16 MC 464 (PKC)

AO 93 (SDNY Rev. 05/10) Search and Seizure Warrant

ORIGINAL

# UNITED STATES DISTRICT COURT

for the

Southern District of New York

16 MAG 7063

| | | |
|---|---|---|
| In the Matter of the Search of<br>*(Briefly describe the property to be searched or identify the person by name and address)*<br><br>A Laptop Computer, Further Described Below and in Attachment A | )<br>)<br>)<br>)<br>)<br>) | Case No. |

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Southern District of New York *(identify the person or describe the property to be searched and give its location)*:

A Laptop Computer, Further Described As a Silver Dell Inspiron 15 7000 Series (7548) Laptop Computer Bearing Service Tag [redacted] Containing a Toshiba One Terabyte Hard Drive Bearing Serial Number [redacted] and That Is Currently Housed at the Federal Bureau of Investigation, New York Field Office, as described in Attachment A.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

**YOU ARE COMMANDED** to execute this warrant on or before 11/13/16 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10 p.m. ☑ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court.

☒ Upon its return, this warrant and inventory should be filed under seal by the Clerk of the Court. KNF *USMJ Initials*

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐for _____ days *(not to exceed 30)*.

☐until, the facts justifying, the later specific date of _____.

Date and time issued: 10/30/16 12:32 P.M. Kevin Nathaniel Fox *Judge's signature*

City and state: New York, New York Honorable Kevin Nathaniel Fox *Printed name and title*

AO 93 (Rev. 01/09) Search and Seizure Warrant (Page 2)

**Return**

| Case No.: | Date and time warrant executed: | Copy of warrant and inventory left with: |
|---|---|---|

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the Court.

Date: _____

_____
*Executing officer's signature*

_____
*Printed name and title*

## Attachment A

### I. Device To Be Searched

The device to be searched is a silver Dell Inspiron 15 7000 Series (7548) laptop computer bearing service tag [redacted] containing a Toshiba one terabyte hard drive bearing serial number [redacted] (the Subject Laptop), and that is currently housed at the Federal Bureau of Investigation, New York Field Office, 26 Federal Plaza, New York, New York 10278.

### II. Review of ESI on the Subject Devices

Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the Subject Laptop for the following evidence, contraband, fruits, and/or other items illegally possessed in violation of Title 18, United States Code, Section 793(e) and (f) (the Subject Offenses):

1. Data and information associated with the operation, use, maintenance, backup, auditing, and security functions of the Subject Laptop including, but not limited to:
   a. Emails and attachments, in any form;
   b. User and system files stored on the laptops, including file fragments and items carved from unallocated space;
   c. Logs, configuration files, and backups;
   d. Executable code and scripts; and
   e. Documents, database files, and spreadsheets;

2. Data and information electronically stored on the Subject Laptop related to communications with email accounts used by former Secretary of State Hillary Clinton during her tenure as Secretary of State;

3. Data and information on the Subject Laptop that might identify the person or persons who accessed classified information present on the Subject Laptop, including names, addresses, telephone numbers and other identifiers, email addresses, business information, the length of service (including start date), types of services utilized, means and source of payment for services (including any credit card or bank account number), and information about any domain name registration; and

4. Data and information stored on the Subject Laptop that might identify activity related to a computer intrusion, including, but not limited to evidence of malware or viruses, executable code or scripts, log files, audit files, system files, user and account information, IP addresses, computer hardware addresses, intrusion-detection logs, firewall and other network logs, anti-virus logs or anti-malware logs.

## III. Seizure for Later Review of Electronically Stored Information

### A. Seizure of Computer and Media

This warrant authorizes the seizure of a computer and electronic storage media as set forth below. In lieu of seizing any particular electronic storage media, this warrant also authorizes the copying of electronically stored information for later review. Electronic storage media which may be seized or copied include without limitation:

Computer devices, electronic media and electronic storage devices, including, but not limited to, a computer, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners and the data within the aforesaid objects relating to said materials, which may contain information within the scope of this warrant.

