

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA)
)
 v.)
)
 JACK DOUGLAS TEIXEIRA,)
)
)
)
 Defendant.)

Crim. No. 23-mj-4293-DHH

**GOVERNMENT’S SUPPLEMENTAL MOTION IN SUPPORT OF
PRETRIAL DETENTION**

Defendant Air National Guardsman Jack Douglas Teixeira (“the Defendant”) has been charged with unauthorized disclosures of classified national defense information in violation of the Espionage Act, 18 U.S.C. § 793(b) and (d), and the Act prohibiting Unauthorized Removal or Retention of Classified Documents or Material, 18 U.S.C. § 1924. All of the charged offenses are felonies.

The government respectfully submits that the Defendant must remain detained pursuant to 18 U.S.C. § 3142(f)(2)(A) and (B).

In the first place, the Defendant poses a serious flight risk. He currently faces 25 years in prison—and potentially far more—and other serious consequences for his conduct; the evidence against him is substantial and mounting; the charged conduct would very obviously end his military career; and he accessed and may still have access to a trove of classified information that would be of tremendous value to hostile nation states that could offer him safe harbor and attempt to facilitate his escape from the United States.

Second, the Defendant's own obstructive and deceptive acts to date compound his risk of flight and dangerousness, have undermined any counterarguments he could offer in response, and give rise to "a serious risk that such person will obstruct or attempt to obstruct justice." 18 U.S.C. § 3142 (f)(2)(B). Not only does the Defendant stand charged with having betrayed his oath and his country but—when those actions began to surface—he appears to have taken a series of obstructive steps intended to thwart the government's ability to ascertain the full scope of what he has obtained and the universe of unauthorized users with whom he shared these materials. This includes instructions the Defendant gave to other online members of a social media platform (including to "delete all messages" and "[i]f anyone comes looking, don't tell them shit") as well as the fact that following his arrest, authorities searched a dumpster at his residence and found a tablet, a laptop, and an Xbox gaming console, all of which had been smashed. These efforts appeared calculated to delay or prevent the government from gaining a full understanding of the seriousness and scale of his conduct. Any promise by the Defendant to stay home or to refrain from compounding the harm that he has already caused is worth no more than his broken promises to protect classified national defense information. And if the Defendant were released, it would be all too easy for him to further disseminate classified information and would create the unacceptable risk that he would flee the United States and take refuge with a foreign adversary to avoid the reach of U.S. law.

Third, the Defendant poses an ongoing risk both to the national security of the United States and to the community. The nature of the materials that the Defendant accessed—not all of which have publicly surfaced—have the capacity to cause additional exceptionally grave damage to the U.S. national security if disclosed. In addition, the Defendant's troubling history raises serious concerns about what he would do if released into the community.¹

¹ As discussed more fully below, the Defendant was suspended in high school based on concerning comments the Defendant made about Molotov cocktails and other weapons. The Defendant, who owned multiple guns, including a

Any one of the foregoing reasons warrants the Defendant's detention. Taken together, the case for the Defendant's detention pending trial is overwhelming.

I. STATEMENT OF PRIOR PROCEEDINGS

On April 13, 2023, the government charged the Defendant by criminal complaint (23-mj-4293-DHH) with violations of 18 U.S.C. § 793(b) and (d) and 18 U.S.C. § 1924. The Complaint alleges that the Defendant made unauthorized disclosures of a significant amount of classified information and disseminated that information without authorization to individuals—who likely included foreign citizens—not entitled to receive that information.

On April 14, 2023, at the Defendant's initial appearance, the government moved for detention pursuant to 18 U.S.C. § 3142(f)(2)(A) and (B) because no condition or combination of conditions will reasonably ensure that the Defendant does not flee, and that the Defendant would not take further steps to obstruct justice, including through the destruction of evidence or other action that would further endanger the U.S. national security or the physical safety of his community. The government now supplements its earlier, oral motion for pretrial detention.²

II. STATEMENT OF PROFFERED FACTS

The government proffers facts herein in support of the Defendant's flight risk and danger to the community through counsel and the attached declarations (attached hereto as Attachments A through K).³

high-capacity AK-style weapon, had regular discussions about violence and murder on the social media platform on which he disclosed the classified information.

² The government's motion is timely. *See United States v. Vargas*, 804 F.2d 157, 161 (1st Cir. 1986).

³ The Federal Rules of Evidence do not apply to pretrial detention hearings. *See* 18 U.S.C. § 3142(f)(2)(B) ("The Rules concerning admissibility of evidence in criminal trials do not apply to the presentation and consideration of information at the hearing."); *see also* FED. R. EVID. 1101(d)(3) (exception to application of federal evidence rules for "miscellaneous proceedings such as . . . considering whether to release on bail or otherwise."). Defendants at pretrial detention hearings are expressly authorized by the Bail Reform Act of 1984 to "present information by proffer or otherwise." 18 U.S.C. § 3142(f)(2)(B). Because the Act ratified existing practice, the government is likewise authorized to present information by proffer. Prior to the initial detention hearing, the government advised defense counsel that it intended to proceed by proffer. Defense counsel did not object.

A. The Defendant's Professional History

The Defendant enlisted in the U.S. Air National Guard (“USANG”) in September 2019. Since May 2022, the Defendant has served as an E-3/Airman, with the title of Cyber Defense Operations Journeyman. During that time, he was stationed at Otis Air National Guard Base in Massachusetts.

The Defendant held a security clearance at the Top Secret//Sensitive Compartmented information level since 2021. In connection with his enlistment, the Defendant signed multiple security and non-disclosure agreements, including, among others, a Sensitive Compartmented Information Nondisclosure Agreement; a Rules of Behavior and Acceptable Use Standard for Information Technology Agreement; and a General Information Systems Acceptable Use Policy and User Agreement *See* Attachments A (“SCINA”), B (“Rules”) and C (“General Information”). As part of these agreements, the Defendant agreed, among other things, that he would “never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency . . . that last authorized my access to SCI.” In some of these agreements, the Defendant also acknowledged that the unauthorized disclosure of classified information could constitute a criminal offense.

Nevertheless, government records reflect that, beginning in approximately February 2022, the Defendant began to access hundreds of classified documents containing national defense information that had no bearing on his role as essentially an information technology (“IT”) support specialist. *See* Attachment D, (the Church Audit Declaration).

B. The Defendant's Personal History

The Defendant is twenty-one years old. The Defendant graduated from high school in 2019 and does not have a college degree. In March 2018, while still in high school, the Defendant was suspended when a classmate overheard him make remarks about weapons, including Molotov cocktails, guns at the school, and racial threats. In the pretrial services interview, the Defendant attributed those remarks to a reference to a video game.⁴ See Attachment E, (Dighton Police Reports, redacted and filed separately under seal).

In 2018, while still a teenager, the Defendant applied for a firearms identification card ("FID"). His application was denied due to the concerns of the local police department over the Defendant's remarks at his high school. The Defendant remained undeterred and applied again in 2019 and 2020. In his 2020 application, the Defendant cited his position of trust in the United States government as a reason he could be trusted to possess a firearm. *See* Attachment F, (the Teixeira Letter).

The Defendant's primary residence is with his mother and stepfather in North Dighton, Massachusetts. The Defendant kept his gun locker approximately two feet from his bed. *See* Attachment G, (Search photos of Defendant's room). In the gun locker were multiple weapons, including handguns, bolt-action rifles, shotguns, an AK-style high-capacity weapon, and a gas mask. FBI special agents also found ammunition and tactical pouches on his dresser and what appeared to be a silencer-style accessory in his desk drawer. *Id.* When FBI special agents searched the dumpster outside the house, they located a military-style helmet with a mounting bracket—

⁴ The government has reviewed records relating to the 2018 incident from the Dighton Police Department. In these reports, a copy of which is being provided to the court and counsel under seal, the Defendant admitted he had been told to not speak of guns at school. The Defendant claimed he was speaking about a video game. Other students, however, indicated that Defendant's comments about the Molotov cocktail and guns were not related to any conversations about a video game.

such as those used for cameras—affixed to the top of the helmet. A GoPro camera⁵ was also found in the dumpster. *See* Attachment H, (GoPro photo).

A review of records received from a social media platform also indicate that the Defendant regularly made comments about violence and murder. *See* Attachment I, (the Church Social Media Declaration). The Defendant’s statements included the following:

- In November 2022, the Defendant stated that if he had his way, he would “kill a [expletive] ton of people” because it would be “culling the weak minded.”
- In February 2023, the Defendant told a user that he was tempted to make a specific type of minivan into an “assassination van.”
- Also in February 2023, the Defendant sought advice from another user about what type of rifle would be easy to operate from the back of an SUV. He describes how he would conduct the shooting in a “crowded urban or suburban environment.”
- In March 2023, the Defendant described SUVs and crossovers as “mobile gun trucks” and “[o]ff-road and good assassination vehicles.”

