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

Alexandria Division

IN THE MATTER OF THE SEARCH OF THE SAMSUNG GALAXY S9+ WIRELESS TELEPHONE ASSIGNED TELEPHONE NUMBER 610-348-4313 AND IMSI 310410189527000	Case No.1:19-sw-1343 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, Donny Kim, Special Agent of the Federal Bureau of Investigation ("FBI"), being duly sworn, depose and state that:

INTRODUCTION AND AGENT BACKGROUND

1. I am an investigative or law enforcement officer of the United States, within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") assigned to the Washington Field Office, and have been since 2007. During this time, I have received training at the FBI Academy located at Quantico, Virginia, specific to counterintelligence and espionage investigations. I currently am assigned to investigate counterintelligence and espionage matters. From 1999 to 2007, I was a Special Agent with the U.S. Department of State, Diplomatic Security Service and worked counterintelligence and espionage matters. Based on my experience and training, I am familiar with efforts used to unlawfully collect and disseminate sensitive government information, including national defense information ("NDI").

3. I make this affidavit in support of an application for a warrant to seize and search a black Samsung Galaxy S9+ wireless telephone assigned telephone number 610-348-4313 and IMSI 310410189527000 ("DEVICE") and subscribed to by Henry Kyle FRESE, further described in Attachment A, for the evidence described in Attachment B. As further described below, this application specifically seeks authority to open and search either a device storage lockbox on the Reston, Virginia, premises of the Defense Intelligence Agency ("DIA"), located at 12300 Sunrise Valley Drive, Reston, Virginia 20191, or a black Nissan Rogue with Virginia license plate 4790-PT and VIN 5N1AT2MV9HC842483, registered to Henry Kyle FRESE, in order to seize the DEVICE.

4. As a result of my personal participation in this investigation, and reports made to me by United States Intelligence Community Agency 1 ("U.S. Government Agency 1") and the Defense Intelligence Agency ("DIA"), I am familiar with all aspects of this investigation. On the basis of this familiarity, and on the basis of other information that I have reviewed and determined to be reliable, I believe that the facts in this affidavit show that there is probable cause to believe that FRESE has committed, is committing, and will continue to commit violations of 18 U.S.C. § 793(d), willful transmission of national defense information. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. These acts occurred within the Eastern District of Virginia. There is probable cause to seize and search the black Samsung Galaxy S9+ wireless telephone assigned telephone number 610-348-4313 and IMSI 310410189527000 for evidence of the crimes further described in Attachment B.

STATUTORY AUTHORITY AND DEFINITIONS

6. For the reasons set forth below, I believe that there is probable cause to believe that FRESE committed violations of Title 18, United States Code, Section 793(d) and (e), willful transmission of national defense information (the "Subject Offenses").

7. Under 18 U.S.C. § 793(d), "[w]hoever, lawfully having possession of, access to, or control over any document . . . or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted" or attempts to do or causes the same "to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it" shall be fined or imprisoned not more than ten years, or both.

8. Under 18 U.S.C. § 793(e), "[w]hoever, having unauthorized possession of, access to, or control over any document . . . or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted" or attempts to do or causes the same "to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to

the officer or employee of the United States entitled to receive it" shall be fined or imprisoned not more than ten years, or both.

9. Under Executive Order 13526, information in any form may be classified if it: (1) is owned by, produced by or for, or is under the control of the United States Government; (2) falls within one or more of the categories set forth in the Executive Order [Top Secret, Secret, and Confidential]; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security.

10. Where such unauthorized disclosure could reasonably result in damage to the national security, the information may be classified as "Confidential" and must be properly safeguarded. Where such unauthorized disclosure could reasonably result in serious damage to the national security, the information may be classified as "Secret" and must be properly safeguarded. Where such unauthorized disclosure could reasonably result in exceptionally grave damage to the national security, the information may be classified as "Top Secret" and must be properly safeguarded.

11. Classified information of any designation may be shared only with persons determined by an appropriate United States Government official to be eligible for access, and who possess a "need to know." Among other requirements, in order for a person to obtain a security clearance allowing that person access to classified United States Government information, that person is required to and must agree to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified

information in unauthorized locations. If a person is not eligible to receive classified information, classified information may not be disclosed to that person. In order for a foreign government to receive access to classified information, the originating United States agency must determine that such release is appropriate.

12. Pursuant to Executive Order 13526, classified information contained on automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information must be maintained in a manner that: (1) prevents access by unauthorized persons; and (2) ensures the integrity of the information.

