

UNITED STATES DISTRICT COURT
for the
District of Massachusetts

United States of America
v.
Jack Douglas Teixeira

Case No.
23-4293-DHH

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of February 28, 2023 in the county of Bristol in the
District of Massachusetts, the defendant(s) violated:

Table with 2 columns: Code Section, Offense Description. Rows include 18 U.S.C. § 793(b) and (d), 18 U.S.C. § 1924, and descriptions of unauthorized retention and transmission of national defense information.

This criminal complaint is based on these facts:

See Affidavit of FBI Special Agent Patrick Lueckenhoff, attached hereto and incorporated herein.

Continued on the attached sheet.

Signature of Patrick Lueckenhoff
Complainant's signature
Special Agent Patrick Lueckenhoff, FBI
Printed name and title

Subscribed and sworn to via telephone in accordance
with Federal Rule of Criminal Procedure 4.1

Date: 04/14/2023

City and state: Boston, Massachusetts

Signature of David H. Hennessey
Hon. David H. Hennessey, Magistrate Judge
Printed name and title
Seal of the United States District Court for the District of Massachusetts

**AFFIDAVIT IN SUPPORT OF AN APPLICATION
FOR A CRIMINAL COMPLAINT AND ARREST WARRANT**

I, Patrick M. Lueckenhoff, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation and have been since 2018. During this time, I have received training at the FBI Academy located in Quantico, Virginia, to include training on investigative methods and training specific to counterintelligence and espionage investigations. I am currently assigned to a squad at the FBI Washington Field Office, Counterintelligence Division, where I primarily investigate counterintelligence and espionage matters. During the course of these investigations, I have conducted or participated in witness and subject interviews, service of subpoenas, the execution of search and arrest warrants, physical surveillance, the seizure of evidence, including computer, electronic, and email evidence, as well as requested and reviewed pertinent records. Based on my experience and training, I am familiar with the requirements for the handling of classified documents and information. I am also familiar with the methods used by individuals engaged in the unlawful use or disclosure of classified information, including national defense information.

2. Your affiant is currently investigating the activities of JACK DOUGLAS TEIXEIRA (“TEIXEIRA”), whom your affiant believes willfully retained and transmitted classified national defense information to a person not entitled to receive it in violation of 18 U.S.C. § 793(b) and (d) and 18 U.S.C. § 1924 (the “SUBJECT OFFENSES”). These acts occurred within the District of Massachusetts and elsewhere. Your affiant submits this Criminal Complaint in support of the arrest of TEIXEIRA.

3. The facts in this affidavit come from your affiant’s personal observations, training, and experience, and information obtained from other U.S. Government officers, agents,

and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for TEIXEIRA's arrest and does not set forth all of your affiant's knowledge about this matter.

STATUTORY AUTHORITY AND DEFINITIONS

4. For the reasons set forth below, I submit that there is probable cause to believe that TEIXEIRA committed a violation of Title 18, United States Code, Sections 793(b) and (d) and Title 18, United States Code, Section 1924.

5. Pursuant to 18 U.S.C. § 793(b), “[w]hoever . . . copies, takes, makes, or obtains, or attempts to copy, take, make or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense” shall be fined or imprisoned not more than ten years, or both.

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

7. Pursuant to 18 U.S.C. § 1924, it is illegal for any officer, employee, contractor, or consultant of the United States, who, by virtue of his/her office, employment, position, or contract, becomes possessed of documents or materials containing classified information, to

knowingly remove such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location.

8. Under Executive Order 13526, the unauthorized disclosure of material classified at the “TOP SECRET” level (“TS”), by definition, “reasonably could be expected to cause exceptionally grave damage to the national security” of the United States. Exec. Order 13526 § 1.2(a)(1), 75 Fed. Reg. 707, 707–08 (Jan. 5, 2010). The unauthorized disclosure of information classified at the “SECRET” level (“S”), by definition, “reasonably could be expected to cause serious damage to the national security” of the United States. Exec. Order 13526 § 1.2(a)(2). The unauthorized disclosure of information classified at the “CONFIDENTIAL” level (“C”), by definition, “reasonably could be expected to cause damage to the national security” of the United States. Exec. Order 13526 § 1.2(a)(3).

9. Sensitive Compartmented Information (“SCI”) means classified information concerning or derived from intelligence sources, methods, or analytical processes, which is further restricted, with the requirement that it be handled within formal access control systems established by the Director of National Intelligence.

10. 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.

11. 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.

12. 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

13. As described more fully below, there is probable cause to believe that TEIXEIRA improperly and unlawfully retained and transmitted national defense information classified at the TS//SCI level to persons not authorized to receive such information.

14. The FBI has been investigating the unauthorized disclosure of classified national defense information in connection with the posting of dozens of images of documents on various public Internet sites. Many of the documents depicted in these images bear classification markings, including “TOP SECRET” markings, which would serve to indicate the presence of U.S. Government classified information, including national defense information (the

“Government Information”). Many of these images were posted on a publicly accessible U.S. social media platform (“Social Media Platform 1”¹). Certain of the images appear to depict Government Information that was used to inform senior military and civilian government officials during briefings at the Pentagon in Arlington, Virginia.

15. On or about April 10, 2023, the FBI interviewed a user of Social Media Platform 1 (“User 1”). According to User 1, an individual using a particular username (the “Subject Username”) began posting what appeared to be classified information on Social Media Platform 1 in or about December 2022 on a specific server (“Server 1”) within Social Media Platform 1. According to User 1, the individual using the Subject Username was the administrator of Server 1. User 1 indicated that the purpose of Server 1 was to discuss geopolitical affairs and current and historical wars.

