IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. NATHAN VILAS LAATSCH, Defendant.	Case No. 1:25-mj-325

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT AND ARREST WARRANT

I, Matthew T. Johnson, being duly sworn, depose and state:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), a position I have held since October 2004. 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 matters. As an FBI Special Agent, I have conducted or participated in witness and subject interviews, physical surveillance, service of subpoenas, the execution of search and arrest warrants, the seizure of evidence, including computer, electronic, and e-mail 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. This affidavit is submitted in support of a criminal complaint and arrest warrant for NATHAN VILAS LAATSCH for attempting to transmit national defense information to an

officer or agent of a foreign government, in violation of Title 18, United States Code, Section 794(a).

3. The facts in this affidavit are based on my personal observations, my training and experience, and information obtained from other agents, U.S. Government personnel, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Where I have reported statements made by others, or from documents that I have reviewed, those statements are summarized, unless otherwise noted. When I refer to a specific date or time, I mean to refer to "on or about" such date or time.

4. Pursuant to 18 U.S.C. § 794(a), "Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government . . . or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly . . . any document, writing, . . . note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life . . . ."

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

6. Where such unauthorized disclosure could reasonably result in damage to the national security, the information may be classified as "Confidential" and must be properly

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

7. Sensitive Compartmented Information ("SCI") means classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems.

8. As detailed below, the FBI's investigation to date has revealed that LAATSCH, a current employee of the Defense Intelligence Agency ("DIA"), has passed, and continues to attempt to pass, classified information relating to the national defense of the United States to individuals he believes are agents or officers of a foreign government ("COUNTRY 1").

PROBABLE CAUSE

9. In March 2025, the FBI commenced an operation after the FBI was provided with an email in which an individual—now known to be LAATSCH—offered to provide classified information to COUNTRY 1, a friendly foreign government. In that email, which had the subject line, "Outreach from USA Defense Intelligence Agency (DIA) Officer," the sender wrote, among other things:

> I am an officer of the Defense Intelligence Agency (DIA) serving in a technical role in support of our internal Officer of Security (SEC). The recent actions of the current administration are extremely disturbing to me . . . . I do not agree or align with the values of this administration and intend to act to support the values that the United States at one time stood for.
>
> To this end, I am willing to share classified information that I have access to, which are completed intelligence products, some

> unprocessed intelligence, and other assorted classified documentation.

The email was sent to an email account associated with COUNTRY 1.

10. The user of the email account ("EMAIL ACCOUNT 1") also wrote that he had "intimate knowledge of how DIA tracks and monitors user activity." To communicate further, the sender also provided COUNTRY 1 with a username to an encrypted messaging application (the "Messaging Application") that could be used to contact him (the "MESSAGING ACCOUNT").

11. The EMAIL ACCOUNT 1 user also attached copies of the front and back of two U.S. Government identification cards, which the EMAIL ACCOUNT 1 user said were "images of badges that I use to enter workspaces, with identifying information removed." Based on my training and experience, I know that the images of the two U.S. Government identification cards that the EMAIL ACCOUNT 1 user provided appear to be badges commonly possessed by employees in the U.S. Government and/or the U.S. Intelligence Community (the "U.S. Government IDs").

12. Although the individual's name and photograph were redacted from the images of the U.S. Government IDs that were sent to COUNTRY 1, through other information that was not redacted on one of the U.S. Government IDs, law enforcement was able to determine that the U.S. Government ID belonged to LAATSCH, a DIA employee. As discussed in greater detail below, LAATSCH possesses a Top Secret security clearance and has access to multiple Special Access Programs by virtue of his work in information security for DIA.

13. In addition to the information on the U.S. Government ID that identified LAATSCH as the U.S. Government ID owner and likely user of EMAIL ACCOUNT 1, information provided to law enforcement from the email service provider reflects that EMAIL

ACCOUNT 1 was created by LAATSCH. For example, EMAIL ACCOUNT 1 was established on March 2, 2025, the same day that EMAIL ACCOUNT 1 was used to send the offer to provide classified information to COUNTRY 1. That same day, EMAIL ACCOUNT 1 received an email—which was possibly a test email—from an email address ("EMAIL ACCOUNT 2") that includes LAATSCH's full name. Account information associated with EMAIL ACCOUNT 2 indicates that the user of EMAIL ACCOUNT 2 provided LAATSCH's full name, date of birth, and phone number to set up EMAIL ACCOUNT 2. Additionally, the user of both EMAIL ACCOUNT 1 and EMAIL ACCOUNT 2 logged in from the same IP address, which is associated with LAATSCH's residence, based on information provided to law enforcement.