Any physical keys, encryption devices, and similar physical items that are necessary to gain access to the computer equipment, storage devices or data mentioned above, or any passwords, password files, test keys, encryption codes or other information necessary to access the above-mentioned computer equipment, storage devices or data.

### B. Review of Electronic Storage Media and Electronically Stored Information

Following creation of forensic image copies as may be necessary to preserve the integrity of seized electronically stored information, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and outside technical experts under government control) are authorized to review the seized information for information and data within the scope of this warrant.

In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence, contraband, fruits and/or other items illegally possessed in violation of the Subject Offenses. Such techniques may include, but shall not be limited to, surveying various file directories or folders and the individual files they contain; conducting a file-by-file review by "opening" or 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 data; scanning storage areas for deliberately hidden files; and performing electronic "key word" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation. Forensically trained law enforcement personnel may also search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the data falls within the list of items to be seized as set forth in this affidavit. ESI that is responsive to the warrant will be identified and/or copied for further use in the investigation and any resultant prosecution.

AO 106 (Rev. 06/09) Application for a Search Warrant

# UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*

A Laptop Computer, Further Described Below and in Attachment A

Case No. 16 MAG 7063

## APPLICATION FOR A SEARCH 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)*:
A Laptop Computer, Further Described As a Silver Dell Inspiron 15 7000 Series (7548) Laptop Computer Bearing Service Tag [redacted] Containing a Toshiba One Terabyte Hard Drive Bearing Serial Number [redacted]

located in the Southern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

PLEASE SEE ATTACHED AFFIDAVIT AND ATTACHMENT A.

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

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

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. § 793(e) and (f) | Gathering, transmitting or losing defense information |

The application is based on these facts:

PLEASE SEE ATTACHED AFFIDAVIT AND ATTACHMENT A.

☑ Continued on the attached sheet.

☐ Delayed notice of ____ 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.

[redacted]
*Applicant's signature*

[redacted], Supervisory Special Agent, FBI
*Printed name and title*

Sworn to before me and signed in my presence.

Date: 10/30/2016

S/Kevin Nathaniel Fox
*Judge's signature*

City and state: New York, New York

Honorable Kevin Nathaniel Fox
*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 a Laptop Computer, Further Described As a Silver Dell Inspiron 15 7000 Series (7548) Laptop Computer Bearing Service Tag [redacted] Containing a Toshiba One Terabyte Hard Drive Bearing Serial Number [redacted] and That is Currently Housed at the Federal Bureau of Investigation, New York Field Office, 26 Federal Plaza, New York, New York 10278. | **TO BE FILED UNDER SEAL**<br><br>**Agent Affidavit in Support of Application for Search Warrant** |

SOUTHERN DISTRICT OF NEW YORK) ss.:

[redacted], being duly sworn, deposes and says:

INTRODUCTION AND AGENT BACKGROUND

1. [redacted]

2. This affidavit relates to a criminal investigation concerning the improper transmission and storage of classified information on unclassified email systems and servers. The investigation began as a result of a review of emails undertaken by the U.S. Department of State (State Department) in connection with Freedom of Information Act (FOIA) litigation.

During this FOIA review, it was determined that certain emails containing classified information were sent and received on systems unauthorized for the transmission or storage of such information. On or about July 6, 2015, the Inspector General for the Intelligence Community notified the FBI of a potential compromise of classified information involving the emails discovered through the FOIA review. After an initial review of the matter, the FBI opened a criminal investigation to, among other things, identify any unauthorized systems which the emails in question have transited, identify any person(s) who may have introduced classified information onto unauthorized systems and all circumstances surrounding such introduction, identify any person(s) who may have transmitted such information over any such systems, and identify whether classified information has been compromised through computer intrusions or unauthorized access into these systems.

3. The FBI's investigation has established that emails containing classified information were transmitted and stored on multiple forms of electronic media. One of the items identified as having contained such emails is a server which was used by former Secretary of State Hillary Rodham Clinton (Clinton) during her tenure at the State Department to transmit, receive, and store email for a personal email account or accounts she maintained (the Clinton Server). One domain on the Clinton Server was @clintonemail.com.