C. The Defendant’s Behavior Prior to Arrest

The Complaint Affidavit alleges that the Defendant posted Government Information (as defined therein) to a social media platform beginning in or around December 2022. Records from the social media platform reflect that the Defendant was an administrator of the server where the Government Information was posted. Those records also reflect the following activity under the username associated with the Defendant:

- The Defendant posted photographs of certain of his prior posts containing information that appears U.S. government classified information;
- The Defendant acknowledged on multiple occasions that he had posted classified information and that he had done so before December 2022;
- The Defendant referenced the intelligence community agencies from which the information was allegedly derived;

⁵ A GoPro camera is a durable camera that can be mounted to a helmet or sports equipment to record live action content.

- The Defendant encouraged other users to make specific requests for information they wanted to see him post;
- In March 2023, the Defendant stated that, although he “was very happy and willing and enthusiastic to have covered this event for the past year and share with all of you something that very few people in fact, get to see . . . I’ve decided to stop with the updates”; and
- In April 2023, the Defendant began using a new username, told another user that “[i]f anyone comes looking, don’t tell them shit.” He also encouraged that user to “delete all messages” and told him to pass the message on to other users to do the same.

See Attachment I.

In or around April 2023, the server where the Government Information described in Complaint was posted ceased to exist, suggesting that the server administrator—the Defendant—deleted the server in its entirety.

The Defendant also appears to have engaged in the attempted physical destruction of other evidence prior to his arrest. A search of the dumpster at the Defendant’s residence uncovered a tablet, a laptop, and an Xbox gaming console. *See* Attachment J, (Search photos of devices and location). All three devices were physically smashed. The FBI also located a box for a new iPhone in the dumpster. *Id.* The Defendant told several colleagues just two days before his arrest that he had a new phone number and email address. The Defendant told one colleague that his phone had flown out of his truck window and was run over by a semi-truck. *See* Attachment D.

III. STANDARD OF PROOF AND STATUTORY FACTORS

Congress empowered judicial officers to release or detain defendants pending trial. 18 U.S.C. § 3141(a). Detention determinations proceed pursuant to the terms of 18 U.S.C. § 3142. Under § 3142(f)(2), the Court must hold a detention hearing upon the government’s motion (or *sua sponte*) when the case involves “a serious risk that [the defendant] will flee” or “a serious risk that [the defendant] will obstruct or attempt to obstruct justice.” 18 U.S.C. § 3142(f)(2). Ultimately, the Court shall detain a criminal defendant pending trial upon a determination that “no

condition or combination of conditions will reasonably assure the appearance of the person as required and the safety of any other person and the community....” 18 U.S.C. § 3142(e); *United States v. Montalvo–Murillo*, 495 U.S. 711, 716–17 (1990). On the issue of flight, the government must prove that the defendant is a serious risk of flight by a preponderance of the evidence. *United States v. Patriarca*, 948 F.2d 789, 791-93 (1st Cir. 1991).

Although the Court cannot order the defendant’s detention based on dangerousness alone, *see United States v. Ploof*, 851 F.2d 7, 11 (1st Cir. 1988), obstruction of justice is a stand-alone basis justifying detention pending trial. *See United States v. Acevedo-Ramos*, 755 F.2d 203 (1st Cir. 1985) (upholding detention before trial based on the risk that the defendant would obstruct or attempt to obstruct justice); *see also U.S. v. Mehanna*, 669 F. Supp. 2d 160, 160, 166 (noting that obstruction is an independent ground for detention under (f)(2) and finding that the government met its burden to detain the defendant on that basis). Once the Court determines that the government has met its burden under risk of flight and/or obstruction of justice, dangerousness is a relevant consideration in determining whether the Defendant can ultimately be released on conditions.

In evaluating whether conditions can reasonably be fashioned, the Court must consider the following: (1) the nature and circumstances of the offense; (2) the weight of the evidence; (3) the defendant’s history and personal characteristics; and (4) dangerousness. 18 U.S.C. § 3142(g). With respect to dangerousness, the Senate Report accompanying the Bail Reform Act explains that dangerousness is not limited to physical violence and includes continued criminal activity:

The reference to safety of any other person is intended to cover the situation in which the safety of a particular identifiable individual, perhaps a victim or witness, is of concern, while the language referring to the safety of the community refers to the danger that the defendant might engage in criminal activity to the detriment of the community. The committee intends that the concern about safety be given a broader construction than merely danger of harm involving physical violence.

S. Rep. No. 225, 98th Cong., 1st Sess. 12 (1983), *reprinted in* 1984 U.S.C.C.A.N. 3182, 3195; *see United States v. Tortora*, 922 F.2d 880, 884 (1st Cir. 1990) (“Danger, in this context, was not meant to refer only to the risk of physical violence.”).

In prior cases alleging unauthorized removal and disclosure of classified national defense information, courts have readily found that the risk of future disclosures is a danger to the community sufficient to support pretrial detention. *See United States v. Winner*, 1:17-cr-00034-JRH-BKE, Dkt. 163, at 14 (S.D. Ga. Nov. 27, 2017) (“Given the uncertainty with respect to Defendant’s level of knowledge or possession of classified information, together with evidence that she planned to anonymously release information to online news outlets and that she has antipathy toward the United States, the Court finds that releasing Defendant prior to trial would pose a danger to the community, particularly to the national security.”); *United States v. Martin*, 1:17-cr-00069-RDB, Dkt. 24 (D. Md. Oct. 21, 2016) (“Under 3142(g)(4) – if considered, [the defendant’s] release presents a serious risk of danger to the *public due to his information, knowledge he possesses.*”) (18 U.S.C. § 793 charge; emphasis added).

IV. ARGUMENT: THE DEFENDANT SHOULD BE DETAINED PENDING TRIAL

The Defendant is accused of criminal conduct that reflects a profound breach of the trust our nation placed in him. He engaged in an incredibly large and damaging dissemination of classified national defense information and faces a significant term of imprisonment upon conviction. He has an enormous incentive to flee, and there are numerous adversaries of the United States that could provide him the means to do so, regardless of the conditions set by the Court. Additionally, his release would heighten the risk that he would make further unauthorized disclosures of classified national defense information. Further, it is clear that the Defendant has already attempted to obstruct justice by destroying evidence and tampering with witnesses.

Analyzed in light of the factors listed under the Bail Reform Act, there is no condition of release that can be set that will reasonably assure his future appearance at court proceedings or the safety of the community. He should be detained.

A. Nature and Circumstances of the Offense Charged – 18 U.S.C. 3142(g)(1)

The seriousness of the offense supports detention. The Defendant is currently charged with the unauthorized disclosure of a Top Secret document concerning the status of the Russia-Ukraine conflict, including troop movements. By definition, the disclosure of Top Secret information can be expected to cause exceptionally grave danger to the U.S. national security.

B. Weight of the Evidence Against the Person – 18 U.S.C. 3142(g)(2)

The weight of the government's evidence is strong. The forensic evidence against the Defendant is overwhelming and includes records of searches the Defendant made on his government computer, multiple admissions by the Defendant to transmitting classified information, and requests to others once his conduct became public to delete information tying him to the crime. Additionally, there is physical evidence that supports the contention that the Defendant, having illegally accessed classified documents, brought documents to the home he shared with his parents and photographed those documents there.

C. History and Characteristics of the Person – 18 U.S.C. 3142(g)(3)

The Defendant is a twenty-one-year-old man who is facing exceptionally grave legal peril both in the U.S. criminal justice system and in the consequences that are likely to be imposed by the U.S. military system. As multiple courts have noted, the more severe the sentence, the greater a defendant's incentive to flee. *United States v. Pierce*, 107 F. Supp. 2d 126, 128 (D. Mass. 2000) (upholding magistrate judge's detention order because defendant as get-away driver in robbery "has an extremely strong incentive to flee based upon the length of the prison term he faces under

the charges pending against him and the likelihood of conviction”); *see also United States v. Kakande*, No. 1:10-cr-00117-JAW, 2011 WL 1790639, *2 (D. Me. May 9, 2011) (“Generally, the longer the sentence the defendant is facing, the greater the incentive not to appear if released.”); *United States v. Almasri*, Crim. A. No. H-07-155, 2007 WL 296480, at *1 (S.D. Tex. Oct. 10, 2007) (finding severity of potential ten-year sentences weighed in favor of detention). The violations of 18 U.S.C. § 793 are punishable by up to ten years’ imprisonment for each violation, and the violation of 18 U.S.C. § 1924 is punishable by up to five years’ imprisonment.

The Defendant is facing mounting inculpatory evidence, potentially years of incarceration, and the loss of his livelihood. These facts alone are enough to incentivize a criminal defendant to flee. But in a case involving sensitive national defense information, these facts also make the Defendant an attractive candidate for recruitment by a foreign government that would seek to procure, disseminate, and use classified information to its benefit and to the detriment of the United States. Indeed, it has already been widely reported that adversaries of the United States have commented on the information the Defendant posted online. Those same adversaries have every incentive to contact the Defendant, to seek additional information he may have physical access to or knowledge of, and to provide him with the means to help him flee the country in return for that information.