14. As explained below, upon identifying LAATSCH as the user of EMAIL ACCOUNT 1, the FBI initiated an operation, wherein the FBI assumed the identity of an official from COUNTRY 1 and began communicating with LAATSCH primarily through the MESSAGING ACCOUNT—the Messaging Application username that the user of EMAIL ACCOUNT 1 (*i.e.*, LAATSCH) provided to COUNTRY 1. During the course of those communications, LAATSCH indicated that he had access to multiple repositories containing classified information by virtue of his position with DIA and offered to provide classified information to the individual he believed to be a representative of COUNTRY 1.

15. After several communications over the course of multiple weeks, LAATSCH confirmed that he had exfiltrated classified information from his workplace. Thereafter, the FBI planned a dead drop operation at a public park in Arlington, Virginia, where LAATSCH was to deposit the classified information for COUNTRY 1 to retrieve.

16. On or about May 1, 2025, FBI surveillance observed LAATSCH depart his residence and proceed to the agreed-upon public park. FBI surveillance observed LAATSCH

walk to the specified dead drop location and deposit an item. Following LAATSCH's departure, the FBI retrieved the item, which was a thumb drive later found to contain a message from LAATSCH and nine typed documents, each containing information that was portion-marked up to the Secret or Top Secret levels.

A. NATHAN VILAS LAATSCH

17. NATHAN VILAS LAATSCH is a 28-year-old resident of Alexandria, Virginia. LAATSCH obtained his B.S. in Cyber Security from Florida Polytechnic University in 2018. Based on my training and experience and conversations with other law enforcement officials, I know that an individual with a background in cyber security would be knowledgeable about secure methods of communication, including encrypted emails and messaging services, such as the Messaging Application.

18. Beginning on August 5, 2019, LAATSCH became a civilian employee of the DIA. His current role is as a Data Scientist and IT Specialist of Information Security, and LAATSCH is assigned to a DIA facility in the Washington, D.C. metro area where he works with the Insider Threat Division. Among other things, LAATSCH's duties include enabling user activity monitoring on individuals with access to DIA systems, including individuals who are under investigation. LAATSCH's duties also include assisting external partners, such as law enforcement, on the use of insider threat tools.

19. As required for his assignment at DIA, LAATSCH holds a Top Secret security clearance, which took effect upon his entry on duty to DIA in August 2019. Based on my training and experience in counterintelligence investigations, I know that to acquire his security clearance, LAATSCH would have signed a lifetime binding non-disclosure agreement in which

he would have acknowledged that the unauthorized disclosure of protected information may invoke criminal penalties prescribed by, among other statutes, 18 U.S.C. Sections 793 and 794.

20. In addition to LAATSCH's Top Secret clearance, he maintained access to Special Access Programs ("SAPs"), which are highly compartmentalized classified programs. In the indoctrination memoranda for the SAPs, LAATSCH acknowledged that "the briefing officer has made available Sections 793, 794, 798, and 952 of Title 18 United States Code . . . so that I may read them at this time, if I so choose." LAATSCH signed the SAP indoctrination agreement on September 6, 2022.

21. Based on my training and experience in counterintelligence matters, I also know that, to maintain his security clearance, LAATSCH would have received training on his duty to protect classified materials from unauthorized disclosure. Based on that training, LAATSCH would have been aware that the unauthorized disclosure of Top Secret information reasonably could be expected to cause exceptionally grave damage to the national security of the United States and that the unauthorized disclosure of Secret information reasonably could be expected to cause serious damage to the national security of the United States.

B. FBI Operation

22. On March 23, 2025, using an account on the Messaging Application set up for this purpose, the FBI (the "FBI Agent") sent a message to the MESSAGING ACCOUNT. The message stated: "Good afternoon, I received your message and share your concerns. We are glad you reached out. I look forward to your response and learning more about your work." The user of the MESSAGING ACCOUNT did not immediately respond.