13. 32 C.F.R. Parts 2001 and 2003 regulate the handling of classified information. Specifically, 32 C.F.R. § 2001.43, titled "Storage," regulates the physical protection of classified information. This section prescribes that Secret and Top Secret information "shall be stored in a GSA-approved security container, a vault built to Federal Standard (FHD STD) 832, or an open storage area constructed in accordance with § 2001.53." It also requires periodic inspection of the container and the use of an Intrusion Detection System, among other things.

PROBABLE CAUSE

14. Henry Kyle FRESE ("FRESE") is under investigation for improperly removing and transmitting classified U.S. government national defense materials to a journalist ("Journalist 1") employed by a certain news outlet ("News Outlet 1"), and to a second journalist ("Journalist 2") employed by a second news outlet ("News Outlet 2"), from on or about April 2018 through the present. FRESE is a DIA employee assigned to a workspace in Reston, Virginia, in the Eastern District of Virginia. He has been employed at DIA since in or about February 2018 as a

counterterrorism analyst. Prior to that, from in or about January 2017 until in or about February 2018, FRESE was a contract employee with a cleared intelligence contractor working in a DIA workspace in the Eastern District of Virginia. Throughout this time, FRESE has held a Top Secret//Sensitive Compartmented Information ("TS//SCI") security clearance.

15. FRESE works inside a Sensitive Compartment Information Facility (SCIF) at the DIA workspace in Reston, Virginia, in the Eastern District of Virginia. Employees are not allowed to bring their cellular telephones into the SCIF. Generally, employees either store their cellular telephones inside DIA-provided lockboxes outside of the SCIF spaces, or simply leave their cellular telephones in their vehicle in the facility parking lot. Based on ongoing law enforcement surveillance of FRESE, I know that FRESE generally commutes to work at the DIA facility in his black Nissan Rogue with Virginia license plate 4790-PT and VIN 5N1AT2MV9HC842483. Also based on this surveillance, I believe that FRESE routinely stores the DEVICE inside his vehicle in the DIA facility parking lot while he is at work, when he does not use the DIA-provided lockboxes.

16. U.S. government agencies have confirmed that between at least early May 2018 and mid-July 2018, News Outlet 1 published eight articles that contain classified national defense information that relates to the capabilities of certain foreign countries' weapons systems. Journalist 1 is the author of all of these articles. These articles contained classified intelligence from five intelligence reports (the "compromised intelligence reports") dated on or about early March 2018 through mid-June 2018. The eight articles published by News Outlet 1, and the intelligence reporting from which they are derived, both contain information that is classified up to the TS//SCI level, indicating that its unauthorized disclosure could reasonably be expected to

result in exceptionally grave damage to the national security. The compromised intelligence reports are marked as such.

17. U.S. Government information technology system audit logs analyzed by FBI show that only 26 individuals, one of whom is FRESE, accessed all five of the compromised intelligence reports.

18. In his most current background security form (the "SF-86") in December 2017, on file at the U.S. Government Organization, FRESE listed his mobile phone number as "610-348-4313" (the telephone number associated with the DEVICE). Records checks for FRESE also show the DEVICE as a telephone number associated with FRESE. Public records checks for Journalist 1 show a certain telephone number ("TELEPHONE 2") as a telephone number associated with Journalist 1.

19. The FBI conducted public record and open source checks on the individuals to determine the genesis of contact between FRESE and the News Outlet. Open source records checks showed that FRESE has a public Twitter account. Journalist 1 also maintains a public Twitter account that FRESE "follows," meaning that FRESE's Twitter account subscribes to Journalist 1's Tweets and account updates. Journalist 1's Twitter account also follows FRESE's Twitter account.[1] Public records checks also show that FRESE and Journalist 1 had the same residential address from August 2017 through August 2018. Based on reviews of FRESE's and Journalist 1's public social media pages, it appears that they were involved in a romantic relationship for some or all of that period of time.

---

[1] A Twitter user can "follow" other Twitter users, which means subscribing to those users' Tweets and site updates. Each user profile page includes a list of the people who are following that user (*i.e.*, the user's "followers" list) and a list of people whom that user follows (*i.e.*, the user's "following" list).

20. On August 26, 2019, the Honorable Leonie M. Brinkema, United States District Judge for the Eastern District of Virginia, authorized an Order for the interception of wire and electronic communications to and from the DEVICE pursuant to Section 2518 of Title 18, United States Code (the "Title III monitoring"). The Title III monitoring of the DEVICE showed that FRESE accessed Twitter on the DEVICE. Twitter records also show periodic logins to FRESE's Twitter account from an Internet Protocol ("IP") address that resolves back to an IP address range registered to AT&T Mobility LLC, the same cellular phone carrier as the DEVICE.

