AO 91 (Rev. 11/11) Criminal Complaint

FILED
OCT 08 2021
U.S. DISTRICT COURT-WVND
MARTINSBURG, WV 25401

UNITED STATES DISTRICT COURT

for the

Northern District of West Virginia

United States of America
v.

Jonathan Toebbe and Diana Toebbe

Defendant(s)

Case No. 3:21 MJ 138

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 04/01/2020 - 10/09/2021 in the county of Jefferson County in the Northern District of West Virginia, the defendant(s) violated:

Code Section	*Offense Description*
42 USC § 2274(a)	Conspiracy to Communicate Restricted Data
42 USC § 2274(a)	Communication of Restricted Data

This criminal complaint is based on these facts:

See attached Affidavit (incorporated by reference).

☑ Continued on the attached sheet.

Complainant's signature

Justin Van Tromp, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/08/2021

Judge's signature

City and state: Martinsburg, WV

Robert W. Trumble, United States Magistrate Judge

Printed name and title

FILED
OCT 08 2021
U.S. DISTRICT COURT-WVND
MARTINSBURG, WV 25401

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF WEST VIRGINIA

Martinsburg Division

UNITED STATES OF AMERICA

v.

JONATHAN TOEBBE and
DIANA TOEBBE,

Defendants.

Case No. 3:21MJ138

AFFIDAVIT IN SUPPORT OF
CRIMINAL COMPLAINT

I, Justin Van Tromp, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of a Criminal Complaint alleging that the defendants, **JONATHAN TOEBBE** and **DIANA TOEBBE**, have violated 42 U.S.C. § 2274(a).

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") assigned to the FBI Pittsburgh Field Office. I have been a Special Agent with the FBI since May 2018. I completed Special Agent training at the FBI training center in Quantico, Virginia, in September 2018, which includes curriculum on conducting counterintelligence and counterproliferation investigations. Upon graduation from the FBI academy, I have been assigned to work counterintelligence investigations and have been working multiple cases involving economic espionage. Prior to joining the FBI, I was employed by the United States Secret Service as a Special Agent for 11 years. As a U.S. Secret Service agent, I worked financial crimes investigations and served on the Presidential Protective Division. During that time, I also worked on the Joint Terrorism Task Force at the FBI's Washington Field Office and conducted complex counterterrorism investigations. Prior to that, I was employed as a Special Agent with the Air

Force Office of Special Investigations, working counterintelligence and general criminal investigations.

3. The facts in this affidavit come from my personal investigation and observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for this Criminal Complaint and the requested arrest warrants and does not set forth all of my knowledge about this matter. I have set forth only the facts I believe are necessary to establish probable cause that the defendants have violated 42 U.S.C. § 2274(a).

RELEVANT STATUTES, REGULATIONS, AND AUTHORITIES

4. The Atomic Energy Act (the "Act") prohibits, *inter alia*, individuals who have possession of, access to, control over, or are entrusted with any document, writing, sketch, photograph, plan, model, instrument, appliance, note, or information involving or incorporating Restricted Data from communicating, transmitting, or disclosing it to any individual or person, or attempting or conspiring to do so, with the intent to injure the United States or to secure an advantage to any foreign nation. 42 U.S.C. § 2274(a). "Restricted Data" consists of "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy," but does not include data that has been declassified or removed from the Restricted Data category. 42 U.S.C. §2014(y).

PROBABLE CAUSE

5. As detailed below, the FBI's investigation has revealed that **JONATHAN TOEBBE**, a current employee of the United States Navy, has passed, and continues to attempt to pass, Restricted Data as defined by the Atomic Energy Act, specifically 42 U.S.C. § 2014(y), to a

foreign government, hereinafter "COUNTRY1," with the witting assistance of his spouse, **DIANA TOEBBE**.

The FBI Retrieves Package Containing U.S. Navy Documents from LEGAT in COUNTRY1

6. On or about December 20, 2020, the FBI's attaché ("LEGAT") in COUNTRY1 obtained a package representatives from COUNTRY1 had received in April 2020 through a mail carrier from the U.S. by an unidentified subject in an attempt to establish a covert relationship. The package contained U.S. Navy documents, a letter containing instructions, and an SD card containing specific instructions on how COUNTRY1 should respond using an encrypted communication platform, and additional documents.

7. In the letter, the sender stated a desire to sell documents containing U.S. Navy information marked CONFIDENTIAL that included printouts, digital media files containing technical details, operations manuals, and performance reports. The letter requested the transmission of the enclosed technical data to COUNTRY1's military intelligence agency. The sender wrote: *"I apologize for this poor translation into your language. Please forward this letter to your military intelligence agency. I believe this information will be of great value to your nation. This is not a hoax."*

8. The package that contained the material described above was a brown envelope with four U.S. postage stamps, a postal barcode, and a sent date of April 1, 2020. The return address was identified as a location in Pittsburgh, Pennsylvania.