23. On April 4, 2025, using an email account set up for this purpose, the FBI Agent sent a similar message to LAATSCH via EMAIL ACCOUNT 1. On April 14, 2025 at 1:44 p.m.,

LAATSCH, using EMAIL ACCOUNT 1, responded to the FBI Agent and indicated that a response had also been sent on the Messaging Application. At 1:45 p.m., the user of MESSAGING ACCOUNT—who I believe to be LAATSCH—wrote, "Apologies for no response until now[.] I didn't hear anything for a while and had not checked recently[.] What I originally wrote remains true. Arguably more so now."

24. As discussed above, I believe that the user associated with both the MESSAGING ACCOUNT and EMAIL ACCOUNT 1 is LAATSCH. First, LAATSCH's assertion in his first email to COUNTRY 1 that he has "intimate knowledge of how DIA tracks and monitors user activity" is consistent with LAATSCH's responsibilities at DIA. Second, EMAIL ACCOUNT 1 provided the username for the MESSAGING ACCOUNT to COUNTRY 1, and the information associated with one of the U.S. Government IDs that EMAIL ACCOUNT 1 sent to COUNTRY 1 indicates that the user of EMAIL ACCOUNT 1 is LAATSCH. Third, the FBI received information indicating that EMAIL ACCOUNT 1 received an email from EMAIL ACCOUNT 2, which appears to be LAATSCH's personal email account, on the same day EMAIL ACCOUNT 1 was created; that LAATSCH's name, phone number, and date of birth were used to set up EMAIL ACCOUNT 2; and that LAATSCH's home IP address was used to access both EMAIL ACCOUNT 1 and EMAIL ACCOUNT 2. Finally, the April 14, 2025 message from EMAIL ACCOUNT 1 was sent approximately one minute before the message from the MESSAGING ACCOUNT and said, "I have responded on [the Messaging Application]. I am also available here."

25. After receiving LAATSCH's response, on April 17, 2025, the FBI Agent responded to the MESSAGING ACCOUNT, expressing concern to LAATSCH about security and requesting details about the types of information that LAATSCH might be able to share.

Approximately two hours after receiving this message, LAATSCH responded, stating, among other things, that: (1) he possesses a Top Secret//SCI clearance, which allows him "access to a significant amount of information and finished products"; (2) he has access to multiple classified systems; (3) the intelligence he has access to covers multiple categories; and (4) he would need to "copy things manually," which would "somewhat limit[]" what he could provide. LAATSCH went on to say that he could nevertheless provide several products a day.

26. In conclusion, LAATSCH stated, "I've given a lot of thought to this before any outreach, and despite the risks, the calculus has not changed. I do not see the trajectory of things changing, and do not think it is appropriate or right to do nothing when I am in this position."

27. On April 18, 2025, the FBI Agent again emphasized concerns about security and told LAATSCH that "[t]here is much to do together." Approximately four hours later, LAATSCH responded and provided a significant amount of detail on the monitoring and audit capabilities of the DIA and other U.S. Government agencies, including the use of specific programs and how those programs work. Based on my training and experience in counterintelligence matters and discussions with DIA officials, it appears that certain details that LAATSCH provided to the FBI Agent on April 18 are likely classified.

28. LAATSCH then proposed to copy classified materials "by hand . . . to paper." LAATSCH explained that the "majority of products are text only or in text grids or charts that aren't difficult to copy fully" and that he could therefore copy them, "recreate them electronically and distribute to you or an otherwise determined method."

29. On April 22, 2025, the FBI Agent agreed with LAATSCH that manually copying and exfiltrating classified information would be the best way for LAATSCH to proceed. The FBI Agent also asked LAATSCH if he was able to access the Washington, D.C. region.

30. Approximately eight minutes after receiving the FBI Agent's message, LAATSCH confirmed that his workplace was in Washington, D.C. and that he lives approximately "15 minutes from DC."

31. On April 27, 2025, the FBI Agent—who LAATSCH still believed to be a representative of COUNTRY 1—requested that LAATSCH provide "a sample" of the classified information he said he had access to so that it could be reviewed and authenticated. The FBI Agent advised that instructions on where to leave the information would subsequently be provided.

32. Approximately twenty-five minutes after receiving the FBI Agent's message, LAATSCH responded, "Expected this would be coming at some point, understood and will accommodate. I will use my personal computer to digitize what I collect." LAATSCH further stated that he could have the information ready approximately three to four days later.

