikiLeaks stated that the Classified Information originated from "an isolated, high-security network."

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 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.³

e. As described above (*see supra* Part II.A.8.c), because the most recent timestamp associated with the Classified Information appears to be March 7, 2016, it is likely that the Classified Information was copied from the Back-Up Server after the daily back-up on March 7, 2016, and before the daily back-up on March 8, 2016.

D. TARGET SUBJECT JOSHUA ADAM SCHULTE Was One of Only Three Employees Across the Entire CIA 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

³ 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.

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.⁴

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.

⁴ 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, at least theoretically, gain access to the Back-Up Server by finding a "back-door" into the Back-Up Server.

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 entire 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 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 7 and 8, 2016—The Likely Dates of the Copying of the Classified Information

13. As described above (see *supra* Part II.C.10), it appears likely that the Classified Information was copied between March 7 and March 8, 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. 10:01 a.m. until 7:16 p.m. on March 7, 2016; and
- ii. 10:19 a.m. until 7:40 p.m. on March 8, 2016.

b. Based on my conversations with other law enforcement agents and others, and my review of documents, I know that on March 8, 2016, the CIA Group held an offsite management retreat for many of its senior and midlevel managers. Accordingly, on March 8th, much of the CIA Group's management, including some to whom SCHULTE reported, were not present in the CIA Component building where SCHULTE and other CIA Group employees worked.

c. I further 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. At least two of those three employees were at the offsite management retreat on March 8, 2016.

d. As described above, in March 2016, only two CIA employees in addition to SCHULTE were designated Systems Administrators with access to the CIA Group's Back-Up Server from which the Classified Information was likely copied. On March 8, 2016, one of those two other designated Systems Administrators was at the offsite management retreat. (The retreat was held at a location that did not have any access to the CIA Group's LAN, including the Back-up Server, and therefore afforded no access to the Classified Information.)⁵

⁵ On March 7 and 8, 2016, the third of the three CIA employees with Systems Administrator access was located at a CIA facility that did, in fact, have access to the Back-Up Server from which the Classified Information was likely copied.

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-1.⁶

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 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

⁶ 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.

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 the unauthorized duplication, retention and removal of the Classified Information from the CIA Group's computer network, and its placement on the publicly available Internet, exceeds the authorized access to those government-owned and controlled computer networks of any user. *See* 18 U.S.C. § 1030.

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 purposes 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.⁷

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 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:

⁷ 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.

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.”⁸

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

⁸ 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).

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

I. SCHULTE's Recent Inquiries About the Status of the Investigation

20. 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 that 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.

J. SCHULTE's Planned Travel

21. Based on my conversations with other law enforcement agents and others, and my review of documents, including information provided by the Department of Homeland Security, I understand that SCHULTE has booked an international flight departing in four days—Thursday, March 16, 2017. (Return travel to the United States is booked for a few days later.) The aforementioned records and conversations reflect that this is only SCHULTE's second trip reflected in in DHS records outside the United States.

K. Probable Cause Justifying Search of the Subject Premises

22. Thus, based on the above, I submit that there is probable cause to believe that SCHULTE has committed by the Subject Offenses by stealing a substantial amount of classified information from the CIA and has transmitting that information to individuals not authorized to receive it, thereby endangering the nation's national security. Based on my training and

experience, I know that individuals who are involved in the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials use computers and other electronic devices in furtherance of their criminal activities. Based on my training and experience, I also know that individuals typically keep their computers and other electronic devices in their homes.

23. Based on my participation in this investigation, I believe that SCHULTE resides at the Subject Premises. Among other things, I have reviewed records provided by SCHULTE's employer in New York City, which indicate that SCHULTE resides at the Subject Premises. I have also reviewed SCHULTE's credit card records, which reflect that SCHULTE resides at the Subject Premises. I have also spoken with other law enforcement officers who have observed SCHULTE enter and exit the Building on several occasions since on or about March 8, 2017. Those law enforcement officers have also told me that the Building has an electronic directory that lists SCHULTE's name as the individual residing in the Subject Premises.

L. Probable Cause Justifying Search of ESI

24. As noted above, individuals who engage in the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials often use computers and other electronic devices to store documents and records relating to their illegal activity. Individuals engaged in these activities use electronic devices to, among other things, store copies of classified documents or materials; engage in email correspondence relating to their illegal activity; store contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social media accounts; and/or store records of illegal transactions involving classified documents.

25. Individuals who engage in the criminal activity described herein, in the event that they change computers, will often back up or transfer files from their old computers' hard drives to that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity. In addition, individuals who engage in such criminal activity will often also store or transfer files on electronic storage media other than computer hard drives, including thumb drives, flash memory cards, CD-ROMs, or portable hard drives to, for example, facilitate the use of the information or to transfer it to co-conspirators in support of the criminal scheme.

26. Individuals who engage in criminal activity involving computers and electronic devices also often maintain physical evidence of their criminal activity, including, among other things, printouts of documents and records that are also stored electronically, as described above, or handwritten notes of the same, for example as a backup in case of a failure of the electronic media on which they were stored or to facilitate use of the data.

27. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files can be stored on a hard drive for years at little or no cost. 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. Specifically, when a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Deleted files, or remnants of deleted files, may accordingly reside in "slack space" (space that is not being used for storage of a file) for long periods of time before they are overwritten. In addition, a computer's operating system may keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via

the Internet are generally automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

28. Based on the foregoing, I respectfully submit that there is probable cause to believe that SCHULTE is committing or has committed the Subject Offenses, and that evidence of this criminal activity is likely to be found in the Subject Premises and on computers and electronic media found in the Subject Premises.

III. Items to Be Seized

29. Closed or Locked Containers. Based on my training, experience, participation in this and other investigations, I know that individuals who participate in criminal activities routinely secrete and store books, records, documents, currency and other items of the sort described in Attachment A in secure locations like safety deposit boxes, suitcases, safes, key-lock strong boxes, and other types of locked or closed containers in an effort to prevent the discovery or theft of said items. The requested warrant and search procedure includes a search of any closed containers on the Subject Premises, including cabinets, vehicles, doors to rooms, sheds, outbuildings, and other appurtenances located on or within the Subject Premises whether they are locked or unlocked.

30. Electronic Devices. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the requested warrants would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. Based upon my training and experience and information related to me by agents and others involved in the forensic

examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, thumb drives, magnetic tapes and memory chips. I also know that during the search of the Subject Premises it may not be possible to fully search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process, which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

b. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the Subject Premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 160 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 80 million pages of data, which, if printed out, would result in a stack of paper over four miles high.

c. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files;

however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

31. In light of these concerns, I hereby request the Court's permission to copy at the Subject Premises information stored on computer hardware (and associated peripherals) that may contain some or all of the evidence described in Attachment A hereto, and to conduct an off-site search of such copies for the evidence described, using the general procedures described in Attachment A. However, to the extent law enforcement is unable to copy electronic devices at the Subject Premises, I hereby request the Court's permission to seize those devices and search them off-site.

IV. Procedures for Searching ESI

A. Execution of Warrant for ESI

32. Federal Rule of Criminal Procedure 41(c)(2)(B) provides that a warrant to search for and seize property "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review." Consistent with Rule 41, this application requests authorization to search and/or seize any computer devices and storage media and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

- First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.
- Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.
- Third, there are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.
- Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

B. Review of ESI

33. Following the search of any computer devices and storage media and/or the creation of forensic image copies, 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 therein for information responsive to the warrant.

34. In conducting this review, law enforcement personnel 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 or 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.)

35. 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 personnel may need to conduct a complete review of all the ESI from searched devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

C. Return of ESI

36. If the Government seizes any electronic devices, later determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return these items, 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.

V. Execution of the Search Warrant: Necessity of Covert Search and Delayed Notification

37. I respectfully request that the search warrant permit law enforcement agents to execute the search at any time in the day or night. I also respectfully request that the search warrant permit law enforcement agents to execute the search warrant covertly without advance or contemporaneous notice of the execution of the warrant, or if they deem covert execution impracticable to execute the search warrant overtly without further order of the Court. Law enforcement agents will provide notice of the execution of the warrant, if it is executed covertly, within seven days of execution unless there is a new showing, made to the Court, that delayed notice is appropriate. If the warrant is executed overtly, notice will be provided at or as soon as practicable after the execution.

a. As described in greater detail above and below, there is probable cause to believe that SCHULTE has stolen a substantial amount of classified information and transmitted that information to those not authorized to receive it, thereby endangering the nation's national security.

b. SCHULTE likely engaged in these activities by using sophisticated computer skills to exfiltrate a substantial amount of data onto a removable drive and then covertly removed that drive from the CIA.

c. If SCHULTE is provided advance or contemporaneous notice of the execution of this search warrant, it may allow him to destroy evidence of his crimes on electronic devices by, for example, deleting drives or activating encryption programs that would make his devices virtually impossible to access.

d. Moreover, law enforcement agents will likely need some time to review and analyze any electronic devices identified at the Subject Premises. If SCHULTE is provided advance or contemporaneous notice of the search of the Subject Premises, he may be able to destroy evidence that can be developed based on the search of electronic devices.

38. Pursuant to Title 18, United States Code, Section 3103a(b)(1), delayed notification may be provided for a search warrant obtained pursuant to Rule 41 of the Federal Rules of Criminal Procedure if “the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result.” Delayed notification pursuant to this provision may only be provided for a reasonable period not to exceed 30 days, although it may be extended by the court for good cause shown, pursuant to Title 18, United States Code, Sections 3103a(b)(3) and 3103(c). A delayed notice warrant obtained pursuant to this provision prohibits “the seizure of tangible property, any wire electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, *except where the court finds reasonable necessity for the seizure.*” Title 18, United States Code, Section 3103(b)(2) (emphasis added).