9. A subject-matter expert at the U.S. Navy with knowledge of the documents included in the package sent to COUNTRY1 informed the FBI that these documents were U.S. Government documents that contained Restricted Data.

10. On December 23, 2020, the FBI analyzed the encryption keys that were in the SD card sent in the original envelope. There were three keys located on the SD card: Alice Hill – Public Key, Bob Burns – Private Key, and a ProtonMail Public Key. In cryptography, Alice and Bob are commonly used as placeholders in discussions about cryptographic protocols or systems. The FBI noted that the public key Alice Hill had two sub-keys. The first sub-key was used to sign and certify.

11. The private key Bob Burns had two sub-keys. The first sub-key was used to sign and certify. The second sub-key was used for encryption. The ProtonMail public key had two sub-keys.

12. ProtonMail is an end-to-end encrypted email service founded in 2013 in Geneva, Switzerland. ProtonMail uses client-side encryption to protect email content and user data before they are sent to the ProtonMail servers. The service can be accessed through a webmail client, the onion router (also known as the Tor) network, or dedicated iOS or Android apps. The service is run by Proton Technologies AG. The company also operates ProtonVPN, a VPN service. In my training and experience, individuals who engage in activities that they wish to keep hidden or secret, or when they wish to keep their location hidden or secret, use an encrypted email service like ProtonMail.

13. In addition, the FBI determined that the SD card contained metadata showing that the card had been connected to a computer with a Macintosh operating system.

The FBI Begins Undercover Communication with "ALICE"

14. On December 26, 2020, the FBI initiated the first of several emails to "ALICE" on ProtonMail. The FBI utilized a ProtonMail account utilizing the pseudo name "BOB." The email stated, "*We received your letter. We want to work with you. It has been many months, so we need*

to know if you are still out there. Please respond to this message, then we will provide instruction how to proceed."

15. On February 10, 2021, "ALICE" responded and stated, *"Thank you for contacting me. I am still here. The covid disease has made it more difficult to find chances to check this email. Let us discuss how to proceed."*

16. On February 24, 2021, an FBI agent acting in an undercover capacity ("the UC") responded and stated, *"We understand the delay and hope you are well. Our experts reviewed the information you provided. We would like as sample your [U.S. Navy Information – Specific Sections].*[1] *We have a trusted friend in your country who has a gift for you to compensate for your efforts . . . ."*

17. On March 5, 2021, "ALICE" replied with the following. *"I am uncomfortable with this arrangement. Face to face meetings are very risky for me, as I am sure you understand. I propose exchanging gifts electronically, for mutual safety. I can upload documents to a secure cloud storage account, encrypted with the key I have provided you. You can send me a suitable gift in Monero cryptocurrency to an address I will provide. 100,000 usd should be enough to prove to me that you are not an unwelcome third party looking to make trouble for me. When I have confirmed receipt of your gift, I will provide you the download link. We are both protected. I understand this is a large request. However, please remember I am risking my life for your benefit and I have taken the first step. Please help me trust you fully."*

---

[1] The specific wording here contains non-public Restricted Data.

18. According to public sources, Monero is a decentralized cryptocurrency that uses a publicly distributed ledger with privacy-enhancing technologies that obfuscate transactions to achieve anonymity and fungibility.

19. On March 18, 2021, the UC posing as a representative of COUNTRY1 wrote, *"We understand a face to face meeting would be uncomfortable. We suggest a neutral drop location. When you visit the location alone, you retrieve a gift and leave behind the sample we request . . . . We hope to have a very long friendship that benefits mutually."*

20. On March 22, 2021, "ALICE" replied. *"I understand your proposal to start a dead drop. I am concerned that using a dead drop location your friend prepares makes me very vulnerable. If other interested parties are observing the location, I will be unable to detect them. I am not a professional, and do not have a team supporting me. I am also concerned that a physical gift would be very difficult to explain if I am questioned. For now, I must consider the possibility that you are not the person I hope you are. It would be very easy for the serial numbers of bills to be recorded. Tracking devices and other nasty surprises must be considered as well. I propose to modify your plan in the following ways:*

> *1. I will place the sample you requested on a memory card and place it in a drop location of my choosing....I am not a professional, and I am sure that publicly available information on this subject is incomplete.*
>
> *2. The samples will be encrypted using GnuPG symmetric encryption with a randomly generated passphrase.*
>
> *3. I will tell you the location and how to find the card. I will also give you a Monero address. This form of gift protects both of us very well. I am very aware of the*

risks of blockchain analysis of BitCoin and other cryptocurrencies, and believe Monero gives both us excellent deniability.