The Defendant’s limited means support this concern that he would be susceptible to payment and recruitment by an adversary. As noted in the Pretrial Services Report, prior to arrest, the Defendant’s net worth was approximately \$19,000—approximately half of which appears to be tied to the value of his guns. If the Defendant is convicted of multiple felonies, the Defendant’s ability to find gainful employment after any period of incarceration would be limited. Even if the Defendant’s passport is taken away, if an adversary or even an ideological supporter provided the

means and the opportunity to evade the reach of U.S. law, there is nothing to suggest that—like others before him—the Defendant would not accept the opportunity to flee.

The Defendant’s risk of flight is further supported by the very nature of his betrayal. When the Defendant joined the U.S. Air National Guard, the Defendant took an oath to support and defend the Constitution of the United States. The Defendant signed multiple non-disclosure agreements with the Air Force. But neither solemn vow nor binding contract was enough to stop the Defendant from serving his own interests. For these reasons, the Government respectfully submits that any conditions imposed by this Court would similarly fail. Put simply, a preponderance of the evidence reflects a serious risk of flight. On this basis alone, the Defendant should be detained.

D. Nature and Seriousness of the Danger to Any Person or the Community – 18 U.S.C. 3142(g)(4)

1. The Defendant Destroyed Evidence and Tampered with Witnesses Before His Arrest and Is Likely to Continue to Obstruct Justice if Released

As noted above, the Defendant has already tampered with witnesses and has attempted to destroy inculpatory evidence. In so doing, he has exposed himself to additional legal peril. If released, there is nothing to suggest that the Defendant would not continue to destroy evidence, influence witnesses, and otherwise seek to obstruct justice prior to trial. Accordingly—and as contemplated in the Senate Report accompanying the Bail Reform Act—because the Defendant poses a danger to the integrity of this proceeding, the Defendant must be detained.

As discussed above, since multiple media outlets began to report on the unauthorized disclosure of purported classified information on or about April 6, 2023, the Defendant has taken or appears to have taken the following actions to obstruct justice:

- Deleted the social media server where he posted the Government Information;

- Encouraged others to delete inculpatory evidence;
- Procured a new phone number and email address; and
- Smashed multiple electronic devices and disposed of them in a dumpster.

It appears that the Defendant took these steps with the intent to cover his tracks and to obscure his role in multiple crimes. The government further believes that the Defendant would have no hesitation, if released, to continue in his efforts to obstruct efforts to bring him to justice, facts the Court must weigh in assessing the dangerousness prong of the Bail Reform Act.

The defense has indicated that they will seek release to the home of the Defendant's father. However, the Defendant has proven to be nothing short of deceptive and coercive, exposing others to peril in pursuit of his own freedom. Even if the Defendant's devices are removed from his father's home, his father certainly cannot be expected to spend every moment monitoring his son's access to electronic devices that remain in the home. Moreover, the Defendant's extensive background in computers would aid him in his efforts to hide his access to these devices. The Defendant has received instruction in the fundamentals of information technology, computer system familiarization, network fundamentals, and cyber security. *See* Attachment K, (CCAF Teixeira transcript). Based on this training and his many attempts to obstruct justice to date, the Defendant has not only the means but the motive and the skills to circumvent any potential restrictions of online activity this Court would impose upon him. Accordingly, the government submits that there is clear and convincing evidence to show that the Defendant poses a threat to the integrity of this judicial proceeding. For these reasons, the Defendant must be detained.

2. The Defendant is an Ongoing Risk to the National Security of the United States because of the Likelihood of Future Disclosures of Classified National Defense Information

Should he be released, the Defendant poses a direct threat of causing additional exceptionally grave damage to the U.S. national security. Between February 2022 and April 2023, the Defendant viewed hundreds of classified documents, many of which were classified at the Top Secret//Sensitive Compartmented Information level. The Defendant conducted hundreds more keyword searches in an effort to find classified information and even solicited requests from his online friends for specific information. *See* Attachment D. Many of the Defendant’s searches related to the Russia-Ukraine conflict. *Id.* The Defendant accessed these documents in what appears to be a deliberate effort to disseminate this country’s secrets.

As noted above, in considering the “safety of the community” as expressed in § 3142, the Court should consider more than merely a danger of harm involving physical violence and may consider, for example, a continuing generalized threat of criminal activity. *See United States v. Millan*, 4 F.3d 1038, 1048 (2d Cir. 1993). There can be no doubt that protecting the nation’s security secrets is of vital importance. As the Supreme Court has noted, “[i]t is ‘obvious and unarguable’ that *no governmental interest is more compelling* than the security of the Nation,” *Haig v. Agee*, 453 U.S. 280, 307 (1981) (emphasis added), which includes the “substantial interest in protecting sensitive sources and methods of gathering information.” *United States v. Abu Ali*, 528 F.3d 210, 247 (4th Cir. 2008) (quoting *United States v. Smith*, 780 F.2d 1102, 1108 (4th Cir. 1985)).

The information to which the Defendant had access—and did access—far exceeds what has been publicly disclosed on the Internet to date, a fact the Defendant himself acknowledged in a social media chat record from December 2022. In that record, the Defendant stated that he

“omit[s] a decent amount” of information because he was “[n]ot gonna type out 35 pages of information it’s just not happening.” He went on to state, “I tailor it and take important parts and include as many details as possible.” *See* Attachment I.

The Defendant’s release of additional national defense information could continue to cause “exceptionally grave damage to the national security.” *See* Executive Order 13526, § 1.2(a)(1). Here, the government is still investigating whether and where the Defendant may have retained any physical or digital copies of stolen classified information, including information that has not surfaced publicly. In this effort, the Defendant has a head-start on the government. The Defendant knows where the information is. He knows how to access it. And based on his specialized IT skills, he presumably knows how to disseminate that information without being immediately noticed.

But even if the government were to seize all physical or digital information the Defendant took and disseminated without authorization, the government cannot erase the knowledge the Defendant has acquired by virtue of his access to—and apparent study of—classified information over the course of at least a year. Put simply, there is nothing a court can do to ensure the Defendant’s compliance with his conditions of release other than take the Defendant at his word. *See Winner*, 1:17-cr-00034-JRH-BKE, Dkt. 163, at 14; *see also Martin*, 1:17-cr-00069-RDB, Dkt. 24. And the Defendant’s history of honoring similar types of agreements is abysmal. There simply is no condition or combination of conditions that can ensure the Defendant will not further disclose additional information still in his knowledge or possession.⁶ The damage the Defendant has

⁶ *See United States v. Tortora*, 922 F. 2d 880, 887 (1st Cir. 1990) (“Given the breadth of human imagination, it will always be possible to envision some set of release conditions which might reasonably assure the safety of the community. For instance, agents could be posted by the government to watch Tortora at all times to ensure that he remains compliant; the guards could search all visitors, dog Tortora's footsteps en route to all appointments, and otherwise act as private jailers. But the Bail Reform Act, as we read it, does not require release of a dangerous defendant if the only combination of conditions that would reasonably assure societal safety consists of heroic measures beyond those which can fairly be said to have been within Congress's contemplation.”).

already caused to the U.S. national security is immense. The damage the Defendant is still capable of causing is extraordinary. Detention is necessary to ensure that the Defendant does not continue on his destructive and damaging path.

3. The Defendant Poses a Physical Danger to the Community

As discussed above, the Defendant undoubtedly poses a danger to the U.S. at large based on his ability to cause exceptionally grave danger to the U.S. national security. However, there is also evidence to suggest that the Defendant may also pose a physical danger to the community.

The Defendant repeatedly engaged in detailed and troubling discussions about violence and murder on the social media platform where he also posted classified information. *See* Attachment I. Even giving the Defendant the benefit of the doubt and assuming some of his comments were hyperbolic, in 2018, the Defendant's school took his comments about weapons seriously enough to suspend him.

Moreover, as discussed above, the Defendant had multiple weapons just feet from his bed. A search of the Defendant's primary and secondary residences—that of his mother and father—also revealed the existence of a virtual arsenal of weapons, including bolt-action rifles, rifles, AR- and AK-style weapons, and a bazooka. Although the Bureau of Alcohol, Tobacco, and Firearms seized a number of weapons from the Defendant's primary residence, his father's weapons were not seized. And it is his father's home to which the Defendant is asking to be released.

Of additional concern, as discussed in Attachment D, the declaration of FBI Special Agent Luke Church the government is also aware that in July 2022, the Defendant used his government computer to search for the following terms: "Ruby Ridge," "Las Vegas shooting," "Mandalay Bay shooting," "Buffalo tops shooting," and "Uvalde." These searches were not related to the Defendant's position in information technology. While it has been reported in the media that these

searches may have been tied to the Defendant's belief that the government had prior notice of these threats and failed to act, the combination of these search terms, the Defendant's violent statements on social media, and the Defendant's arsenal of weapons is troubling.

The Defendant has already proved himself to be untrustworthy. The Defendant has already proved himself to be a danger to the U.S. national security. And in light of the physical danger posed by the Defendant if released, there is simply no condition or combination of conditions that can be fashioned to adequately address and mitigate the risk posed by his release.

