

UNITED STATES DISTRICT COURT
for the
District of Rhode Island

United States of America
v.

ANDREW MARFO NYAMEKYE

Case No. 1:22-MJ-86PAS

Defendant(s)

CRIMINAL COMPLAINT

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

On or about the date(s) of November 12, 2022 in the county of in the
District of Rhode Island, the defendant(s) violated:

Code Section 18 U.S.C. § 115
Offense Description Influencing, Impeding, or Retaliating Against a Federal Official by Threatening

This criminal complaint is based on these facts:

See the attached Affidavit of Special Agent Thomas Donnelly of the Department of Veterans Affairs, Office of the Inspector General (VA OIG)

Continued on the attached sheet.

Thomas Donnelly (handwritten signature)

Complainant's signature

SA Thomas Donnelly-VA OIG

Printed name and title

Sworn telephonically and signed electronically

Sworn to before me and signed in my presence.

Date: November 16, 2022

City and state: Providence, Rhode Island

Patricia A. Sullivan (handwritten signature)

Judge's signature

Patricia A. Sullivan, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT OF VA OIG SPECIAL AGENT THOMAS DONNELLY

I, Special Agent Thomas Donnelly, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Department of Veterans Affairs, Office of the Inspector General (VA OIG), where I have been employed since June 2021. Prior to joining VA OIG, I was employed as a Special Agent with the Naval Criminal Investigative Service (NCIS) for approximately six years. I am a graduate of the Federal Law Enforcement Training Center's Criminal Investigator Training Program and the NCIS Special Agent Basic Training Program. Prior to NCIS, I served as a uniformed police officer for the Department of Defense and the Department of Veterans Affairs.
2. I am currently assigned to the Manchester, NH Resident Agency of the VA OIG. My duties include, conducting investigations related to threats and numerous other violations of Title 18 of United States Code.
3. During my law enforcement career, I have participated in investigations involving threatening communications.
4. As described below, there is probable cause to believe that ANDREW MARFO NYAMEKYE (DOB: xx/xx/1984) committed a violation of federal law, specifically Title 18 U.S.C. § 115 (Influencing, Impeding, or Retaliating Against a

Federal Official by Threatening), hereinafter referred to as the SUBJECT OFFENSE. Federal employees are further defined under 18 U.S.C. § 1114.

5. I am aware, based on my training and experience, that Title 18, United States Code, Section 115 makes it a federal offense for any person to threaten to assault, kidnap, or murder an employee of any branch of the United States Government on account of their duties. Section 115 also makes it a federal offense for any person to threaten to assault, kidnap, or murder a member of the immediate family of any officer or employee of the United States Government on account of that employee or officer's duties.
6. I submit this affidavit in support of a criminal complaint charging NYAMEKYE with having communicated an interstate threat to kill or harm employees of the Department of Veterans Affairs (VA), Veterans Benefits Administration (VBA).
7. I likewise submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the people, places, and things described in Attachments A-1 and A-2 for evidence as specified in Attachment B. Attachments A-1 and A-2 identifies the following:
 - a. The person of NYAMEKYE; and
 - b. NYAMEKYE's residence of 10 Martha's Way, Centerville, MA (hereinafter the "SUBJECT PREMISES").
8. The things to be searched for and seized, as more fully described in Attachment B, include electronic devices, and physical and electronic records, notes, ledgers,

correspondence, customer lists, call logs, calendars, photographs, work papers, and other evidence of the SUBJECT OFFENSE.

9. The statements contained in this affidavit are based on my participation in this investigation and conversations with other law enforcement officers involved in the investigation. This affidavit is submitted for the limited purpose of establishing probable cause to believe that NYAMEKYE violated 18 U.S.C. § 115. It therefore does not set forth all the information that I and other law enforcement personnel have obtained during the course of the investigation.

NYAMEKYE'S BACKGROUND

10. NYAMEKYE served in the United States Army from 2007 to 2011 as an enlisted soldier. NYAMEKYE's served as an indirect fire infantryman (Military Occupational Specialty 11C) and infantrymen (Military Occupational Specialty 11B). NYAMEKYE completed Airborne School, Emergency Medical Technician Basic Course, and Javelin Missile Training. NYAMEKYE attended the Defense Language Institute for Iraqi Arabic. NYAMEKYE completed the US Army Ranger Indoctrination Program. He served in Afghanistan circa 2009 and earned a Combat Infantryman Badge, among other awards and decorations.
11. After leaving the U.S. Army, NYAMEKYE gained employment with the VBA in Providence, RI circa 2012. NYAMEKYE was terminated circa March 2022 for poor performance. NYAMEKYE is currently a resident of Centerville, MA.