4. Once I confirm receipt of my gift, I will give you the passphrase.

Your friend and I will never go to the same drop location twice. I will give you a new Monero address each time. The decryption key will be different each time. No patterns for third parties to observe. The only electronic footprints will be Proton to Proton, so there is less risk of encrypted traffic being collected for future analysis by third parties. That part is not perfect. Perhaps as our friendship develops we will change addresses periodically?"

21. On April 1, 2021, the UC posing as a representative of COUNTRY1 responded to "ALICE" and stated, *"We understand your concern and appreciate the thoughtful plan...as a sign of good faith and trust we wish to pay you equivalent of 10,000 USD immediately on Monero to address you provide. Drop locations are safest and allow us to make exchanges without coming in contact and of course leave no electronic footprint...Your proposed method of memory card with encryption/passphrases is acceptable. For the small sample we requested you will receive another 20,000 USD. Once you confirm Monero address we will activate payment. Our next step will be information on drop location we have selected. This method will build trust between us for a larger transaction in future. Our experts are interested in information you have but we insist on maintaining our discretion and security as a priority."*

The FBI Conducts a Signal Operation in the Washington, D.C. Area over Memorial Day Weekend

22. On April 9, 2021, "ALICE" wrote, *"I am sorry to be so stubborn and untrusting, but I can not agree to go to a location of your choosing. I must consider the possibility that I am*

communicating with an adversary who has intercepted my first message and is attempting to expose me. Would not such an adversary wish me to go to a place of his choosing, knowing that an amateur will be unlikely to detect his surveillance? If you insist on my physically delivering the package, then it must be a place of my choosing. I ask you to consider the viability of an electronic dead drop. I can establish an encrypted online storage account without providing any identifying information and without provoking any suspicion...Another possibility occurs to me: is there some physical signal you can make that proves your identity to me? I could plan to visit Washington D.C. over the Memorial Day weekend. I would just be another tourist in the crowd. Perhaps you could fly a signal flag on your roof? Something easily observable from the street, but nothing to arouse an adversaries suspicion?...".

23. On April 23, 2021, the UC posing as a representative of COUNTRY1 emailed the following: *"You do not need to apologize. We appreciate you being careful. That is much better than someone reckless. Your thoughtful plans indicate you are not amateur. This relationship requires mutual comfort. There is risk on both sides and we understand your need for safety assurance of who you are communicating with. As you suggest we can accommodate a signal in Washington D.C. over the Memorial Day weekend. We will set a signal from our main building observable from the street. It will bring you comfort with signal on display from area inside our property that we control and not a [sic] adversary. If you agree please acknowledge. We will then provide more instruction about the signal. We hope this plan will continue to build necessary trust and comfort of our identity."*

24. On May 5, 2021 "ALICE" wrote, *"I will make plans to be in the capitol [sic] over the Memorial Day weekend. It would be best to leave the signal visible for the entire holiday*

weekend so I can plan to pass by in the natural course of my tourist day. I may be on foot, or passing by in a bus or car or bicycle, so please plan for something easy to spot.

25. On May 17, 2021, the UC posing as a representative of COUNTRY1responded and said, in part, *"We are happy to set a signal to bring you comfort and build necessary trust between us. The signal will be inside our main building from Saturday morning until Sunday evening Memorial Day weekend."*

26. During the weekend of May 29-30, 2021, the FBI conducted an operation in the Washington, D.C. area that involved placing a signal at a location associated with COUNTRY1 in an attempted effort to gain bona fides with "ALICE."

27. On May 31, 2021, the FBI received confirmation via the ProtonMail from "ALICE" that the signal was received. "ALICE" also wrote that, *"Now I am comfortable telling you your assumption that Pittsburgh would be a convenient location for me is incorrect...for now I can tell you I am located near Baltimore, Maryland. Please let me know when you are ready to proceed with our first exchange. Once you have drop location details for me, I will give you the Monero address and prepare the sample you have requested."* "ALICE" went on to request clarity of the U.S. Navy information requested by the UC posing as a representative of COUNTRY1.

The FBI Pays ALICE $10,000 USD as Sign of Good Faith and Trust

28. On June 4, 2021, the UC posing as a representative of COUNTRY1 requested the Monero address to provide "ALICE" a payment of $10,000 USD as a sign of good faith and trust. The UC also informed "ALICE" that new communication instructions would be provided at the exchange location.