V. CONCLUSION

Based upon the foregoing, the government has met its burden to show that no conditions of release will reasonably assure the Defendant's appearance, the safety of any person or the community, or the integrity of this proceeding. Accordingly, the government requests the Court order the Defendant detained prior to trial.

The government further requests that, if the Court is inclined to release the Defendant on conditions, it stay its order for such time as to permit the government to file a motion for revocation of the order of release under 18 U.S.C. § 3145(a).

Respectfully submitted,

RACHAEL S. ROLLINS
United States Attorney

/s/ Nadine Pellegrini
NADINE PELLEGRINI
JARED C. DOLAN
JASON CASEY
Assistant United States Attorneys
One Courthouse Way
Boston, MA 02210

MATTHEW G. OLSEN
Assistant Attorney General

/s/ Christina A. Clark
CHRISTINA A. CLARK
Trial Attorney
National Security Division
United States Department of Justice
950 Pennsylvania Ave., NW
Washington, DC 20530

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/S/ Nadine Pellegrini

NADINE PELLEGRINI
Assistant United States Attorney

Date: April 26, 2023

UNCLASSIFIED / FOR OFFICIAL USE ONLY / PRIVACY ACT APPLIES

Apply appropriate classification level and any control markings (if applicable) when filled in.

(U) SENSITIVE COMPARTMENTED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement between

JACK TEIXEIRA

and the United States.

(Name - Printed or Typed)

1. (U) Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to information or material protected within Special Access Programs, hereinafter referred to in this Agreement as Sensitive Compartmented Information (SCI). I have been advised that SCI involves or derives from intelligence sources or methods and is classified or is in process of a classification determination under the standards of Executive Order 13526 or other Executive order or statute. I understand and accept that by being granted access to SCI, special confidence and trust shall be placed in me by the United States Government.
2. (U) I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SCI, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information or material have been approved for access to it, and I understand these procedures. I understand that I may be required to sign subsequent agreements upon being granted access to different categories of SCI. I further understand that all my obligations under this agreement continue to exist whether or not I am required to sign such subsequent agreements.
3. (U) I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency (hereinafter Department or Agency) that last authorized my access to SCI. I understand that it is my responsibility to consult with appropriate management authorities in the Department or Agency that last authorized my access to SCI, whether or not I am still employed by or associated with that Department or Agency or a contractor thereof, in order to ensure that I know whether information or material within my knowledge or control that I have reason to believe might be, or related to or derived from SCI, is considered by such Department or Agency to be SCI. I further understand that I am also obligated by law and regulation not to disclose any classified information or material in an unauthorized fashion.
4. (U) In consideration of being granted access to SCI and of being assigned or retained in a position of special confidence and trust requiring access to SCI, I hereby agree to submit for security review by the Department or Agency that last authorized my access to such information or material, any writing or other preparation in any form, including a work of fiction, that contains or purports to contain any SCI or description of activities that produce or relate to SCI or that I have reason to believe are derived from SCI, that I contemplate disclosing to any person not authorized to have access to SCI or that I have prepared for public disclosure. I understand and agree that my obligation to submit such preparations for review applies during the course of my access to SCI and thereafter, and I agree to make any required submissions prior to discussing the preparation with, or showing it to, anyone who is not authorized to have access to SCI. I further agree that I will not disclose the contents of such preparation with, or show it to, anyone who is not authorized to have access to SCI until I have received written authorization from the Department or Agency that last authorized my access to SCI that such disclosure is permitted.
5. (U) I understand that the purpose of the review described in paragraph 4 is to give the United States a reasonable opportunity to determine whether the preparation submitted pursuant to paragraph 4 sets forth any SCI. I further understand that the Department or Agency to which I have made a submission will act upon it, coordinating within the Intelligence Community when appropriate, and make a response to me within a reasonable time, not to exceed 30 working days from date of receipt.
6. (U) I have been advised that any breach of this Agreement may result in my termination of my access to SCI and removal from a position of special confidence and trust requiring such access, as well as the termination of my employment or other relationships with any Department or Agency that provides me with access to SCI. In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute violations of United States criminal laws, including provisions of Sections 793, 794, 798, and 952, Title 18, United States Code, and of Section 783(b), Title 50, United States Code. Nothing in this agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.
7. (U) I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I have been advised that the action can be brought against me in any of the several appropriate United States District Courts where the United States Government may elect to file the action. Court costs and reasonable attorney's fees incurred by the United States Government may be assessed against me if I lose such action.
8. (U) I understand that all information to which I may obtain access by signing this Agreement is now and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a court of law. Subject to such determination, I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials that may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials. If I do not return such materials upon request, I understand this may be a violation of Section 793, Title 18, United States Code.
9. (U) Unless and until I am released in writing by an authorized representative of the Department or Agency that last provided me with access to SCI, I understand that all conditions and obligations imposed on me by this Agreement apply during the time I am granted access to SCI, and at all times thereafter.
10. (U) Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect. This Agreement concerns SCI and does not set forth such other

FORM 4414 (Rev. 12-2013)

UNCLASSIFIED / FOR OFFICIAL USE ONLY / PRIVACY ACT APPLIES

Page 1 of 2

CL: _____
DECL ON: _____
DRV FROM: _____

UNCLASSIFIED / FOR OFFICIAL USE ONLY / PRIVACY ACT APPLIES

Apply appropriate classification level and any control markings (if applicable) when filed in.

conditions and obligations not related to SCI as may now or hereafter pertain to my employment by or assignment or relationship with the Department or Agency.

11. (U) I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available Sections 793, 794, 798 and 952 of Title 18, United States Code, and Section 783(b) of Title 50, United States Code, and Executive Order 13526, as amended, so that I may read them at this time, if I so choose.

12. (U) I hereby assign to the United States Government all rights, title and interest, and all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.

13. (U) These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

14. (U) These restrictions are consistent with and do not supersede conflict with or otherwise alter the employee obligations rights or liabilities created by Executive Order 13526; or any successor thereto, Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosures to Congress by members of the Military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosure of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), sections 7(c) and 8H of the Inspector General Act of 1976 (5 U.S.C. App.) (relating to disclosures to an inspector general, the inspectors general of the Intelligence Community, and Congress); section 103H(g)(3) of the National Security Act of 1947 (50 U.S.C. 403-3h(g)(3)) (relating to disclosures to the inspector general of the Intelligence Community); sections 17(d)(5) and 17(e)(3) of the CIA Act of 1949 (50 U.S.C. 403q(d)(5) and 403q(e)(3)) (relating to disclosures to the Inspector General of the Central Intelligence Agency and Congress); and the statutes which protect agent disclosure which may compromise the national security, including Section 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Control Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

15. (U) This Agreement shall be interpreted under and in conformance with the law of the United States.

16. (U) I make this Agreement without any mental reservation or purpose of evasion.

Jocelynne Signature 07 July 2021 Date

The execution of this Agreement was witnessed by the undersigned who accepted it on behalf of the United States Government as a prior condition of access to Sensitive Compartmented Information

WITNESS and ACCEPTANCE: [Redacted] Signature 07 July 2021 Date

SECURITY BRIEFING / DEBRIEFING ACKNOWLEDGMENT

SI	TK	G	HCS-P	****	****
****	****	****	****	****	****
(Special Access Programs by Initials Only)					
SSN (See Notice Below)		Printed or Typed Name		Organization	
BRIEF Date <u>07 July 2021</u> I hereby acknowledge that I was briefed on the above SCI Special Access Program(s): <u>Jocelynne</u> Signature of Individual Briefed			DEBRIEF Date _____ Having been reminded of my continuing obligation to comply with the terms of this Agreement, I hereby acknowledge that I was debriefed on the above SCI Special Access Program(s): _____ Signature of Individual Briefed		
_____ Printed or Typed Name			_____ Organization (Name and Address)		

(U) NOTICE: The Privacy Act, 5 U.S.C. 522a, requires that federal agencies inform individuals, at the time information is obtained from them, whether the disclosure is mandatory or voluntary, by what authority such information is collected, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSAN) is Executive Order 9397, as amended. Your SSAN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above, 2) determine that your access to the information has terminated, or 3) certify that you have witnessed a briefing or debriefing. Although disclosure of your SSAN is not mandatory, your failure to do so may impede such certifications or determinations.



102d Intelligence Wing

Information Technology User Agreement

Rules of Behavior and Acceptable Use Standards for Information Technology

The following statements reflect mandatory behavioral norms and standards of acceptable use of Air Force Information Technology. By signing below, you indicate both your understanding of these standards, and your agreement to act in accordance with them as a condition of your service with or access within the Air Force. Air Force Instruction 17-130, *Cybersecurity Program Management*, applies.

1. I WILL adhere to and actively support all legal, regulatory, and command requirements.

- a. I understand that Air Force Information Technology is to be used primarily for Official/ Government Business, and that limited personal use must be of reasonable duration and frequency that have been approved by the supervisors and do not adversely affect performance of official duties, overburden systems or reflect adversely on the Air Force or the DoD.
- b. I will not use my access to government information or resources for private gain.
- c. I waive my expectation of privacy in my Air Force electronic communications. This is not a waiver of my rights to attorney-client privilege, medical information privacy, or the privacy afforded communications with religious officials/ chaplains.
- d. I will observe all software license agreements and Federal copyright laws.
- e. I will encrypt sign and any message containing For Official Use Only or Personally Identifiable Information.
- f. I will promptly report all security incidents in accordance with Air Force policy.