4. In recent months, the FBI and the Department of Justice have made public statements concerning the conclusion of the investigation. However, as with any case, if new, pertinent information comes to light after an investigation is completed, the FBI will take appropriate investigative steps to determine the significance of that information.

5. [redacted]

[redacted]

6. In executing the search of the laptop computer (the Subject Laptop) [redacted], FBI agents sorted the emails on the Subject Laptop to segregate emails [redacted]. As a result, the FBI reviewed non-content header information for emails on the Subject Laptop to facilitate its search. In so doing, the FBI observed non-content header information indicating that thousands of emails of [redacted] [redacted] resided on the Subject Laptop. Because [redacted] emails were outside of the scope [redacted] the FBI did not review the content of those emails.

7. [redacted] The non-content header information that FBI agents reviewed on the Subject Laptop indicates that the emails on the Subject Laptop include emails sent and/or received by [redacted] and at a [redacted] email account appearing to belong to [redacted] as well as correspondence between one or both of these accounts and State Department email accounts during and around [redacted] The FBI's investigation of the improper transmission and storage of classified information on unclassified email systems and servers has established that emails containing classified information were transmitted through multiple email accounts used by [redacted] including [redacted] and [redacted] email accounts.

8. The Subject Laptop, which is a silver Dell Inspiron 15 7000 Series (7548) laptop computer bearing service tag [redacted] containing a Toshiba one terabyte hard drive bearing

serial number [redacted] is currently housed at the Federal Bureau of Investigation, New York Field Office, 26 Federal Plaza, New York, New York 10278, within the Southern District of New York, as described in Attachment A to this affidavit. There is probable cause to believe that the Subject Laptop contains evidence, contraband, fruits, and/or other items illegally possessed in violation of 18 U.S.C. § 793(e) and (f).

9. 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 Subject Laptop for the items and information described in Attachment A. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation, and information from other FBI and U.S. Government personnel. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and part, except where otherwise indicated.

## STATUTORY AUTHORITY AND DEFINITIONS

10. For the reasons set forth below, I believe that there is probable cause to believe that the Subject Laptop contains evidence, contraband, fruits, and/or other items illegally possessed in violation of Title 18, United States Code, Section 793(e) and (f) (the Subject Offenses).

11. 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 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.

12. Under 18 U.S.C. § 793(f), "[w]hoever, being entrusted with or having lawful possession or control of any document . . . or information, relating to the national defense" either "(1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed," or "(2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer" shall be fined or imprisoned not more than ten years, or both.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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 (FED 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.

18. As used herein, the following terms have the following meaning:

a. "Computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1).

b. "Directory" or "folder" means a simulated electronic file folder or container used to organize files and directories in a hierarchical or tree-like structure.

c. "Electronically Stored Information" or "ESI" includes, consistent with Federal Rule of Criminal Procedure 41 and the Advisory Committee Comments to the 2009 amendments, writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained, including all types of computer-based information as may be developed over time. "Computer data" as used herein is synonymous with ESI.

d. "File" means a collection of related data or information stored as a unit under a specified name on storage medium. Not all ESI is stored in files.

PROBABLE CAUSE FOR SEARCH

19. At all times relevant to this affidavit, Clinton and [redacted] had security clearances, as described in paragraph 15 above.

20. As a result of a records request from the State Department, Clinton produced to the State Department approximately 30,490 email communications sent to or from Clinton at the @clintonemail.com domain that resided on Clinton's Server. As a result of a FOIA request, the

State Department ultimately reviewed these 30,490 emails. The FOIA process implemented by the State Department required that these emails be reviewed by government agencies for classified information prior to public release. In February 2016, the State Department completed its review and determined that 2,115 of the 30,490 emails contain information that is presently classified. Out of these 2,115 emails, the State Department determined that 2,028 emails contain information classified at the Confidential level; 65 contain information classified at the Secret level; and 22 contain information classified at the Top Secret level. The State Department did not make a determination as to whether the information in these emails was classified at the time that the emails were sent.