29. On June 8, 2021, "ALICE" wrote that, *"For maximum security it is very important that you do not send Monero to the same address twice."* "ALICE" then provided the FBI with a

payment address. "ALICE" then went on to state, *"I will place information you have requested, encrypted, on a memory card along with the address for the second payment you offered in a plain text file. After I confirm the second payment, I will provide you with the decryption passphrase using the new communication method. I am also excited to continue our relationship . . . ."*

30. On June 10, 2021, the FBI paid "ALICE" approximately $10,000 USD in Monero cryptocurrency.

31. On June 17, 2021, "ALICE" thanked the FBI for the first payment and stated that he/she was, *"eagerly waiting for your instructions."*

The FBI Conducts Dead Drop Operation in Jefferson County, West Virginia

32. On June 18, 2021, the UC posing as a representative of COUNTRY1 emailed "ALICE" to provide detailed instructions on servicing a dead drop location in Jefferson County, West Virginia to occur on June 26, 2021. The UC discussed instructions regarding the next payment to "ALICE" as well as additional assurance that "ALICE" would be paid $20,000 upon the sample verification and authenticity of the information provided at the drop location.

33. On June 23, 2021, "ALICE" sent the FBI a confirmation email stating, *"I understand your instructions and am ready to move forward."*

34. On June 26, 2021, at approximately 10:41 a.m., the FBI observed **JONATHAN TOEBBE** physically service a dead drop location in Jefferson County, West Virginia. Records show that **JONATHAN TOEBBE** is a government employee working as a nuclear engineer for the United States Navy and holds an active Top Secret Security Clearance through the United States Department of Defense and an active Q clearance from the United States Department of Energy.

35. On the same date and time, the FBI also observed **JONATHAN TOEBBE**'s spouse, **DIANA TOEBBE**, standing approximately one meter away from **JONATHAN TOEBBE** during the servicing of the dead drop location. Based on my experience and training, it appeared that **DIANA TOEBBE** assisted **JONATHAN TOEBBE** during the dead drop operation. **DIANA TOEBBE** appeared to act as a lookout for **JONATHAN TOEBBE** during the drop and survey the surrounding area. Thereafter, **DIANA TOEBBE** signaled to **JONATHAN TOEBBE** to proceed on a trail after **JONATHAN TOEBBE** completed the drop. Records show that **DIANA TOEBBE** is a faculty member and humanities teacher in Annapolis, Maryland. Both **JONATHAN TOEBBE** and **DIANA TOEBBE** reside in Annapolis, Maryland.

36. Following the servicing of the dead drop location, both **JONATHAN TOEBBE** and **DIANA TOEBBE** were observed walking through a more populated area near the location of the dead drop. From my experience and training, it appeared that both **JONATHAN TOEBBE** and **DIANA TOEBBE** were conducting surveillance detection routes, meaning that they were moving in a way to attempt to detect whether they were being surveilled or followed.

37. In total, the FBI observed **JONATHAN TOEBBE** and/or **DIANA TOEBBE** arrive in the location of the dead drop at approximately 9:44 a.m. and depart the location at approximately 11:22 a.m. During this approximate time frame, the FBI observed a vehicle registered to **JONATHAN TOEBBE** parked in a visitor's lot.

38. Later on the same date, June 26, 2021, the FBI recovered a blue 16GB SanDisk SD Card left by **JONATHAN TOEBBE** at the dead drop location. The SD card was wrapped in plastic and placed between two slices of bread on a half of a peanut butter sandwich. The half sandwich was housed inside of a plastic bag.

39. On June 28, 2021, "ALICE" sent a ProtonMail message, providing the Monero address for payment. On the same date, the FBI electronically paid "ALICE" approximately $20,000 USD in Monero.

40. On June 29, 2021, "ALICE" provided the password to the FBI in an encrypted ProtonMail message. The FBI subsequently opened the provided SD card and provided the contents to the U.S. Navy subject matter expert. The U.S. Navy determined that multiple documents on the SD card contained Restricted Data. Specifically, the U.S. Navy subject matter expert determined that several of the documents contained militarily sensitive design elements, operating parameters, and performance characteristics of Virginia-class submarine reactors.

41. The SD card contained the following typed message from "ALICE":

I hope your experts are very happy with the sample provided and I understand the importance of a small exchange to grow our trust. Most of the material I possess is similar in format – multiple pages per sheet. Drafted drawings are split over several regular sheets to preserve good detail. And I used color where it seemed important – like graphs with several lines.

I expect your new communication instructions will be just as clear and safe as your drop instructions. However, I suggest you continue to monitor your Proton until I am able to establish contact with your new method. If there is a problem, I will use it to request help. All of my previous emails have been signed:

Yours truly,

Alice

If it is ever necessary to Proton you again, I will end the email with

Sincerely,

Alice

instead to assure you the message is from me and that I am not under duress.