NYAMEKYE COMMUNICATED THREATS VIA TEXT MESSAGE

- 12.** On November 12, 2022, at approximately 0930, NYAMEKYE initiated a group text message with two current employees of the Providence, RI Veterans Affairs Regional Office (VARO) of the VBA. Those employees are identified as “MT” and “JB.” NYAMEKYE’s initial text asked if MT and JB were still employed with VA, to which the pair responded affirmatively. MT is a resident of Massachusetts. JB is a resident of Rhode Island.
- 13.** As background, JB was NYAMEKYE’s first line supervisor when NYAMEKYE was employed by VBA. JB was identified as NYAMEKYE’s supervisor from approximately 2012 to 2015. JB did not maintain contact with NYAMEKYE after NYAMEKYE was terminated in early 2022. MT was identified as one of NYAMEKYE’s coworkers. The pair was hired around the same time and attended training together. MT did not maintain contact with NYAMEKYE and had not seen him in about five years.
- 14.** Later that day, at approximately 15:33, NYAMEKYE texted MT and JB with the statement, “Yea, umm FUCK this racist country.” NYAMEKYE next wrote, “Tell EJ his bitchass better not leave the house this weekend, and that’s a direct threat.” At approximately 17:25, NYAMEKYE again texted MT and JB with, “We will lay in the bushes waiting for the bastards to get home.” JB asked NYAMEKYE if he was “okay,” noting the behavior seemed out of character for

NYAMEKYE. NYAMEKYE responded, "Very much ok, however, you bastards will pay for your treachery as deserved. Rangers Lead the Way!"

15. In an interview with law enforcement on November 14, 2022, both JB and MT stated they personally felt threatened by NYAMEKYE's statements. JB and MT had no information regarding why NYAMKEYE chose them to communicate with.

16. On November 12, 2022, NYAMEKYE began texting a former employee of the VBA identified as "RB." RB was assigned to the Providence, RI VARO of the VBA and is now retired. RB was actively working at VBA when NYAMEKYE was still employed. At approximately 20:15 in the evening, NYAMEKYE texted RB and asked if RB was "still alive." RB responded affirmatively. NYAMEKYE then texted, "Hope you're ready for the civil war" followed by "Tell that red head bitch ["EJM"] he better do his best to restore the Tuskegee airmen to their rightful place or else, and that's a direct threat. Had enough of this racist piece of dirt of a cuntry." RB advised NYAMEKYE he was now retired. This prompted NYAMEKYE to text, "Yea well we don't give a fuck about your retirement buddy, you bastards will still pay for what you've done. We will lay in the bushes waiting for the bastards to get home. And those animal noises they hear might not be animals!"

17. NYAMEKYE then texted RB with, "Yea It's funny until Semtex, Tannerite and rdx are strapped to a drone with your GPS coordinates pro-grammed." RB

intimated he would tell law enforcement if NYAMEKYE committed any of the acts described. NYAMEKYE responded, “Yea we are so so scared of the corrupt racist pigs lol. We forgot all our Army Ranger training. Hope they don’t trip the booby traps and mines.”

18. “EJM” is the current executive director of the Providence, RI VARO. He has been employed in the position since July 2016. As background, the decision to terminate NYAMEKYE from VA employment in early 2022 was ultimately made by EJM.

19. Following the text message exchanges, RB, JB, and MT all notified their supervisors of the threats. These supervisors relayed the information to EJM. EJM contacted the Providence Police Department to advise them of the threat.

20. In an interview with law enforcement, JB stated NYAMEKYE was texting from phone number 508-395-1515. This number was queried in a database commonly available to law enforcement. The results indicated this number was a New Cingular Wireless fully dedicated cellular phone associated to NYAMEKYE. The address on file (10 Martha’s Way, Centerville, MA) matched the address associated with NYAMEKYE’s concealed carry license and residence for VA benefits purposes.