16. According to User 1, the individual using the Subject Username initially posted the Government Information as paragraphs of text. However, in or around January 2023, the Subject Username began posting photographs of documents on Server 1 that contained what appeared to be classification markings on official U.S. Government documents.

17. According to User 1, one of the documents that was posted on Server 1 by the individual using the Subject Username was a document that described the status of the Russia-Ukraine conflict, including troop movements, on a particular date (the “Government Document”). The Government Document is based on sensitive U.S. intelligence, gathered through classified sources and methods, and contains national defense information. An Original Classification Authority has confirmed that the Government Document is classified at the

¹ Social Media Platform 1 is a VOIP and instant messaging social platform. Users of Social Media Platform 1 have the ability to communicate with voice calls, video calls, text messaging, and can post media and files in private chats or as part of communities called “servers.” A Social Media Platform 1 server is a collection of persistent chat room and voice channels, some of which can only be accessed via invitation from a current chat room member.

TS//SCI level. As described above, the unauthorized disclosure of TOP SECRET information “reasonably could be expected to cause exceptionally grave damage to the national security” of the United States. Exec. Order 13526 § 1.2(a)(1), 75 Fed. Reg. 707, 707–08 (Jan. 5, 2010).

18. User 1 told the FBI that he spoke to the individual using the Subject Username at various times using a video chat application, voice calls, or the chat function on Server 1. According to User 1, during one of those conversations, the individual using the Subject Username explained that he had become concerned that he may be discovered making the transcriptions of text in the workplace, so he began taking the documents to his residence and photographing them.

19. User 1 also described to the FBI his interactions with the individual posting under the Subject Username. In the course of those interactions, User 1 learned that the individual posting under the Subject Username called himself “Jack,” appeared to reside in Massachusetts, and claimed that he was in the United States Air National Guard (“USANG”). User 1 described the individual posting under the Subject Username as a white male who was clean-cut in appearance and between 20 and 30 years old.

20. On or about April 12, 2023, Social Media Platform 1 provided the FBI with records pursuant to legal process. These records included information related to User 1’s Social Media Platform 1 Account and the subscriber information for the administrator of Server 1 to which User 1 belonged.

21. According to these records, the individual using the Subject Username is the administrator of Server 1, the billing name associated with the Subject Username is “Jack Teixeira,” and the billing address associated with the Subject Username is a specific residence in North Dighton, Massachusetts. Teixeira listed the North Dighton, Massachusetts residence as

his primary residence on employment paperwork with the USANG. On April 13, 2023 the FBI arrested TEIXEIRA at that residence in North Dighton, Massachusetts.

22. On April 13, 2023, User 1 also identified TEIXEIRA's Registry of Motor Vehicles photo from a photo lineup as the individual he knew as "Jack" who had posted Government Information under the Subject Username on Social Media Platform 1.

23. According to a review of government records and information, since May 2022, TEIXEIRA has been serving as an E-3/Airman First Class in the USANG and has been stationed at Otis Air National Guard Base in Massachusetts. TEIXEIRA enlisted in the USANG in September 2019 as an E-1 rank. As of February 2023, TEIXEIRA's title was Cyber Defense Operations Journeyman.

24. As required for this position, TEIXEIRA holds a Top Secret security clearance, which was granted in 2021. Based on my training and experience, I know that to acquire his security clearance, TEIXEIRA would have signed a lifetime binding non-disclosure agreement in which he would have had to acknowledge that the unauthorized disclosure of protected information could result in criminal charges.

25. In addition to TEIXEIRA's Top Secret clearance, he maintained sensitive compartmented access (SCI) to other highly classified programs. He has also had this access since 2021.

26. The Government Document posted on Social Media Platform 1 was accessible to TEIXEIRA by virtue of his employment with USANG. According to a U.S. Government Agency, which has access to logs of certain documents TEIXEIRA accessed, TEIXEIRA accessed the Government Document in February 2023, approximately one day before User 1

reposted the information on the Internet. User 1 told the FBI that the information he reposted was originally posted on Server 1 by the individual using the Subject Username.

27. In addition, according to a second U.S. Government Agency, which can monitor certain searches conducted on its classified networks, on April 6, 2023, TEIXEIRA used his government computer to search classified intelligence reporting for the word “leak.” The first public reporting regarding the Government Information appeared on or around April 6, 2023. Accordingly, there is reason to believe that TEIXEIRA was searching for classified reporting regarding the U.S. Intelligence Community’s assessment of the identity of the individual who transmitted classified national defense information, to include the Government Document.

CONCLUSION

28. Your affiant submits that the facts set forth in this affidavit establish probable cause to believe TEIXEIRA committed a violation of 18 U.S.C. Sections 793(b) and (d), and 18 U.S.C. Section 1924. Therefore, your affiant respectfully requests this Court issue an arrest warrant for TEIXEIRA.

Sworn to under the pains and penalties of perjury,

Patrick M Lueckenhoff

Patrick M. Lueckenhoff
Special Agent, Federal Bureau of Investigation

~~Subscribed and~~ sworn to before me via telephone on April 14, 2023. 9:49 a.m.

David H. Henneberry

Hon. David H. Henneberry
United States Magistrate Judge