21. The U.S. Government's determination that 2,028 emails contain information classified at the Confidential level is significant because it means that the unauthorized disclosure of those emails could result in damage to national security. The U.S. Government's determination that 65 emails contain information classified at the Secret level is significant because it means that the unauthorized disclosure of those emails could result in serious damage to national security. The U.S. Government's determination that 22 emails contain information classified at the Top Secret level is significant because it means that the unauthorized disclosure of those emails could result in exceptionally grave damage to national security.

22. In conjunction with this investigation, the FBI sought a determination by the relevant original classification authorities as to whether certain of the 30,490 emails contained classified information at the time they were sent. In response to the FBI's requests for classification determinations, the relevant original classification authorities determined that 81

email chains,[1] which the FBI investigation determined were transmitted and stored on the Clinton Server, contained classified information ranging from the Confidential to Top Secret/Special Access Program levels at the time they were sent between 2009 and 2013. The relevant original classification authorities determined that information in 68 of these email chains remains classified.

23. [redacted]

24. The FBI's investigation determined that [redacted] using [redacted] various email accounts, typically communicated with Clinton's @clintonemail.com email account on a daily basis. Analysis of emails in the FBI's possession revealed more than 4,000 work-related emails

[1] For the purpose of the FBI investigation, an email chain is defined as a set of emails having the same initial email. The subject line may be edited in these chains to reflect the purpose of the forward or reply.

between [redacted] and Clinton from 2009 to 2013.

25. The FBI's investigation established that 27 email chains containing classified information, as determined by the relevant original classification authorities, have been transmitted through [redacted] and/or [redacted] accounts. Out of the 27 email chains, six email chains contained information that was classified at the Secret level at the time the emails were sent, and information in four of those email chains remains classified at that level now, while two email chains contain information that is currently classified at the Confidential level. Information in the remaining 21 email chains was classified at the Confidential level at the time the emails were sent, and of those 21 email chains, information in 16 of them remains classified as Confidential.

26. Given the information indicating that there are thousands of [redacted] emails located on the Subject Laptop – including emails, during and around [redacted] from [redacted] account as well as a [redacted] account appearing to belong to [redacted] – and the regular email correspondence between [redacted] and Clinton, there is probable cause to believe that the Subject Laptop contains correspondence between [redacted] and Clinton [redacted] Because it has been determined by relevant original classification authorities that many emails were exchanged between [redacted] using [redacted] and/or [redacted] accounts, and Clinton that contain classified information, there is also probable cause to believe that the correspondence between them located on the Subject Laptop contains classified information which was produced by and is owned by the U.S. Government. The Subject Laptop was never authorized for the storage or transmission of classified or national defense information.

27. A complete forensic analysis and review of the Subject Laptop will also allow the

FBI to determine if there is any evidence of computer intrusions into the Subject Laptop, and to determine if classified information was accessed by unauthorized users or transferred to any other unauthorized systems.

## PROCEDURES FOR SEARCHING ESI

### Review of ESI

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

29. In conducting this review, law enforcement may use various techniques to determine which files or other ESI contain evidence, contraband, fruits, and/or other items illegally possessed in violation of the Subject Offenses. Such techniques may include, for example:

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

subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

30. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant.

Return of the Subject Laptop

31. If the Government determines that the Subject Laptop is no longer necessary to retrieve and preserve the data on the device, and that the Subject Laptop is not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return the Subject Laptop. 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.

CONCLUSION

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

33. In light of the confidential nature of this investigation, the full scope of which is not known to [redacted] or the public, as well as the confidential nature of the underlying investigation in which the Subject Laptop was initially obtained by the Government, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.

[redacted]
Supervisory Special Agent
Federal Bureau of Investigation

Sworn to before me on
the 30th day of October, 2016.