**NYAMEKYE HAS THE MEANS AND TRAINING TO CARRY OUT THE
THREATS**

21. As discussed in paragraph eight, NYAMEKYE has combat experience and extensive training in combat arms. Database checks with the State of Massachusetts indicate NYAMEKYE holds a valid concealed carry license, allowing him to legally carry a firearm in the State of Massachusetts. Additionally, NYAMEKYE is listed as the owner of eight firearms.
22. When interviewed by law enforcement, JB stated he knew NYAMEKYE to own “tactical gear” and firearms. JB also stated he believed NYAMEKYE to be in good physical condition and capable of carrying out the threats.
23. Open-source internet research found a page on “Zola.com.” The page was setup to commemorate a wedding in April 2022. A brief biography and picture of each member of the wedding party was included. NYAMEKYE’s name and picture appear on the page, under which is written, “Former Army vet has more drones than the NSA.”
24. NYAMEKYE referenced using a drone laden with Semtex, RDX, and Tannerite to conduct an attack. Semtex is a plastic explosive used for both commercial and military purposes. RDX is a type of military high explosive. Both Semtex and RDX are highly regulated and restricted explosives. Tannerite is a binary explosive widely available for civilian purchase; no explosives license is required to purchase the substance. Tannerite is sold as two separate compounds that are

not explosive by themselves. When mixed together and shot with a high-velocity bullet, Tannerite explosively detonates.

25. In addition to referencing the use of drones, NYAMEKYE is currently taking flight lessons. NYAMEKYE does not yet hold a valid private pilot's license at this time but has access to aircraft.
26. On November 12, 2022, local law enforcement in the vicinity of Centerville, Massachusetts conducted a welfare check at the SUBJECT PREMISES based on the aforementioned threats. Upon arriving at the SUBJECT PREMISES, NYAMEKYE refused to come out of his bedroom and speak to law enforcement for the first twenty minutes, instead sending his wife to speak as an intermediary without opening the door. After being told that they needed to see him to ensure his well-being, NYAMEKYE instead stood at the top of a staircase visible from the front door window. NYAMEKYE informed a responding officer that he sent the aforementioned messages because he is upset how the VA is treating him and others. NYAMEKYE informed officers that he was fine, and local officers concluded their welfare check.

SEIZURE OF COMPUTER EQUIPMENT AND DATA

27. As described above and in Attachment B, this application seeks permission to search for records that might be found in the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data

stored on a phone, tablet, or computer's hard drive or other storage media.

Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

28. Probable cause. I submit that if a tablet, phone, or computer or other storage medium is found in the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

29. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

30. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

31. Wholly apart from user-generated files, computer storage media – in particular, computers’ internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
32. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
33. Based on actual inspection of other evidence related to this investigation, namely messages received by JB, MT, and RB from NYAMEKYE, I am aware that computer equipment with messaging capabilities was used to send the messages by which NYAMEKYE outlined his threats. Based on my training and experience, SMS or iMessages can be sent via variety of devices, including phones, tablets, or personal computers. There is reason to believe that such devices are currently located in the SUBJECT PREMISES.
34. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence

that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

- 35.** Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- 36.** As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information

stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its

file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

37. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
38. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators.

Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

39. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
40. Necessity of seizing or copying entire computers or storage media. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

41. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

42. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data in the SUBJECT PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

43. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.
44. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

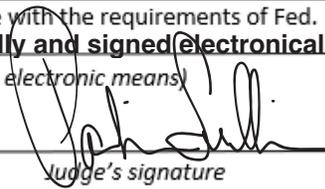
CONCLUSION

45. Based on these facts, I submit there is probable cause to believe that Andrew NYAMEKYE knowingly threatened employees of the United States Government on account of their duties in violation of 18 U.S.C. § 115. I likewise submit that there is probable cause to believe that evidence, fruits, and instrumentalities of this crime, as described in Attachment B, are contained within the premises described in Attachments A to the proposed search warrants for the SUBJECT PREMISES and NYAMEKYE's person.

46. I declare the foregoing is true and correct to the best of my knowledge and belief.



THOMAS DONNELLY
SPECIAL AGENT, VA OIG

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 <u>by</u> Sworn telephonically and signed electronically <i>(specify reliable electronic means)</i>	
November 16, 2022 <hr/> <i>Date</i>	 <hr/> <i>Judge's signature</i>
Providence, Rhode Island <hr/> <i>City and State</i>	Patricia A. Sullivan, USMJ <hr/> <i>Magistrate Judge Patricia A. Sullivan</i>