21. AT&T records associated with the DEVICE show 508 total calls and 37 text messages between the DEVICE and **Journalist 1** from March 1, 2018 through October 7, 2019. AT&T records associated with the DEVICE show 22 calls and 150 text messages between the DEVICE and **Journalist 2** from May 1, 2018 through October 7, 2019. On August 4, 2019, subsequent to receiving a June preservation request from the FBI, AT&T provided returns for a search warrant on the DEVICE, but there was no text message content provided. I have spoken with a representative of AT&T who has confirmed that AT&T does not have in its possession any text messages to or from the DEVICE. I believe that seizing the phone will likely allow the FBI to see the historical text exchanges between FRESE and Journalist 1 and Journalist 2 that predate the Title III monitoring that began August 26, 2019.

22. TELEPHONE 3 is the registered phone number for **Journalist 2's** known social media accounts, including her Twitter account, in which she self identifies as a correspondent covering national security for **News Outlet 2**. Public records checks also show **Journalist 2** as the user of TELEPHONE 3.

23. **Journalist 2** works for **News Outlet 2**. **News Outlet 1** and **News Outlet 2** are owned by the same parent company and are part of the same group of publicly affiliated news outlets. **Journalist 1** and **Journalist 2** report on the same topics and were assigned to cover the same location from mid-2018 into 2019. **Journalist 2** is a more senior journalist, who has been assigned to that location for over a decade. In early July 2019, **Journalist 1** and **Journalist 2** co-authored an article related to topics similar to Journalist 1's article containing classified NDI. On **Journalist 1's** personal Twitter page, **Journalist 1** Tweeted a link to the early July 2019 article, noting it was the first co-authored piece of the pair. On **Journalist 2**'s personal Twitter page, **Journalist 2** Tweeted a link to the article and stated **Journalist 1** was a "colleague" who helped co-author the news article. **Journalist 1** subsequently retweeted **Journalist 2's** Tweet.

24. Computer network logs from DIA show FRESE ran searches using terms related to the same topics discussed in the compromised intelligence reports. These topics fall outside the scope of FRESE's job duties for his position as a counterterrorism analyst with the DIA.

25. In the spring of 2018, **Journalist 1** called the DEVICE. Approximately 34 minutes later, **Journalist 1** called the DEVICE for a call that lasted approximately six minutes. The next day, FRESE used search terms related to the topics contained in the five compromised intelligence reports, which contained information classified up to the TS//SCI level. The search terms were not related to topics FRESE would search as part of FRESE's job responsibilities. Approximately 29 minutes after conducting the search, FRESE accessed **Intelligence Report 1**, one of the five compromised intelligence reports. Three days later, FRESE again accessed **Intelligence Report 1**.

26. Search warrant returns from Twitter show that, seven days after FRESE accessed **Intelligence Report 1** for the second time, **Journalist 1** wrote a Twitter Direct Message ("DM")

to FRESE in which she asked whether FRESE would be willing to speak with **Journalist 2**. FRESE stated that he was "down" to help **Journalist 2** if it helped **Journalist 1** because he wanted to see **Journalist 1** "progress." During the same Twitter exchange, **Journalist 1** also indicated that certain officials within the United States government were calling into question information related to the topic of **Intelligence Report 1**. FRESE characterized the denial as "weird" and commented that a separate U.S. Intelligence Agency, **U.S. Government Agency 2**, had supplied certain information contained within **Intelligence Report 1**.

27. The same day following the Twitter conversation discussed above, at 7:42 p.m., **Journalist 1** placed a call to the DEVICE that lasted approximately eight minutes. At 1:31 a.m. the following day, **Journalist 1** placed a call to the DEVICE that lasted approximately 15 minutes.

28. Several days later, **Journalist 2** sent the DEVICE a text message. Approximately six hours later, **Journalist 2** sent the DEVICE another text message. Within the next 45 minutes, FRESE and **Journalist 2** exchanged five additional text messages with each other. Then, at approximately 3:38 p.m., the DEVICE called **Journalist 1**.

29. The morning of the next day, FRESE again used search terms related to the topics contained in **Intelligence Report 1**, which contained information classified up to the TS//SCI level. The search terms were not related to topics FRESE would search as part of FRESE's job responsibilities. At approximately 12:15 p.m., the DEVICE called **Journalist 1**. The call lasted approximately seven minutes. At approximately 3:24 p.m., the DEVICE called **Journalist 2**. That call lasted approximately 36 minutes. At approximately 4:01 p.m., **Journalist 1** then called the DEVICE. That call lasted approximately one minute. Approximately 30 minutes later, **News Outlet 1** published an online article ("**Article 1**"), authored by **Journalist 1**, which

contained classified national defense information from **Intelligence Report 1**. **Journalist 1** then Tweeted a link to **Article 1**. The next day FRESE re-Tweeted **Journalist 1's** Tweet of **Article 1**. U.S. government agencies have confirmed that **Article 1** contains classified NDI. I believe that FRESE passed **Journalist 1** the classified NDI from **Intelligence Report 1** that appeared in **Article 1.**

30. AT&T records show that, on at least eight separate occasions in mid-2018, the DEVICE communicated with either **Journalist 1** or **Journalist 2**, or both, on the same day as **Journalist 1's** publication of an article containing classified NDI from the compromised intelligence reports..