For now, I propose we continue with weekend exchanges at suitable parks and trails, similar to this one. Details of my daily routine may narrow an investigator's

search too much if your organization is infiltrated by an adversary one day. Hiking and visiting historical sites is easier to explain than unexpected stops during rush hour if they ever take a special interest in me.

If we are to continue using this method of exchange long term, it is very important that I have as much flexibility in timing my deliveries as possible. I would like to create a natural legend for my interest in visiting a particular place in the future – reading articles about ten fun things to do in Baltimore this month and "stumbling" across a beautiful hike close to home, for example. Bad weather on one day might ruin that cover story.

I hope you will forgive my excess caution. I want our relationship to be very successful for us both, and that means that I must be very careful at every step.

Yours truly,

Alice

42. In addition, FBI analysis of the SD card showed that it contained metadata indicating that the card had been connected to a computer with the same version of Macintosh operating system as the SD card contained in the package postmarked April 1, 2020, and described in Paragraph 13 above.

Investigation Reveals JONATHAN TOEBBE is a U.S. Navy Technical Expert on the Information Passed in the April 2020 Package and at the June 2021 Dead Drop with a Prior Working History at a U.S. Navy Facility Located Near Pittsburgh

43. As indicated above, the FBI determined that **JONATHAN TOEBBE** performed the June 26, 2021 dead drop described above. **JONATHAN TOEBBE** has worked for the U.S. government since 2012.

44. From October 2012 to the present, **JONATHAN TOEBBE** has worked on matters of naval nuclear propulsion. **JONATHAN TOEBBE** has been assigned to the Reactor Engineering Division of the U.S. Navy, which is responsible for new and operating reactor plant noise and vibration technology and for assisting with reactor plant shock technology and design, manufacturing, and testing. **JONATHAN TOEBBE** has also been assigned to Bettis Atomic

Power Laboratory, a U.S. Government-owned research and development facility in the Pittsburgh suburb of West Mifflin, Pennsylvania that works exclusively on the design and development of nuclear power for the U.S. Navy. During one or both of these assignments, **JONATHAN TOEBBE** had access to the U.S. Navy information passed in both the physical letter to COUNTRY1 as well as the electronic U.S. Navy information passed in the dead drops on June 26, 2021, and August 28, 2021, which is described below in paragraphs 52-64.

45. On September 28, 2017, **JONATHAN TOEBBE** was released/discharged from Active Duty and maintained a reserve obligation termination date of July 23, 2020. The reason listed for his separation was that **JONATHAN TOEBBE** completed his required active service.

46. On March 25, 2020, **JONATHAN TOEBBE**'s TS clearance was renewed. This renewal was just days before the April 1, 2020 postmark date on the package sent to COUNTRY1.

The FBI Conducts a Dead Drop Operation in South-Central Pennsylvania

47. Concurrent with its investigation into **JONATHAN TOEBBE** and **DIANA TOEBBE**, the FBI planned the next dead drop operation for south-central Pennsylvania.

48. On July 31, 2021, the FBI observed **JONATHAN TOEBBE** and **DIANA TOEBBE** travel from their Annapolis residence to south-central Pennsylvania, where **JONATHAN TOEBBE** was observed servicing a dead drop. While **JONATHAN TOEBBE** serviced the dead drop, **DIANA TOEBBE** was nearby. When **JONATHAN TOEBBE** finished servicing the dead drop, he signaled for **DIANA TOEBBE** to follow him as he departed the location. Within seconds, the FBI observed **DIANA TOEBBE** following **JONATHAN TOEBBE** as he departed the location of the dead drop. The FBI observed that **JONATHAN TOEBBE** and **DIANA TOEBBE** arrived and departed the area in the same vehicle used to travel to and from the dead drop location on June 26, 2021.

49. Later on the same date, July 31, 2021, the FBI recovered a 32GB SD card left by **JONATHAN TOEBBE** at the dead drop location. The SD card was hidden in a sealed Band-Aid wrapper with a Band-Aid inside a clear Zip Lock bag. The FBI had observed **JONATHAN TOEBBE** remove the Ziploc bag from his left shorts pocket, place the bag in an FBI-designed container, and remove a written message the FBI had placed in the container for him.

50. The SD card contained the following typed message from "ALICE." The word [REDACTED] appears where the original message contained classified information or Restricted Data.