2. I WILL use the system in a manner that protects information confidentiality, integrity and/or availability.

- a. I will not store or process classified information on any system not approved for classified processing.
- b. I will protect my Common Access Card/hardware token from loss, compromise, or premature destruction. I will not share my token/credentials with anyone, use another person's token/credentials, or use a computer or terminal on behalf of another person.
- c. I will protect my passwords/Personal Identification Numbers from disclosure: I will not post or write these down in my work space.
- d. I will lock or log-off my computer or terminal any time I walk away.
- e. I understand that my password/Personal Identification Numbers must adhere to current Air Force standards for length, key-space, and aging requirements.
- f. I will not disclose any non-public Air Force or DoD information to unauthorized individuals.
- g. I understand that everything done using my Common Access Card/hardware token/password/Personal Identification Number will be regarded as having been done by me.
- h. I will employ anti-malware software and update it as required; I will immediately notify my CFP or WCO if I believe Air Force Information Technology assets entrusted to me have been compromised; I will take immediate measures to limit damage.

3. I WILL protect the physical integrity of computing resources entrusted to my custody or use.

- a. I will protect Air Force Information Technology from hazards such as liquids, food, smoke, staples, paper clips, etc.
- b. I will protect Air Force Information Technology from tampering, theft or loss; I will take particular care to protect any portable devices and media entrusted to me, such as laptops, cell phones, tablets, disks, and other portable electronic storage media.
- c. I will protect Air Force Information Technology storage media from exposure to physical, electrical, and environmental hazards. I will ensure that media is secured when not in use based on the sensitivity of the information contained, and practice proper labeling procedures.
- d. I will not allow anyone to enter DoD or Air Force facilities without proper authorization.
- e. I will not install, relocate, modify, or remove any Air Force Information Technology without proper approval.

4. I WILL NOT attempt to exceed my authorized privileges.

- a. I will not access, research, or change any account, file, record, or application not required to perform my job.
- b. I will not modify the operating system configuration on Air Force Information Technology without proper approval.
- c. I will not move equipment, add or exchange system components without authorization by the appropriate approval of my local systems manager or local hardware custodial personnel.
- d. I will not use, or connect to, non-official hardware, software or networks for official business without proper approval and without the use of authorized mobile device network encryption.

5. I WILL NOT use systems in a way that brings discredit on Air Force users or the Air Force, or degrade Air Force missions.

- a. I will practice operational security in accordance with guidance contained in Air Force Instruction 10-701, *Operations Security*.
- b. I will not receive or send inappropriate material using my official email or Internet accounts.
- c. I will not originate or forward chain letters, hoaxes, or items that advocate or support a political, moral or philosophical agenda.
- d. I will not add slogans, quotes, or other personalization to an official signature block.
- e. I understand that pornography, sexually explicit or sexually oriented material, nudity, hate speech or ridicule of others on the bases of protected class (e.g., race, creed, religion, color, age, sex, disability, national origin), gambling, illegal weapons, militant, extremist, or terrorist activities will not be tolerated.
- f. I will not connect or remove any form of removable media without proper approval.

6. I WILL NOT waste system and network resources.

- a. I will not make excessive use of my official computer to engage with social media for personal purposes (e.g., Facebook, Twitter, Instagram, Snapchat, etc.)
- b. I will not make excessive use of my official computer for shopping, or to view full-motion video from non-official sources (e.g., YouTube, online multiplayer video games, etc.)
- c. I will not auto forward e-mail from my official account to a personal e-mail account.

Teixeira, Jack, D

Name (Last, First, MI)

TEIXEIRA.JACK.DOUGLAS.1539098230
39098230

Signature

Digitally signed by
TEIXEIRA.JACK.DOUGLAS.1539098230
Date: 2021.07.28 18:03:51 -04'00'

28-Jul-2021

Date

AB/E-1

Rank/Position



102nd ISR Group DGS-MA



General Information Systems Acceptable Use Policy and User Agreement

This agreement is for all users (military, civilian, and contractor) of any and all current and future networks and Information Systems installed and operated at 102 ISRG / DGS-MA. Compliance with this agreement is mandatory.

The **INDIVIDUAL** provides much of the protection for the information contained in the IS. If your security alertness is relaxed at any time, a security violation or compromise may result which could cause grave damage to national security. In the final analysis, system security depends upon **YOU**, the individual user.

Place your initials in left column and digitally sign when completed indicating that you have read and understand this user agreement. Any questions please contact any member of the 102ISRG Information Assurance Office staff.

1. **Purpose.** To emphasize your individual responsibilities when accessing 102ISRG/DGS-MA Site Information Systems (IS) and resources.
2. **General.** The fundamental approach to security of Information Systems is based on the principles of individual accountability and need-to-know. Procedural and technical security features incorporated into systems are required to provide adequate protection for the system and the data contained within.
3. **Policy.** U.S. Government policy requires all classified information be appropriately safeguarded to ensure the confidentiality, integrity, and availability of the information. Safeguards will be applied such that information is accessed only by authorized persons and processes, is used only for authorized purposes, retains its content integrity, is available to satisfy mission requirements, and is appropriately marked and labeled. The combination of security safeguards and procedures shall assure that the system and users are in compliance with ICD, DoD, NSA, DIA, USAF, ANG and 102ISRG Information Systems security guidance and publications.
4. **Individual Responsibilities.** Upon receipt of your userid and password, you will have access to various Information Systems that process and store classified information (For Official Use Only, Confidential, Secret, Top Secret SCI). The burden of responsibility for the security of classified information stored within these system ultimately rests with each person who uses or has access to the system. No matter how elaborate the built-in precautions and safeguards, they provide little security if each person using the system does not enact personal responsibility for security. The following are key requirements and responsibilities of each individual user associated with the 102ISRG/DGS-MA Site:

4.1 General User Requirements:

- a. Be a U.S. citizen

4.2 Account Access Control/Information Systems Protection

- a. **I will not share or permit my logon userid to be used by anyone else.**
Individuals requiring temporary or permanent network access should only be provided access through the authorization of the Information Assurance Office.
- b. **I will accept responsibility for ANY and ALL activity that occurs under my individual User-ID.**
- c. **I will ONLY use the access or privilege granted to me to perform authorized tasks or mission-related functions.**
- d. User names and passwords will be stored and safe guarded at the same classification level of the Information Systems they permit access.
- e. I will use the system and network, to include access to the Internet, Electronic Mail (E-mail) and network shares for only authorized purposes IAW AFI 33-200, Information Assurance (IA) Management, AFMAN 33-152, User Responsibilities And Guidance For Information Systems, AFI 33-115, Air Force Information Technology (IT) Service Management, and ICD 503.
Reading of the listed documents is highly recommended but not required.
- f. I understand that masking my identity or assuming the identity of another user is strictly prohibited, except by authorized law enforcement personnel.

JT

JT

JT

JT

JT

JT

JT

g. It is your responsibility to control access and utilization of any "private" files, which you have stored under your User ID/password. **YOU** are accountable for any use made of such files or data and for the correct classification, caveats, and any modifications made to them.

JT

h. You must not access the accounts of others with the intent to read, browse, modify, copy, or delete files and directories unless they have given you specific authorization to do so. Authorization is a permissions application within the system, not sharing of password(s).

JT

i. **LOGOFF** properly at the end of each session. If the machine will not give you the required LOGOFF response, inform your ISSO, CMOC or a System Administrator.

JT

j. You must notify the Information Assurance Office Account Management personnel of TDYs exceeding 30 days or more prior to your departure.

JT

k. I will not leave my workstation signed on and unattended without at least utilizing the screensaver password screen-locking function. **When leaving at the end of the duty day, I will properly and completely log off the network.**

JT

l. I will report all security violations, system vulnerabilities, suspicious network activities, and detected viruses to the System Administrator or ISSO.

JT

m. Report all security incidents to the ISSO, ISSM, SSO or SA

JT

n. I will comply with all computer and network security guidance issued by my unit and IA Office and will acknowledge this by going to the *IAO office and acknowledging this to the ISSM.*

JT

o. I will comply with additional policies and procedures prescribed by my ISSO or Unit Security Manager which may be required for operating a classified workstation.

JT

p. **I Will Immediately Report any and all classified data spillages and computer virus activities to ISSM/ISSO and SSO or ISS CMOC.**

JT

q. All AFDGS and JWICS accounts will expire when your Information Assurance (IA) certificate expires. When re-accomplishing your IA certificate please get the Information Assurance Office a soft copy (saved in landscape format so we can see full date), please e-mail it to the 102ISRG IA Office Niprnet group mailbox: 102 IW/IG Information Assurance Org

JT

4.3 PASSWORDS

JT

a. Your password is **FOR YOUR EYES ONLY** and **WILL NOT** be disclosed to, or used by, anyone else regardless of the situation or circumstances.