39. The investigation of the Subject Offenses and SCHULTE is on-going, and remains extremely sensitive. The FBI is continuing to review an enormous volume of electronic evidence, much of which remains highly classified and extremely sensitive. In addition, based on *inter alia* the statements in WikiLeaks March 7, 2017 press release accompanying the Classified Information, it appears at least possible that additional CIA information may have been stolen and provided to WikiLeaks or others not authorized to receive it. Accordingly, ensuring that the investigation remains covert for as long as possible is at its zenith. Public disclosure of the search prematurely could cause evidence to be destroyed or additional information to be hastily released

onto the Internet. In that context, I know, based on my review of the WikiLeaks press release, that they claimed to have refrained from publishing additional information they purport to possess such as “‘armed’ cyberweapons,” which I understand based on my training, experience and involvement in this investigation to mean the specific computer code they claim could actually be used to perpetrate a cyber-attack or penetration). They also claim to have “anonymi[z]ed some identifying information,” which I understand, based on my training, experience, and involvement in this investigation, to include the names of covert CIA operatives and possibly covert United States Government locations. Finally, because SCHULTE has booked an overseas trip for this Thursday, it is critical that, to the extent possible, the search be conducted in such a way as to minimize the possibility that it causes him to flee or to destroy evidence. In light of the foregoing, it is reasonably necessary to conduct the search requested herein covertly.

40. Consistent with Title 18, United States Code, Section 3103a(b)(2), this application requests that any notice otherwise required for the seizure and search of information be delayed for a period of 30 days in light of the reasonable necessity – comprising both the investigatory aims and mitigating goals of this investigation – for such a delay.

VI. Conclusion and Ancillary Provisions

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

42. 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.



JEFF D. DONALDSON
Special Agent
Federal Bureau of Investigation

Sworn to before me on
this 13th day of March 2017

S/Barbara Moses

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

Attachment A

I. Premises to be Searched—Subject Premises

The premises to be searched (the "Subject Premises") is described as follows, and includes all locked and closed containers found therein:

The Subject Premises is particularly described as apartment 8C in a building located at 200 East 39th Street, New York, New York 10016 (the "Building"). The Building is located near the corner of 39th Street and Third Avenue. The Building is nineteen stories high and contains approximately ninety-one apartment units. The Subject Premises is a one-bedroom apartment located on the eighth floor of the Building, and it is clearly identifiable as apartment 8C from the outside of the Subject Premises.

II. Execution of the Warrant

Law enforcement agents are permitted to execute the search warrant at any time in the day or night, and further to execute the search warrant covertly without advance or contemporaneous notice of the execution of the search warrant. Law enforcement agents will provide notice of the execution of the warrant within seven days of execution unless there is a new showing, made to the Court, that delayed notice is appropriate.

III. Items to Be Searched and Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be searched and/or seized from the Subject Premises include the following 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); and (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) (collectively, the "Subject Offenses"):

1. Evidence concerning occupancy or ownership of the Subject Premises, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.
2. Evidence concerning the identity or location of, and communications with, any co-conspirators.
3. Any and all notes, documents, records, correspondence, or materials, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, and handwritten notes), pertaining to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials.
4. Electronic devices (including but not limited to computers, tablets, smartphones, and cellular telephones) and storage media used in furtherance of the Subject Offenses, containing evidence of the Subject Offenses, or containing evidence authorized for seizure in paragraphs 1, 2 and 3 above. The term "storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

5. Electronic forensic evidence relating to the Subject Offenses, including for any electronic device or storage media whose search and/or seizure is authorized by this warrant as described above in paragraph 4 (hereinafter, "Computers"¹), including:

- a. evidence of the times the Computers were used in furtherance of the Subject Offenses;
- b. passwords, encryption keys, and other access devices that may be necessary to access the Computers;
- c. documentation and manuals that may be necessary to access the Computers or to conduct a forensic examination of the Computers;
- d. evidence of software that would allow others to control the Computers, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- e. evidence indicating how and when the Computers were accessed or used in furtherance of the Subject Offenses;
- f. evidence indicating the Computers' user's/users' state of mind as it relates to the Subject Offenses;
- g. evidence of the attachment to the Computers of other storage devices or similar containers for electronic evidence in furtherance of the Subject Offenses;

¹ The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

- h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computers;
- i. records of or information about Internet Protocol addresses used by the Computers;
- j. records of or information about the Computers' Internet activity in furtherance of the Subject Offenses, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

6. If law enforcement personnel seize the computer(s) or other electronic device(s), the personnel will search the computer and/or device(s) within a reasonable amount of time, not to exceed 60 days from the date of execution of the warrant. If, after such a search has been conducted, it is determined that a computer or device contains any data listed in paragraphs 1 through 3, the Government will retain the computer or device. If it is determined that the computer(s) or device(s) are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(b), such materials and/or equipment will be returned within a reasonable time. In any event, such materials and/or equipment shall be returned no later than 60 days from the execution of this warrant, unless further application is made to the Court.

B. Search and Seizure of Electronically Stored Information

The items to be searched and seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section III.A of this Attachment above, including, but not limited to,

desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be searched and seized from the Subject Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.
3. Any evidence concerning the persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, 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 therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques, including but not limited to:

- surveying various file "directories" 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);
- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files;
- scanning storage areas for deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- making reasonable efforts to utilize computer search methodology to search only for files, documents, or other electronically stored information within the categories identified in Sections I.A and I.B of this Attachment.