31. On September 24, 2019, FRESE viewed two additional intelligence reports, **Intelligence Report 2** and **Intelligence Report 3**. Both **Intelligence Report 2** and **Intelligence Report 3** were published in mid-September 2019 and both contained NDI classified up to the SECRET//SCI level. **Intelligence Report 2** and **Intelligence Report 3** both relate to the same subject matter. On September 24, 2019, at 7:11 p.m., FRESE sent a text message to **Journalist 2** asking **Journalist 2** to call him. Less than a minute later, **Journalist 2** called FRESE, and they spoke for approximately five minutes. According to AT&T geolocation data, FRESE was within the Eastern District of Virginia when he sent the text message and spoke with **Journalist 2** from the DEVICE.

32. **Journalist 2** asked FRESE what was "going on at work?" FRESE responded, "Uh, well it's nothing to do with, like what I cover, per usual but um, it's, so it's about, still like [topic of **Intelligence Reports 2 and 3**] . . . And I don't know if anyone's really commented on this but I saw a report, it's a few days old at this point, um, that basically the [foreign country]

are [topic of **Intelligence Report 2 and 3**]." U.S. government agencies have confirmed that the content FRESE provided Journalist 2 in the September 24, 2019 call contains classified information. I believe that FRESE used the DEVICE to provide classified NDI to Journalist 2.

33. **Journalist 2** asked FRESE for information that was "probably outside your lane as well, but if you ever hear anything about this whole like, [topic concerning the U.S. and a foreign government]" then "we'd definitely be interested in that as well." FRESE responded, "Yeah, of course."

TECHNICAL TERMS

34. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing

dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets,

and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

35. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

36. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

37. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

38. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

MANNER OF EXECUTION

39. This warrant seeks authorization to open and search either a device storage lockbox on the Reston, Virginia premises of the Defense Intelligence Agency ("DIA"), located at 12300 Sunrise Valley Drive, Reston, Virginia 20191, or a black Nissan Rogue with Virginia

license plate 4790-PT and VIN 5N1AT2MV9HC842483, registered to Henry Kyle FRESE, in order to seize the DEVICE and conduct the search described above.

CONCLUSION

39. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

_____

Donny Kim
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on _____, 201___

_____

Honorable Michael S. Nachmanoff
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

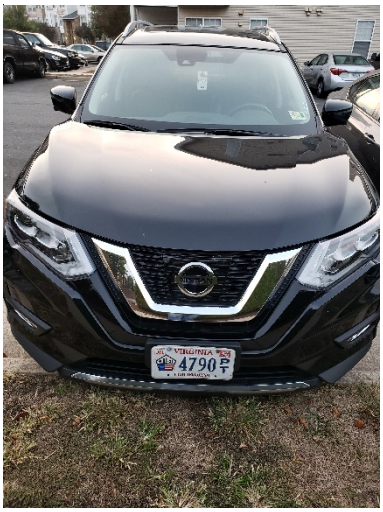
Property to Be Searched

The DEVICE to be seized and searched is a black Samsung Galaxy S9+ wireless telephone assigned telephone number 610-348-4313 and IMSI 310410189527000, with listed subscriber Henry Kyle FRESE.

To the extent necessary to seize the DEVICE, this warrant also authorizes the search of either:

a. A device storage lockbox on the Reston, Virginia, premises of the Defense Intelligence Agency ("DIA"), located at 12300 Sunrise Valley Drive, Reston, Virginia 20191; or

b. A black Nissan Rogue with Virginia license plate 4790-PT, with VIN 5N1AT2MV9HC842483, registered to Henry Kyle FRESE.



This warrant authorizes the forensic examination of the DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

1. All records on the Device described in Attachment A that relate to violations of **Title 18, United States Code Section 793** and involve **Henry Kyle FRESE** since **January 1, 2017,** including:

    a. Classified material

    b. Any U.S. Government material

    c. Any foreign government material

    d. Contacts, by any means, with foreign governments, foreign powers, or agents of foreign powers;

    e. Contact, by any means, with media outlets;

    f. Information, including communications in any form, regarding the retrieval, storage, or transmission of sensitive or classified material;

    g Information regarding tradecraft, how to obtain or deliver sensitive information, and/or how to avoid or evade detection by intelligence officials or law enforcement authorities.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.