JT

b. You **WILL NOT** give out your password nor log on for any individual, whether they have access to the system or not. Such disclosure to, or use by, another is considered a security violation.

JT

c. **Passwords** will **NOT** be written down or stored in desk drawers, programmed into function keys, part of batch or login scripts, et cetera. A user storing his/her password in this manner will have committed a security violation.

JT

d. Your password must meet the complexity requirement of ICS 500-16 and the Information System you have been granted access to. Generally your password must be a minimum of 14 characters in length, must consist of at least two upper case letters, two lower case letters, two numbers and two special characters (non-alpha/numeric). It cannot contain dictionary words or any information that pertains to you (i.e. date of birth, spouse or child name, pet name, etc.) will not contain multiple repeated characters, full dictionary words (in English or any other languages), names, or well-known dates.

JT

e. Report any compromise or suspected compromise of a password to the ISSO or ISSM.

JT

f. **You will change your password at least every 90 days.**

JT

g. **You will protect your password at the classification of the system for which it is assigned.**

JT

4.4 Media Control

a. All Removable/Magnetic media (floppies, CD-ROM's, etc) will be scanned for viruses using established procedures prior to opening the files on any workstation.

b. Comply with ALL rules and regulations for scanning all magnetic media that he/she introduces, mails, or transports into or out of the organization.

- JT c. I will protect all sensitive data (Privacy Act, For Official Use Only or Classified) processed, displayed, printed, or stored at my terminal using the proper guidance.
- JT d. I will appropriately mark any removable storage media containing sensitive/classified data.
- JT e. When not in use, I will properly secure FOUO, Privacy Act, sensitive or classified data to prevent inadvertent access.
- JT f. Provide appropriate classification marking, caveat and safeguard statements on all IS files, output products, and storage media.
- JT g. All Removable Media for use within a 102ISRG SCIF WILL be issued by the ISSM/ISSO. All media (CD- ROMS, DVDs, Tapes, removed hard drives, OEM install disks, etc.) Entering the SCIF MUST be in-checked with the Information Assurance Office.
- JT h. Safeguard and report any unexpected or unrecognizable output products to the ISSO, SysAd or ISSM as appropriate. This includes both display and printed products.
- JT i. Safeguard and report the receipt of any media received through any channel to the appropriate ISSO, SysAd or ISSM for subsequent virus inspection and inclusion into the media control procedures.
- JT j. All media that is no longer needed or needs to be destroyed will be brought to the Information Assurance Office for destruction. All media leaving the SCIF needs to be out-checked with the Information Assurance Office.
- JT k. In the event that media that has been issued is lost. That individual that signed out the media MUST report the loss to the ISSM/ISSO, SSO or ISS CMOC as soon as possible.
- JT l. Suspected misuse or compromise of removable media or information contained therein must be reported to the ISSM/ISSO or SSO immediately.
- JT m. **Network File Transfers:** All Files needing to be transferred from one network to another (Low to High) may be performed by the user through the DoDIIS One-Way Transfer Service(DOTS). Any other transfers will be performed by the Information Assurance Office.(Contact us for details.) If moving down in classification, if it can't go thru T-MAN then it aint gonna happen! No files will be downgraded from any classified classification to unclassified.

4.5 Email

- JT a. USAF email systems are provided to support USAF missions. You are only authorized to use email systems for official, authorized government business related to your duties.
- JT b. You are prohibited from transmitting fraudulent, unethical, harassing, chain letter, or personal messages and files. Do not overburden the e-mail systems with large broadcasts or group mailings.
- JT c. You must not send any electronic mail or other form of electronic communications by forging another user's identity or attempt to conceal the origin of the message in any way.
- JT d. Receipt of prohibited or inappropriate electronic mail or files must be reported to the appropriate ISSO.

5. **Precautions** Following are several specific *precautions* which you must always take in order to protect both yourself and the Information System from possible compromise:

- JT 5.1 **You MUST practice good OPSEC awareness and consider the OPSEC implications and possible vulnerabilities when posting ANY information to ANY social networking sites or commercial websites.**
- JT 5.2 Ensure no other person is in position to see the terminal keyboard while **your password** is being typed.
- JT 5.3 Ensure that when you create, file, or store data, regardless of its originator, that the classification and/or special handling caveats correctly apply to all material embedded within the data or file.

- JT 5.4 Ensure that any data/file that you store or create does not exceed the overall classification and special handling caveats of the Information System.
- JT 5.5 Ensure that all output is handled in accordance with the pertinent document security procedures.
- JT 5.6 Before you leave the terminal area, make sure you are logged off, all paper output is removed from the terminal area and properly secured, and any waste is appropriately shredded.

6. Prohibited activities:

- JT 6.1 **I will not download, install or attempt to configure any software or hardware to either the workstation or network server.**
- JT 6.2 **I WILL NOT attempt to access any files, data, software, devices or network resources which have been readily restricted to me by network permissions and/or software or hardware security mechanisms, or perform a function for which I do not have authorization. I will not attempt to access, modify or configure any system administration resources installed on any network.**
- JT 6.3 **I WILL NOT leave a live terminal unattended. (Log Off or engage the screen-lock.)**
- JT 6.4 **I WILL NOT use your computer system or resource to harass anyone.**
- JT 6.5 **I WILL NOT use computer assets for personal or private financial gain or illegal activities, entertainment, or other private pursuits such as gambling, betting, lottery, pornography, or any similar activity.**
- JT 6.6 **I WILL NOT play music or video CD/DVDs on government systems.**
- JT 6.7 **I WILL NOT Release, Disclose, or Alter information without the consent of the Data Owner or the Disclosure Officer's approval. Violations may result in prosecution of military members under the Uniform Code of Military Justice, Article 92 or appropriate disciplinary action for civilian employees.**
- JT 6.8 **I WILL NOT Attempt to strain or test or bypass or circumvent any computer security features or mechanisms. For example, when users leave their workstation unattended without using appropriate screen lock, other users shall not use the system.**
- JT 6.9 **I WILL NOT Modify the system equipment or software or use it in any manner other than its intended purpose.**
- JT 6.10 **I WILL NOT Relocate or change any IS equipment or the network connectivity of IS equipment without proper security authorization.**
- JT 6.11 **I WILL NOT Introduce malicious code into any IS or network.**
- JT 6.12 **Unauthorized use of software.** You are prohibited from loading any software on any computer system and/or computer network without the approval of the appropriate system administrator. Generally, the system administrator will add new software. This prohibition includes commercial, shareware, freeware, and government-owned software.
- JT 6.13 **You are expressly prohibited** from using USAF computers to make illegal copies of licensed or copyrighted software. Copyrighted software must only be used in accordance with its license or purchase agreement. You do not have the right to own or use unauthorized copies of software or make unauthorized copies of software for yourself or others.
- JT 6.14 **You are prohibited** from using software that is designed to destroy data, provide unauthorized access to the computer systems, or disrupt computing processes in any other way. The use of viruses, worms, Trojan horses, and other invasive software is expressly forbidden. Systems subject to invasive software are equipped with antivirus software, and users are required to use it. You are prohibited from tampering with or turning off this antivirus software.
- JT 6.15 **Use of the Information Systems for other than official government business is strictly prohibited and any violation of this prohibition may result in administrative and/or punitive sanctions.**

7. User Training:

- JT 7.1 I will ensure that my **Information Assurance Certification** stays current. Failure to do so will result in all your accounts being suspended.

JT 7.2 I will attend/complete additional training as directed: TEMPEST, Annual Information Assurance Briefings, etc.

8. CREW COMM DATA SPILLAGE AND INADVERTENT DISCLOSURE:

JT 8.1 I am aware of the capability of the Crew Comm system to connect to a lower classified level. I will constantly be aware of what security level I am communicating at and will be ever vigilant and mindful of what can and cannot be said.

JT 8.2 In the event of inadvertent disclosure of higher classified data on a lower classified network I will IMMEDIATELY self-report the incident to the Mission Supervisor on duty and the Special Security Officer to initiate the Inadvertent Disclosure process.

JT 8.3 I will not use the "Hot Mic" feature of Crew Comm since Hot Mic is the same as an Open Mic and is a Security Risk.

JT 9. **NOTICE AND CONSENT TO MONITORING:** (cao: DTM-08-060, May 9, 2008 /Change 5, 09/25/2013)

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) Information Systems:

- You are accessing a U.S. Government (USG) Information System (IS) (which includes any device attached to this Information System) that is provided for U.S. Government authorized use only.
- You Consent to the following conditions:
 - The U.S. Government routinely intercepts and monitors communications on this Information System for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
 - At any time, the U.S. Government may inspect and seize data stored on this Information System.
 - Communications using, or data stored on, this Information System are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.
 - This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.
 - Notwithstanding the above, using an Information System does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
 - Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an Information System, regardless of any applicable privilege or confidentiality.
 - The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
 - Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
 - A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
 - These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.
- o In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (Le., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.
 - o All of the above conditions apply regardless of whether the access or use of an Information System includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

I understand that failure to comply with the network security policies and procedures that govern the networks I have access to may result in disciplinary action or loss of network access.