> *You can not imaging [sic] my relief at finding your letter just where you told me to look! Indeed, this has been a long journey and I am very happy to have a reliable professional partner in you. I am sure my unconventional approach was worrying your superiors. Thank you for taking the risks you have to build the mutual trust we need to move forward.*
>
> *I appreciate your compliment of my efforts to secure our communication. It was very challenging for an amateur to quietly gather information on how to reach you. Now that we have established a more secure method to write, please tell me if I make a mistake or if you have advice on how to accomplish a task so that I can improve my skills and reduce our shared risk. For example, thank you for the reminder to use cash only. I have been doing so at every step, and do not feel insulted at all. Since my self education is sure to have gaps, it is likely I will not know all things that are simple and obvious to you.*
>
> *You have anticipated my need for flexibility in timing deliveries perfectly. Use of the new Proton with the code method in your letter is a good solution. My new Proton is actually an old one I established quietly with a cash only burner phone while on vacation several years ago. My original contact plan was to give the login details to you, but I abandoned it as needlessly complicated. So it has been unused ever since for any purpose except to sign up for a few innocent, randomly chosen mailing lists to generate regular uninteresting traffic. I will continue to use public WiFi and the TOR .onion connection to Proton to prevent an adversary from watching TOR entrance/exit nodes.*
>
> *In your letter you requested I send two Protons: one with the Monero address and one with the decryption key. On the last SD card, I included the Monero address in the unencrypted file 1.txt. My idea was: your payment for the right amount to the right address tells me you successfully retrieved the card, and my sending the*

key tells you I have received your letter and payment and am ready to take the next step. The only small advantage to my plan is you do not need to wait for my Proton with address. Is there a reason it is safer to send address separate from encrypted data? I will follow the plan in your letter unless you think it is better to change.

As I said in my last letter, I hope your experts are very happy with the sample provided. In total, I possess the following documents:

1. *[REDACTED] 374 pages (4 pages per sheet, as with sample). Note the table of contents indicates there are additional sections [REDACTED]. They were not included in files I had normal access to since they relate mostly to the reactor heavy equipment and there was no plausible reason for me to request them in my job. As this document is only a high level summary of the [REDACTED] design, the missing sections are of little importance.*

2. *[REDACTED] 1032 sheets. Every page of every drawing listed in section [REDACTED] is there. To preserve good detail, I scaled the drawings to fit one large drawing page over several normal sheets. All [REDACTED] are present.*

3. *[REDACTED] 7919 pages (4 pages per sheet). The [REDACTED] reports the detailed results of all [REDACTED] done to predict the behavior of the [REDACTED] during normal [REDACTED]. The [REDACTED] also documents the design basis assumptions used to carry out these analyses. Your technical experts should be able to use this information and the [REDACTED] to verify the results using their own [REDACTED] codes.*

4. *[REDACTED] 1940 sheets – a mix of schematics and drawings (spread over multiple sheets for legibility), operating procedure (2 pages per sheet), and descriptive chapters (4 pages per sheet). The [REDACTED] is the [REDACTED] provided to U.S. Navy crews. How to operate [REDACTED]. How to [REDACTED]. Troubleshooting problems. Routine Maintenance. Your naval experts will be able to adapt these procedures to fit your own operations. Operating a [REDACTED] has many unique aspects, and the [REDACTED] reflects decades of U.S. Navy "lessons learned" that will help keep your sailors safe.*

5. *[REDACTED]. Similar in format and scope to the [REDACTED] they are high level summaries. I did not have access to more detailed files for these projects. But I think you are most interested in the [REDACTED] data anyway.*

This information was slowly and carefully collected over several years in the normal course of my job to avoid attracting attention and smuggled past security checkpoints a few pages at a time. I no longer have access to classified data so unfortunately cannot help you obtain other files. But I can answer your experts

[sic] questions using my own knowledge, if we can establish a secure and confidential means of communication.

I have divided the [REDACTED] into fifty one packages, all but the last have 100 sheets each. The first contains the [REDACTED] and the first of the drawings. If I understand your letter correctly, you offer an additional 70,000 USD Monero for the [REDACTED]. I propose the same payment schedule for the remaining files: 100,000 USD Monero each for the 49 packages, not additional for 51. In total, 5,000,000 USD Monero.

The amount per transaction is, in part, a security measure. As you noted in your letter, U.S. security forces are lazy. They also have limited budgets. Bait of 10,000 or 20,000 USD to catch an agent are within their normal activities. 100,000 USD and more? They may offer it, but they will not deliver such a large amount. New reports confirm this is a common tactic used by U.S. security forces to expose agents. Please do not be offended by this, but your generosity so far also matches exactly an adversaries [sic] likely play to entrap me.

We can exchange multiple packages at a time, if your superiors are comfortable with this arrangement. For security, I would strongly prefer not to make 50 separate drops to complete our business. But I understand you will want experts to evaluate the delivery. Maybe best to start with 1 package and increase as our trust grows? I suggest a simple code sent through Proton: email me the number of packages you want at the next drop. "1" for just the [REDACTED], "2" for the [REDACTED] and another package, and so forth.