S/Kevin Nathaniel Fox
HON. KEVIN NATHANIEL FOX
UNITED STATES MAGISTRATE JUDGE

**Attachment A**

## I. Device To Be Searched

The device to be searched is a silver Dell Inspiron 15 7000 Series (7548) laptop computer bearing service tag [redacted] containing a Toshiba one terabyte hard drive bearing serial number [redacted] (the Subject Laptop), and that is currently housed at the Federal Bureau of Investigation, New York Field Office, 26 Federal Plaza, New York, New York 10278.

## II. Review of ESI on the Subject Devices

Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the Subject Laptop for the following evidence, contraband, fruits, and/or other items illegally possessed in violation of Title 18, United States Code, Section 793(e) and (f) (the Subject Offenses):

1. Data and information associated with the operation, use, maintenance, backup, auditing, and security functions of the Subject Laptop including, but not limited to:
   a. Emails and attachments, in any form;
   b. User and system files stored on the laptops, including file fragments and items carved from unallocated space;
   c. Logs, configuration files, and backups;
   d. Executable code and scripts; and
   e. Documents, database files, and spreadsheets;

2. Data and information electronically stored on the Subject Laptop related to communications with email accounts used by former Secretary of State Hillary Clinton during her tenure as Secretary of State;

3. Data and information on the Subject Laptop that might identify the person or persons who accessed classified information present on the Subject Laptop, including names, addresses, telephone numbers and other identifiers, email addresses, business information, the length of service (including start date), types of services utilized, means and source of payment for services (including any credit card or bank account number), and information about any domain name registration; and

4. Data and information stored on the Subject Laptop that might identify activity related to a computer intrusion, including, but not limited to evidence of malware or viruses, executable code or scripts, log files, audit files, system files, user and account information, IP addresses, computer hardware addresses, intrusion-detection logs, firewall and other network logs, anti-virus logs or anti-malware logs.

## III. Seizure for Later Review of Electronically Stored Information

### A. Seizure of Computer and Media

This warrant authorizes the seizure of a computer and electronic storage media as set forth below. In lieu of seizing any particular electronic storage media, this warrant also authorizes the copying of electronically stored information for later review. Electronic storage media which may be seized or copied include without limitation:

Computer devices, electronic media and electronic storage devices, including, but not limited to, a computer, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners and the data within the aforesaid objects relating to said materials, which may contain information within the scope of this warrant.

Any physical keys, encryption devices, and similar physical items that are necessary to gain access to the computer equipment, storage devices or data mentioned above, or any passwords, password files, test keys, encryption codes or other information necessary to access the above-mentioned computer equipment, storage devices or data.

### B. Review of Electronic Storage Media and Electronically Stored Information

Following creation of forensic image copies as may be necessary to preserve the integrity of seized electronically stored information, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and outside technical experts under government control) are authorized to review the seized information for information and data within the scope of this warrant.

In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence, contraband, fruits and/or other items illegally possessed in violation of the Subject Offenses. Such techniques may include, but shall not be limited to, surveying various file directories or folders and the individual files they contain; conducting a file-by-file review by "opening" or 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 data; scanning storage areas for deliberately hidden files; and performing electronic "key word" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation. Forensically trained law enforcement personnel may also search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the data falls within the list of items to be seized as set forth in this affidavit. ESI that is responsive to the warrant will be identified and/or copied for further use in the investigation and any resultant prosecution.

AO 93 (Rev. 01/09) Search and Seizure Warrant (Page 2)

**Return**

| Case No.: | Date and time warrant executed: | Copy of warrant and inventory left with: |
|---|---|---|
| 16 MAG 7063 | 10/30/2016 1:57 pm | SSA [redacted] |

Inventory made in the presence of: SA[redacted]

Inventory of the property taken and name of any person(s) seized:

Forensic image of a silver Dell Inspiron 15 7000 Series (7548) laptop computer bearing service tag [redacted] containing a Toshiba one terabyte hard drive bearing serial number [redacted]

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the Court.

Date: 10/30/2016

[redacted]

*Executing officer's signature*

SSA [redacted], FBI

*Printed name and title*