I have completed Information Assurance (IA) Training for the year that I am completing this form. This training must be completed prior to signing this User Agreement. Training will be obtained through the applicable unit.

I have read, understand, and will comply with the terms of this agreement.

Teixeira Jack D

PRINT Last Name, First Name, MI

102 ISS

Organization

AB E-1

Rank/Civilian Duty Title

SCOA

Office Symbol

508-968-7839

Duty Phone

7/15/2021

Date

**TEIXEIRA.JAC
K.DOUGLAS.1
539098230**

Signature of User

Digitally signed by
TEIXEIRA.JACK.DOUG
LAS.1539098230
Date: 2021.07.15
15:30:21 -04'00'



U.S. Department of Justice
Federal Bureau of Investigation

**DECLARATION OF LUKE CHURCH, SPECIAL AGENT,
FEDERAL BUREAU OF INVESTIGATION**

I, LUKE CHURCH, do hereby declare and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation and have been since August 2022. As a Special Agent, I have received training at the FBI Academy located in Quantico, Virginia, including 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, 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.

2. I am currently investigating the activities of JACK DOUGLAS TEIXEIRA ("TEIXEIRA"), whom I believe 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.

3. I make the following statements based upon my personal knowledge and information made available to me in my official capacity.

I. U.S. Government Agency Audit Data

4. During the course of my investigation, I had occasion to interact with the second U.S. Government Agency (“U.S. Government Agency 2”) described in the Affidavit in Support of an Application for a Criminal Complaint and Arrest Warrant (“Affidavit”) for TEIXEIRA.

5. As articulated in the Affidavit, U.S. Government Agency 2 has the ability to monitor certain searches conducted on its classified networks. U.S. Government Agency 2 also has the ability to conduct an audit of certain documents and links that a user accesses on its classified networks.

6. On April 17, 2023, I observed an audit conducted by a subject matter expert affiliated with U.S. Government Agency 2 for all searches TEIXEIRA conducted across an Intelligence Community-wide system for which U.S. Government Agency 2 acts as a service provider. The audit yielded results dating back to February 26, 2022.

7. These audit results indicated that TEIXEIRA conducted hundreds of searches on the classified network on a number of subjects, many of which related to the Russia-Ukraine conflict.

8. In addition, on or around July 30, 2022, TEIXEIRA searched for the following terms: “Ruby Ridge”; “Las Vegas shooting”; “Mandalay Bay shooting”; “Buffalo tops shooting”; and “Uvalde.”

9. During the course of my investigation, I have also reviewed audit data from U.S. Government Agency 2 regarding certain documents that TEIXEIRA accessed.

That audit data revealed that TEIXEIRA accessed hundreds of classified reports and/or documents on his classified network.

II. Interviews of Teixeira Colleague


10. As part of my investigation, I have also participated in interviews of multiple individuals who were associated with Teixeira. Among the individuals I interviewed was a colleague of Teixeira in the Air Force National Guard.

11. During the course of that interview, that colleague recalled that on Teixeira's last shift before his arrest, Teixeira told him he had a new phone number and email address. When asked if he had been hacked, Teixeira responded, "something like that." Teixeira then explained that his phone flew out of the window of his truck while he was driving and that it was run over by a semi-truck.

12. The same colleague told me that Teixeira was very quiet, but often talked about guns. He also said he believed he would be the first person Teixeira would shoot if Teixeira were to shoot anyone in the workplace.

* * *

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.



Luke Church
Special Agent, Federal Bureau of Investigation

November 15, 2020

Dear Officer Ferreira,

Thank you very much for calling me last week and giving me the chance to show you and the Chief how I have matured/changed since March 27th, 2018, and for allowing me the opportunity to be considered trustworthy. On or about the same date above I said some things while I was a Sophomore in High School that were inappropriate, and unfortunately I was insensitive to the current events going on at other schools. I lacked some of the social disciplines and the situational awareness needed at that time to make a logical decision on how to express myself verbally. In retrospect, when I was sixteen years of age I never looked at how people reacted to what I said, and I didn't think it would matter or affect my life. I understand now that I couldn't have been more wrong.

After two years and eight months since the date above, I am very cognizant of the world around me and know how powerful words can be. I realized after the incident and of course understand now that what I say matters and to weigh my words, knowing now the "ripple in the pond" effect works. In hindsight, it disturbs me that I made people uncomfortable or even scared because of what I said. I now have the situational awareness and social disciplines I lacked in March of 2018 and am very aware of my surroundings when I speak.

In 2019 I enlisted in the United States Air Force/Air National Guard working for the 102d Intelligence Wing as a Cyber Transport Specialist. I have been to Basic Training and am awaiting my Tech School in January 2021, which the break in training was due to the Covid 19 outbreak. In order to go to Tech School, I needed an adjudicated Top Secret clearance with the Government, which I have now.

The investigation process was extremely thorough, and the events that happened on March 27th, 2018 at Dighton Rehoboth High School were discussed. Everything was explained to the investigator about the incident as well as police reports, school letters and any or all documents that were submitted to the investigator that were generated from this event. I was very concerned that my decisions that I made at 16 would haunt my future in serving my country in the military and am glad they did not.

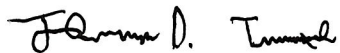
With wearing the uniform and being a representative/ambassador of the United States Air Force, and now having a Top Secret clearance, I now represent much more than myself and need to watch what I say and do both in public and in private, as it affects more than just myself. I think that I have grown as a person, especially after joining the Air Force/ANG and putting on the uniform. I uphold and apply in my personal life as well as my military career the three Air Force core values, Integrity First, Service Before Self, and Excellence in All We Do.

The Air Force/ANG has given me the tools to be an outstanding Airmen and an upstanding citizen, and I intend to make full use of these tools so that I can be the best I can possibly be. These tools will be especially useful as I now hold a lot of responsibility to my name. I will be required to show that I can be a responsible and upstanding person in order to maintain and keep my Top Secret clearance, and that I am to be held responsible for anything that I do or say.

I understand the concern to not grant me the responsibility of having a Firearms ID in 2018. I hope this letter highlights that I have changed as a person from a sixteen year old in High School to a person with a military career in Intelligence/Cyber Intelligence and a person that now has the national trust to safeguard classified information. It is my hopes that you will now consider me for my Firearms ID.

If there is anything further that might need clarification or if there is additional information needed please reach out to me by phone or text at 508-884-6822.

Respectfully Submitted,

A handwritten signature in black ink, appearing to read "Jack D. Teixeira". The signature is written in a cursive style with some loops and flourishes.

Jack D. Teixeira









U.S. Department of Justice
Federal Bureau of Investigation

**DECLARATION OF LUKE CHURCH, SPECIAL AGENT,
FEDERAL BUREAU OF INVESTIGATION**

I, LUKE CHURCH, do hereby declare and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation and have been since August 2022. As a Special Agent, I have received training at the FBI Academy located in Quantico, Virginia, including 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, 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.

2. I am currently investigating the activities of JACK DOUGLAS TEIXEIRA ("TEIXEIRA"), whom I believe 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. I make the following statements based upon my personal knowledge and information made available to me in my official capacity.

3. During the course of my investigation, I have reviewed records lawfully obtained from a social media platform where TEIXEIRA originally posted classified national defense information (the “Social Media Platform”). As described in the Affidavit in Support of an Application for a Criminal Complaint and Arrest Warrant (“Affidavit”) for TEIXEIRA, the Social Media Platform provided the FBI with subscriber information for the user of a particular username that indicated the billing name associated with that username was “Jack Teixeira,” and the billing address associated with that username was a residence I know to be associated with TEIXEIRA.

4. Records from the Social Media Platform reflect that TEIXEIRA sent more than 40,000 messages between November 1, 2022 and April 7, 2023. I have reviewed portions of these records and observed the following interactions between TEIXEIRA and others on the server:

- 23 November 2022:

TEIXEIRA: “I hope isis goes through with their attack plan and creates a massacre at the World Cup”

...

TEIXEIRA: If I had my way I’d kill a fuck ton of people

TEIXEIRA: Bc in all honesty you have to

TEIXEIRA: Whether or not you like it

TEIXEIRA: Seriously I would be forcibly culling the weak minded

- 4 February 2023:

User: Seeing a lot of fed cars sneaking around as well

TEIXEIRA: Like?

User: The usual fedmobile chevies and gmc

TEIXEIRA: See what’s funny is those can be fed cars

TEIXEIRA: but glow[redacted] use dodge caravans ALOT

User: Scary

TEIXEIRA: To make people disappear and shit

...

TEIXEIRA: I've been tempted to buy one and make it an assassination van

...

User: Speaking of caravan

TEIXEIRA: Set up an ar and sniper blind

- 10 February 2023 [soliciting advice for the proper rifle size to operate from the back of an SUV]

TEIXEIRA: . . . i wanted a can on an ar to shoot out of an suv

TEIXEIRA: accurately

...