C. LAATSCH Accesses and Exfiltrates Classified Information

33. During the course of the investigation into LAATSCH, DIA video monitoring in LAATSCH's workplace allowed the DIA to observe LAATSCH's activities. I have reviewed certain portions of the video collected by the DIA and observed that, on April 28, 2025, the day after receiving a request for samples for COUNTRY 1 to review, LAATSCH began reviewing and accessing classified information approximately twenty minutes after entering his office.

34. The videos further show that, over the course of his workday on April 28, 2025, LAATSCH repeatedly wrote on a notepad at his desk while looking at his classified computer system. Based on my review of the DIA videos, it appears that LAATSCH wrote multiple pages of notes, which he then removed from the notepad at his desk and folded into squares. At the

end of his workday, LAATSCH bent under his desk and appears to have placed the folded papers into his socks. LAATSCH departed the office approximately one minute later.

35. On April 29 and April 30, 2025, I similarly observed LAATSCH on the DIA videos accessing classified information on his classified computer system. LAATSCH again wrote information on a notepad at his desk while looking at his classified computer system. On April 29, after transcribing classified information, LAATSCH again removed multiple pages from the notepad, folded the pages into squares, and appears to have placed them in his socks before departing for the day. On April 30, a DIA employee who was monitoring the DIA video in real-time observed LAATSCH place multiple notebook pages in the bottom compartment of his lunchbox. I have also observed photographs of LAATSCH departing his DIA office with what appears to be the same lunchbox later that day.

36. On multiple occasions on both April 29 and April 30, 2025, LAATSCH was observed attempting to hide his notebook when coworkers passed by his desk.

37. On April 30, 2025, approximately three hours after leaving work, LAATSCH sent a message to the FBI Agent stating, "Good afternoon. I have completed gathering the requested products and the drive is ready for drop off. There will be . . . nine in total. Assuming the timing remains for tomorrow it will be feasible."

38. Later that day, on April 30, 2025, the FBI Agent provided information to the user of the MESSAGING ACCOUNT on how to complete the dead drop operation. The FBI Agent advised LAATSCH to proceed to a park located in Arlington, Virginia and provided specific instructions on where LAATSCH could place the drive with the information he had exfiltrated from his workplace. LAATSCH responded approximately thirty minutes later and stated, "Understood. I will let you know when it is done."

39. On April 30, 2025, at approximately 5:36 p.m. (two minutes after LAATSCH sent a message to the FBI Agent), FBI surveillance observed LAATSCH departing his residence. LAATSCH arrived within the vicinity of the dead drop location at the specified Arlington park approximately twenty minutes later, where he was observed viewing a map of the park.

40. The next day, May 1, 2025, an FBI surveillance team again observed LAATSCH departing his residence at approximately 12:36 p.m. LAATSCH proceeded directly to the specified Arlington park.

41. FBI surveillance subsequently observed LAATSCH proceed to the designated location at the specified Arlington park and deposit an object. LAATSCH then returned to his vehicle and drove to his residence.

42. Following LAATSCH's departure, the FBI retrieved a thumb drive from the designated location in the Arlington park, which was subsequently secured and reviewed on a classified system at the FBI. The thumb drive was found to contain a message from LAATSCH and nine typed documents, each containing information that was portion-marked up to the Secret or Top Secret levels.

43. The message from LAATSCH stated, in part:

> I am including his [*sic*] additional document to provide some additional context on the products, selection rationale, and notes having now practically done this.
>
> ***
>
> I choose to include . . . a decent sample size . . . and decently demonstrate the range of types of products. This is not all encompassing, but it should give a good idea.
>
> Whenever possible, I have retained classification markings. This in general applies to the formatting (bolding, italics, etc.) which I have tried to preserve for accuracy. This does not extend to original font, size, and visual embellishments that are sometimes used in original documents.
>
> . . .

> There was no direction provided on topics of interest, so I selected them partially based on assumed interest.
>
> I have to the best of my ability attempted to copy the products by hand, but I cannot guarantee that every single word is completely correct. If there are any mistakes, they would only be a basic word or two, and nothing that would alter the content or meaning of the product.
>
> As anticipated, the process of manually copying by hand will be time-intensive. Many of the provided products took around 40-60 minutes to fully complete, and often two full pages of notebook paper per-product. I did not choose products which were significantly longer than what I've noted as a 'standard' length.

As LAATSCH specified in his cover note, each of the documents on the thumb drive contained classification portion markings.

44. The FBI subsequently sought OCA reviews at one or more U.S. Government agencies. The OCA review(s) confirmed that eight of the nine documents contained on the thumb drive were properly classified as Top Secret and contained Sensitive Compartmented Information.

