IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEIZURE OF DOMAIN NAMES JUSTICEHOMELAND.ORG; KARMABELOW80.ORG; HANDALA-HACK.TO; AND HANDALA-REDWANTED.TO	**Case No.** 1:26-mj-0683-CDA 1:26-mj-0684-CDA **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, [redacted], being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a seizure warrant for domain names justicehomeland.org (**SUBJECT DOMAIN NAME-1**), handala-hack.to (**SUBJECT DOMAIN NAME-2**), Karmabelow80.org (**SUBJECT DOMAIN NAME-3**), and handala-redwanted.to (**SUBJECT DOMAIN NAME-4**) (collectively the "**SUBJECT DOMAIN NAMES**") pursuant to 21 U.S.C. § 853(f) and 18 U.S.C. §§ 982(a)(2) and 1030(i) and (j) because they are being used in and/or intended to be used in facilitating and/or committing violations of the following federal laws: 18 U.S.C. §§ 371 (conspiracy); 1030(a)(5)(A) ("knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization, to a protected computer"[1]); 1030(a)(2)(C) (obtaining information from a protected computer through unauthorized access); 1030(b)

[1] A "protected computer" is defined, in relevant part, as a computer "used in or affecting interstate or foreign commerce or communications, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications of the United States." 18 U.S.C. § 1030(e)(2).

(conspiracy); 1028(a)(2), (3), (6), and (7) (fraud and related activity in connection with identification documents, authentication features, and information); 1028(f) (conspiracy); and 1349 (wire fraud conspiracy) (collectively the "SUBJECT OFFENSES"). This application seeks a seizure warrant because the **SUBJECT DOMAIN NAMES** could be placed beyond process, modified, moved, or deleted, if not seized by warrant.

2. I am a Special Agent with the FBI and have been so since [redacted] I am currently assigned to the Baltimore Division of the FBI, National Security Cyber Squad, where I investigate computer crimes, including computer intrusions.

3. I have received training, and gained experience, in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer evidence identification, computer evidence seizure and processing, social media analysis, and various other criminal laws and procedures. I also have training and experience in conducting cyber-related investigations. I am well-versed in the execution of federal search warrants and seizures and in the identification and collection of computer-related evidence. I am an "investigative or law enforcement officer" of the United States within the meaning of 18 U.S.C. § 2510(7) who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Titles 18 and 21 of the United States Code.

4. The facts and information contained in this Affidavit are based upon my personal knowledge of the investigation, observations of other law enforcement officers and agents involved in this investigation, and information provided by known sources of information. All observations referenced below that I did not personally make were related to me by the persons who made such observations. Moreover, 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.

5. As set forth below, there is probable cause to believe that the **SUBJECT DOMAIN NAMES** are subject to seizure and forfeiture pursuant to 18 U.S.C. § 1030(i) and (j) because they are property used, or intended to be used, to commit or facilitate violations of the SUBJECT OFFENSES. Thus, the **SUBJECT DOMAIN NAMES** are subject to seizure and forfeiture pursuant to 21 U.S.C. § 853(f) and 18 U.S.C. §§ 982(a)(2) and 1030(i) and (j) because the individuals responsible for committing the SUBJECT OFFENSES are using or intending to use these facilities to commit or to facilitate the commission of the SUBJECT OFFENSES. I make this affidavit for a warrant to seize the property described in Attachment A-1 and A-2, specifically, justicehomeland.org and Karmabelow80.org (originally sold by the Public Domain Registry, headquartered in Reston, Virginia), and handala-hack.to and handala-redwanted.to (originally sold by NameCheap, headquartered in Phoenix, Arizona). The procedure by which the government will seize the **SUBJECT DOMAIN NAMES** is described in Attachments A-1 and A-2 and below.

II. JURISDICTION AND VENUE

6. As described below, in March 2024, a Telegram channel operated by a group that called themselves "Handala Hack" leaked a list containing the names of two [redacted] executives. [redacted] is a U.S. defense technology firm based in [redacted], Maryland. Handala Hack's post stated its followers should target these individuals. To assist its followers with "targeting" these victims, the post only provided the victims' names and their [redacted], Maryland-based employer. Based on my training and experience, I believe the Handala Hack team

wanted their followers to use this information to target their victims a[redacted]

7. In March 2025, the FBI in Maryland, acting in an undercover capacity, purchased a large database from a group calling themselves "Homeland Justice" (alternatively "Justice Homeland"), who claimed responsibility for the July 15, 2022, and September 9, 2022, cyber-attacks on the government of Albania.