User: Unless you have the whole passenger area converted for gun activities

User: If so 12.5-14.5 would make sense

TEIXEIRA: w/can?

User: Yeah

User: Cans are important bc it makes it sorta hard to tell where its coming from or what it was

...

TEIXEIRA: well for this it would be a crowded urban or suburban environment

TEIXEIRA: so its essential

User: Would you use it to go through a crowd or nah

TEIXEIRA: the car or the gun?

User: Gun

TEIXEIRA: no

TEIXEIRA: car is parked

TEIXEIRA: window down

TEIXEIRA: stationary or driver

User: Alr

TEIXEIRA: target on a sidewalk or porch

- 18 March 2023:

TEIXEIRA: Yeah I just fuckin hate school

TEIXEIRA: 2nd semester in and I already want to bomb the place

User: Real

User: School sucks shit

User: Just the structure and the campuses and shit

User: All piss me off

TEIXEIRA: I'm going fully online

TEIXEIRA: Bc it's way to far away for me to go in person

TEIXEIRA: Plus fuck college culture

User: Even for a gunsmithing degree the school part of it is just the worst

User: If i lived in a dorm i would firebomb it

TEIXEIRA: Same

TEIXEIRA: Fuck these places

- 30 March 2023:

User: Also I'm now fully convinced SUVs and crossovers serve no fucking purpose

...

TEIXEIRA: The only exception I'll give is Muh Yukons, Escalades, and

suburbans

User: Wagons superior

User: Honestly true SUVs

User: Not the shit we have

TEIXEIRA: They are mobile gun trucks to me

TEIXEIRA: Off-road and good assassination vehicles

- 23 November 2022:

User: Isnt that shit classified

User: ?

TEIXEIRA: everything that ive been telling u guys up to this point has been lol

TEIXEIRA: this isnt different

User: Well

User: You rly trust everyone here then

TEIXEIRA: i have plausible deniability and non of them know anything

incriminating about me

TEIXEIRA: no one has a point of contact to my work

TEIXEIRA: no one knows where i work

TEIXEIRA: and no one knows how to identify me

TEIXEIRA: dw ive thought of that

- 8 December 2022:

TEIXEIRA: that is one page

TEIXEIRA: the entire thing will take up paragraphs of paragraphs

TEIXEIRA: i usually split it up by agency

TEIXEIRA: that portion i posted is from the [REDACTED]

- 13 December 2022:

TEIXEIRA: Since you wanted the full report instead of the brief few summaries I give in [REDACTED] here you go, I've reported stuff like this almost daily as I get it to my friends and have always done it in this format

...

TEIXEIRA: I have not yet done today's

TEIXEIRA: I also omit a decent amount as I don't think it's pertinent and there's just so much of it

TEIXEIRA: Not gonna type out 35 pages of information it's just not happening

TEIXEIRA: So I tailor it and take important parts and include as many details as possible

- 19 March 2023:

TEIXEIRA: Like to thank everyone who came to the thread about the current event, going on and participated and listen to me, cover set event since it's beginning, I was very happy and willing and enthusiastic to have covered this event for the past year and share with all of you something that not many people get to see something very few people in fact, get to see, but despite all of this, I've decided to stop with the updates

...

TEIXEIRA: If you guys do you want happenings that pertain to your country or events or politics or whatever you can DM me and I can tell you what I have, but it's going to always be a brief summary

TEIXEIRA: I can't promise, speed or prompt response, but I will respond to you eventually so offers on the table. If you want to take it until then I'll still be sticking around here still be posting shit, so not going anywhere don't worry about that.

- 6 April 2023:

User: i think your thingies got passed along

User: seeing pro rus telegram with them

TEIXEIRA: Which ones?

User: i screenshotted one can i send?

...

TEIXEIRA: Sure

...

User: is it actually one of them btw?

TEIXEIRA: Not commenting

User: aight

User: ima delete it too

User: did you share them outside of abis?

TEIXEIRA: I think I'm done talking about this
User: ok
TEIXEIRA: Permanently
User: sorry if I pushed you here
TEIXEIRA: It's fine
TEIXEIRA: Just letting u know I'm leaving the server
TEIXEIRA: Don't make a huge deal of it

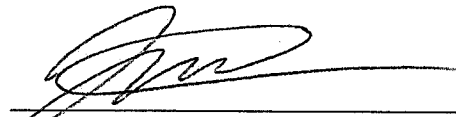
- 7 April 2023:

User: its so over
TEIXEIRA: Ik
TEIXEIRA: Dw about it
...
User: its a pretty dead server anyway
TEIXEIRA: On this note I think it'll be best we head our separate
ways
...
TEIXEIRA: Another thing
TEIXEIRA: If anyone comes looking, don't tell them shit
User: wont
User: wont send any info on your account or screencaps
TEIXEIRA: Pass this on to [User 2, User 3, User 4, User 5] and
most others who were in that thread
...
TEIXEIRA: I mean tell them not to tell anyone
...
TEIXEIRA: Hey u still on?
TEIXEIRA: Whenever you get this, try to delete all my messages
in civil discussions
TEIXEIRA: Especially those not in the thread
User: kk
TEIXEIRA: Wait got an idea
TEIXEIRA: Give me an invite
TEIXEIRA: Then ban me and delete all messages
User: alright
User: gave you access
TEIXEIRA: Ok now do it
TEIXEIRA: It should give an option to delete all messages
User: it only goes to past 7 days
TEIXEIRA: Fuck Alr nvm
TEIXEIRA: Just find stuff from Feb 2022 in civil discussion and
delete it during your free time

5. The interactions described above do not reflect all my knowledge on this matter or all relevant, inculpatory, or violent messages that I observed. They are instead offered to provide the Court with representative sample of certain messages attributable to TEIXEIRA.

* * *

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.



Luke Church
Special Agent, Federal Bureau of Investigation





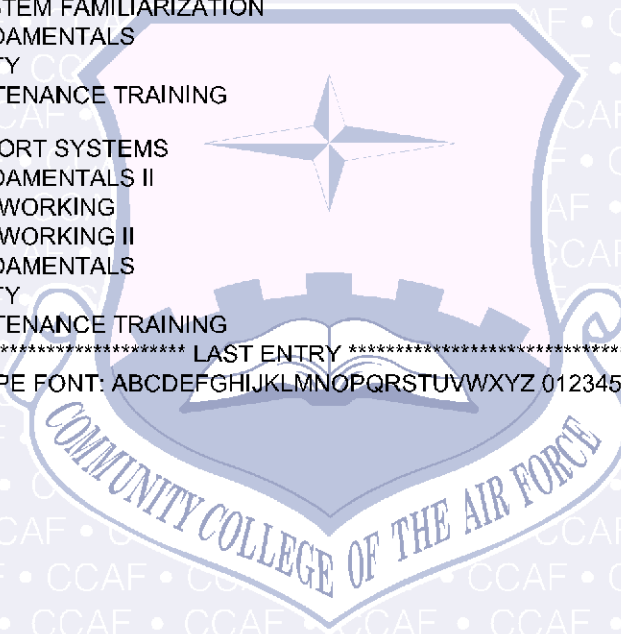
STUDENT NAME: TEIXEIRA, JACK D

JACK TEIXEIRA

STUDENT ID:XXXXX6392
 DOB:21-Dec-XXXX
 SEX:M

REGISTERED FOR 01YY INFORMATION SYSTEMS TECHNOLOGY 15-Nov-2019

AIR FORCE COURSE NO CCAF COURSE CODE	TITLE TITLE	DATE COMPLETED (OR RECORDED) SEM HRS GRADE
MABM9T000 00AC LMM1000	USAF BASIC MILITARY TRAINING BASIC MILITARY STUDIES	LACKLAND AFB 13-Aug-2020 5.00 S
3AQR3D132 02AB	INFORMATION TECHNOLOGY FUNDAMENTALS	KEESLER AFB 16-Feb-2021
IST1102	COMPUTER SYSTEM FAMILIARIZATION	2.00 S
IST1103	NETWORK FUNDAMENTALS	4.00 S
IST1104	CYBER SECURITY	2.00 S
IST1105	GENERAL MAINTENANCE TRAINING	1.00 S
3AQR3D132 01AD	CYBER TRANSPORT SYSTEMS	KEESLER AFB 29-Apr-2021
IST1024	NETWORK FUNDAMENTALS II	3.00 S
IST1025	ADVANCED NETWORKING	5.00 S
IST1026	ADVANCED NETWORKING II	3.00 S
IST1103	NETWORK FUNDAMENTALS	3.00 S
IST1104	CYBER SECURITY	4.00 S
IST1105	GENERAL MAINTENANCE TRAINING	2.00 S



***** LAST ENTRY *****
 ALL VALID ENTRIES ARE IN THIS TYPE FONT: ABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789

Transcript Legend

Air University – Community College of the Air Force

Office of the Registrar

100 South Turner Blvd.

Maxwell AFB-Gunter Annex, AL 36114

registrar.ccaf@us.af.mil