My friend, we have both taken considerable risks to reach this point and with good luck will soon have much to celebrate!

Yours truly,

Alice

51. As referenced above, the Tor network is an open-source software that enables anonymous communication by directing Internet traffic through a free, worldwide, volunteer overlay network consisting of more than six thousand relays to conceal the user's location and usage from anyone conducting network surveillance of traffic analysis. The Tor network allows users to operate websites, called "hidden services," in a manner that conceals the true IP address of the computer hosting the website. Although law enforcement agents may be able to view and

access hidden services that are facilitating illegal activity, the IP address of a Tor hidden service cannot be determined via public lookups. Neither law enforcement nor hidden service users can determine the true IP address – and therefore the location – of the computer server that hosts a hidden service through public lookups or ordinary investigative means.

52. On August 13, 2021, the UC posing as a representative of COUNTRY1 sent an email to the previously provided Proton email address, stating "1" as a signal for a request for one package at the next drop on August 27, 2021.

The FBI Conducts a Dead Drop Operation in Eastern Virginia

53. On August 27, 2021, at approximately 11:12 p.m., the FBI observed **JONATHAN TOEBBE** depart his Annapolis residence as the sole occupant of a vehicle. **JONATHAN TOEBBE** was carrying a backpack.

54. On August 27, 2021, at approximately 11:35 p.m., "ALICE" sent a ProtonMail message confirming the dead drop date of August 28.

55. On August 27, 2021, at approximately 11:36 a.m., "ALICE" provided a Monero address to the FBI in a ProtonMail message.

56. On August 27, 2021, at approximately 11:52 p.m., the FBI observed **JONATHAN TOEBBE** return to his Annapolis residence as the sole occupant of the same vehicle. **JONATHAN TOEBBE** was carrying a backpack. Between approximately 11:12 p.m. and 11:52 p.m., **JONATHAN TOEBBE**'s cell phone remained on and at the residence, according to GPS location information.

57. On August 28, 2021, the FBI observed **JONATHAN TOEBBE** service a dead drop in eastern Virginia. The FBI observed **JONATHAN TOEBBE** place an item in the container and remove a written message placed in the container by the FBI. The FBI did not observe anyone

assisting in the service of the dead drop. **JONATHAN TOEBBE** had arrived at the dead location operating a vehicle in which he was the sole occupant.

58. Later on August 28, 2021, the FBI retrieved the contents of the dead drop, which consisted of an SD card concealed in a chewing gum package.

59. On the evening of August 28, 2021, the FBI electronically paid "ALICE" approximately $70,000 USD in Monero, bringing the total amount paid to date to $100,000 USD.

60. On August 29, 2021, at approximately 8:56 a.m., the FBI observed **JONATHAN TOEBBE** depart his Annapolis residence as the operator of a vehicle also occupied by one of his minor children. **JONATHAN TOEBBE** was carrying a backpack.

61. On August 29, 2021, at approximately 9:35 a.m., "ALICE" provided the password to the FBI in an encrypted ProtonMail message. The FBI subsequently opened the SD card and provided the contents to the U.S. Navy subject matter expert. The U.S. Navy subject matter expert determined that multiple documents on the SD card contained Restricted Data. Specifically, the U.S. Navy subject matter expert determined that the document contained schematic designs for the Virginia-class submarine. Virginia-class submarines are nuclear-powered cruise missile fast-attack submarines, which incorporate the latest in stealth, intelligence gathering, and weapons systems technology. Virginia-class submarines, with a per unit cost of approximately $3 billion, are currently in service with the United States Navy and are expected to remain in service until at least 2060.

62. In addition, FBI analysis of the SD card showed that it contained metadata indicating that the card had been connected to a computer with the same version of Macintosh operating system as the SD card contained in the package postmarked April 1, 2020, and described in Paragraph 13 above.

63. The SD card contained the following typed message from "ALICE":

First: I am very sorry for the confusion about this drop! When I first read your . . . letter, I didn't check what day of the week your proposed date was and assumed it was a Saturday. I was horrified to notice this detail while rereading your letter to walk through the exchange location one last time before sleeping. I hope my amateurish mistake caused you no serious trouble.

When I looked at your proposed drop site on a map, I was at first very alarmed. Considering the rules you explained for selecting a location, it does not seem to be in a very good neighborhood. However, I place my faith in your experience and hope for a happy outcome.