45. One of those documents, which is classified as Top Secret//SCI reflected sensitive methods of intelligence collection, intelligence related to foreign military exercises, and analysis of the impact of those military exercises.

D. LAATSCH Requests Citizenship from COUNTRY 1

46. After receiving confirmation that the FBI Agent had received the thumb drive, on May 7, 2025, LAATSCH sent a message to the FBI Agent, which indicated LAATSCH was seeking something from COUNTRY 1 in return for his provision of classified information. LAATSCH stated, in relevant part:

> Good afternoon, I'm glad to hear what I provided was satisfactory. As I expect there to be more routine exchanges in the future, I am also interested in what or if there will be any contingencies provided in the event of issues.
> . . .
> With my own credibility now hopefully established, I would like to outline something pertaining to the longer term of this arrangement. I'm [*sic*] not

> mentioned compensation throughout this, as that is not my motivation for doing this . . . . There is though something I am interested in, but can be discussed at the appropriate time.

47. In response, the FBI Agent requested additional details about the nature of the compensation and/or contingencies that LAATSCH was seeking. On May 8, 2025, LAATSCH responded that he was interested in "citizenship for your country" because he did not "expect[] things here to improve in the long term, even in the event there is a change in the future." Accordingly, LAATSCH said that he wanted "to pursue an alternative, despite the clear challenges that would come with it." Although he said he was "not opposed to other compensation," he was not in a position where he needed to seek "material compensation." In conclusion, LAATSCH said he would "reply later" with more thoughts on contingencies and said he could "outline some things base [*sic*] on my understanding of how DIA conducts internal investigations." He promised to "elaborate soon."

48. On May 10, 2025, LAATSCH provided the FBI Agent with additional information on how internal investigations are initiated and managed at DIA, based on his role in working closely with DIA's Office of Security. LAATSCH also explained how he would avoid internal monitoring and stated, "it will not be easy for them, for example, to open a case on me without my knowledge since my permissions to see that would need to be changed and I'd notice." He further discussed the "stupid mistakes" others make when cases are opened on them and said these mistakes "should not be too difficult for me to avoid."

E. LAATSCH Takes Steps to Transmit Additional Classified Information

49. On May 14, 2025, the FBI Agent advised LAATSCH that it was prepared to receive additional classified information. The FBI Agent stated that "to maximize efficiency and impact going forward, I will provide you topics on which to focus your efforts. Topics will

become more specific as we progress, depending on the reports provided . . . ." The FBI Agent then provided LAATSCH with three high-level topics for LAATSCH to focus on. LAATSCH responded later that same day, "Understood, I will begin to work with these topics of focus." LAATSCH said that he should be ready to transmit the information by the week of May 26.

50. The next day, May 15, 2025, approximately fifteen minutes after entering his office, DIA videos captured LAATSCH reviewing classified information on his DIA workstation. Over the course of approximately seven hours, LAATSCH transcribed multiple pages of notes while logged into his classified workstation. LAATSCH then folded multiple pages of notes and again appears to have placed the folded notes inside his socks. LAATSCH departed his desk approximately three minutes later.

51. Between May 16 and May 27, 2025, LAATSCH was repeatedly observed transcribing multiple pages of notes, while logged into his classified workstation at DIA. Each day, at the end of the day, LAATSCH folded the pages of notes and appears to have placed the folded notes inside his socks before departing his office.

52. On May 23, 2025, the FBI Agent advised LAATSCH that it would be prepared to receive additional classified information the following week. LAATSCH responded approximately three minutes later and stated, in pertinent part, "Nothing has changed on my end, I have been collecting on the requested topics, and next week is still good for me." When the FBI Agent later suggested that LAATSCH be prepared to transmit the information on Thursday, May 29, 2025, LAATSCH responded, "That can be done."

CONCLUSION

53. Based on the foregoing, there is probable cause to believe that, between March 2, and May 28, 2025, in Arlington, Virginia, within the Eastern District of Virginia, NATHAN VILAS LAATSCH attempted to transmit national defense information to an officer or agent of a foreign government, in violation of Title 18, United States Code, Section 794(a).

Matthew T. Johnson
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to in accordance with
Fed. R. Crim. P. 4.1, by telephone, on this
28th day of May 2025

William E. Fitzpatrick
United States Magistrate Judge