I have considered the possible need to leave on short notice. Should that ever become necessary, I will be forever grateful for your help extracting me and my family. I surmise the first step would be unannounced travel to a safe third country with plans to meet your colleagues. We have passports and cash set aside for this purpose. I pray such a drastic plan will never be needed, but you are right: it is a comfort to know you are ready and willing to aid us. Please let me know what I should do to prepare for this last resort.

You asked if I am working alone. There is only one other person I know is aware of our special relationship, and I trust that person absolutely. I was extremely careful to gather the files I possess slowly and naturally in the routine of my job, so nobody would suspect my plan. We received training on warning signs to spot insider threats. We made very sure not to display even a single one. I do not believe any of my former colleagues would suspect me, if there is a future investigation

.

The previous two exchanges were easy to find thanks to your excellent guidance. Based on the photos of this one, I am sure I had no trouble finding it to put this letter in your hands. I am nervous that this one is further, and more obviously off the typical path. If I am observed, an explanation will be more difficult. I am sure it is a balance, to ensure the container is not found accidentally. But too far from the trail exposes you and me to another risk of not appearing as natural tourists or joggers. For similar reasons, [the south-central Pennsylvania location] made me uncomfortable with only one logical parking area for a motorist and a literal observation tower overlooking the path start. I would prefer future drops to have multiple natural entrances and exits so that I can plan my own approach and retreat more easily. I hope this does not sound to you as overly critical. I am sure a professional would have no trouble, but I am painfully aware that I lack training in observation and blending in. Staying outside cities is very wise – let us continue with locations with [sic] an hour of Baltimore.

I understand your instructions on the use of overlapping Protons and the short signals we can use. Thanks to my mistake on the date, we have both made use of

it. I also emailed the payment address to limit the number of times I go out to connect to public WiFi. Rest assured, I always use a TOR onion connection to Proton, and never use a coffee shop or store close to home.

Although I am not positioned to acquire more documents than those listed in my last letter, I was serious in my offer to help address questions from your technical experts. I hope your letter, or your next will suggest how to open a secure channel for that aid.

Thank you for your partnership as well, my friend. One day, when it is safe, perhaps two old friends will have a chance to stumble into each other at a cafe, share a bottle of wine and laugh over stories of their shared exploits. A fine thought, but I agree that our mutual need for security may make that impossible. Whether we meet or no [sic], I will always remember your bravery in serving your country and your commitment to helping me.
Yours truly,

Alice

64. Based on my training and experience, when **JONATHAN TOEBBE** says "only one other person I know is aware of our special relationship, and I trust that person absolutely," I believe he is referring to his wife, **DIANA TOEBBE**.

65. On August 29, 2021, at approximately 10:12 a.m., the FBI observed **JONATHAN TOEBBE** return to his Annapolis residence as the sole occupant of the same vehicle. **JONATHAN TOEBBE** was carrying a backpack.

CONCLUSION

66. Based on the forgoing, there is probable cause that –

a. From or about an unknown date but no later than on or about April 1, 2020, through on or about October 9, 2021, in Jefferson County, West Virginia, within the Northern District of West Virginia, and elsewhere, the defendants, **JONATHAN TOEBBE** and **DIANA TOEBBE**, lawfully and unlawfully having possession of, access to, control over, and being entrusted with a document, writing, sketch, plan,

note, and information involving and incorporating Restricted Data within the meaning of the Atomic Energy Act, specifically 42 U.S.C. § 2014(y), did combine, conspire, confederate, agree and have a tacit understanding with each other to communicate, transmit, and disclose the same to another person with the intent to injure the United States and to secure an advantage to a foreign nation. During this period, a conspirator committed at least one overt act in furtherance of the conspiracy in the Northern District of West Virginia, in violation of 42 U.S.C. §§ 2274(a) and 2014.

b. On or about June 26, 2021, in Jefferson County, West Virginia, within the Northern District of West Virginia, the defendants, **JONATHAN TOEBBE** and **DIANA TOEBBE**, having possession of, access to, and having been entrusted with a document, writing, sketch, plan, note, and information involving and incorporating Restricted Data within the meaning of the Atomic Energy Act, specifically 42 U.S.C. § 2014(y), to wit: militarily sensitive design elements, operating parameters, and performance characteristics of Virginia-class submarine reactors, did unlawfully and knowingly communicate, transmit, and disclose the same to another person with the intent to injure the United States and to secure an advantage to a foreign nation, in violation of 42 U.S.C. §§ 2274(a) and 2014, and 18 U.S.C. § 2(a).

67. Accordingly, I request that the Court issue the proposed arrest warrants.

Respectfully submitted,

Justin Van Tromp
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on October 8, 2021.

HONORABLE ROBERT W. TRUMBLE
UNITED STATES MAGISTRATE JUDGE