8. In March 2026, the FBI responded to a hack targeting [redacted]. Shortly after the hack, Handala Hack made a post on **SUBJECT DOMAIN NAME-2** claiming credit for the intrusion. In a precaution in response to the hack, hospitals throughout the District of Maryland suspended their connection to [redacted] – a system that helps hospitals analyze [redacted] data and other information related to patient vitals. Furthermore, [redacted] has reported that the work computer of one of its Maryland-based employees was wiped as a result of the cyberattack by Handala Hack and that the employee had to have the work computer restored.

9. As further illustrated below, based on multiple sources, the same actors that call themselves Homeland Justice, also operate the aliases "Handala Hack," and "Karma Below." As a result, I have probable cause to believe that Justice Homeland, Handala Hack, and Karma Below are part of the same conspiracy because they are operated by the same individuals.

10. The threats made by Handala Hack targeted individuals based in the District of Maryland, the data purchased by the FBI in the District of Maryland from Homeland Justice came from the 2022 cyber-attacks targeting the government of Albania, and Handala Hack's targeting of [redacted] also impacted hospitals and patients throughout the District of Maryland. Thus, I believe

venue over the suspected offenses – perpetrated by this same threat actor group using various aliases – is proper. *See* 18 U.S.C. § 3237(a).

11. There is probable cause to believe that the **SUBJECT DOMAIN NAMES** are subject to seizure and forfeiture pursuant to 18 U.S.C. §§ 1030(i)(1)(A) and (j)(1) as personal property that was used, or intended to be used, to commit or to facilitate the commission of a conspiracy to violate, and violations of, § 1030. 18 U.S.C. § 1030(i)(1)(A) provides in relevant part:

> (1) The court, in imposing sentence on any person convicted of a violation of [18 U.S.C. § 1030], or convicted of conspiracy to violate [18 U.S.C. § 1030], shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States –
>
> > (A) such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation . . .."

12. 18 U.S.C. § 1030(j)(1) specifies that "for the purposes of [18 U.S.C. § 1030(i)], the following shall be subject to forfeiture to the United States and no property right shall exist in them: (1) [a]ny personal property used or intended to be used to commit or to facilitate the commission of any violation of [18 U.S.C. § 1030], or a conspiracy to violate [18 U.S.C. § 1030]."

13. Section 1030(i)(2) also provides that "criminal forfeiture of property under [18 U.S.C. § 1030], any seizure and disposition thereof, and any judicial proceedings in relation thereto, shall be governed by [21 U.S.C. § 853], except for subsection (d) of that section." 18 U.S.C. § 1030(i)(2).

14. Forfeiture based on 18 U.S.C. §§ 1030(i)(1)(A) and 1030(j)(1) allows for forfeiture and seizure of property used to facilitate any computer fraud crime, including a domain name. 21 U.S.C. § 853 specifically defines "property subject to criminal forfeiture under this section" to

include "tangible and intangible personal property, including rights, privileges, interests, claims and securities." *See* 21 U.S.C. § 853(b)(2).

15. 21 U.S.C. § 853(l) provides that "[t]he district courts of the United States shall have jurisdiction to enter orders as provided in this section without regard to the location of any property which may be subject to forfeiture under this section, or which has been ordered forfeited under this section."

16. 21 U.S.C. § 853(j) provides that venue for criminal forfeitures brought under this section lies in the district where the defendant owning the criminal forfeiture is located or in the judicial district where the criminal prosecution is brought.

17. To protect the ability of the United States to exercise its right of forfeiture, 21 U.S.C. § 853(e) empowers district courts to enter restraining orders and injunctions to preserve the availability of property that is subject to forfeiture under Section 853(a), respectively. However, if there is probable cause to believe that the property to be seized is subject to forfeiture and that an order pursuant to Section 853(e) may not be sufficient to assure its availability for forfeiture, a district court may issue a warrant authorizing the seizure of such property. 21 U.S.C. § 853(f). Section 853(f) provides that:

> The Government may request the issuance of a warrant authorizing the seizure of property subject to forfeiture under this section in the same manner as provided for a search warrant. If the court determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that an order under subsection (e) may not be sufficient to assure the availability of the property for forfeiture, the court shall issue a warrant authorizing the seizure of such property.

18. 18 U.S.C. § 982(b)(1) authorizes the issuance of a criminal seizure warrant under 21 U.S.C. § 853(f), which provides in relevant part that a seizure warrant for property subject to

forfeiture may be sought in the same manner in which a search warrant may be issued. A court shall issue a criminal seizure warrant if it determines that the property to be seized would, in the event of a conviction, be subject to forfeiture and that a restraining order would be inadequate to assure the availability of the property for forfeiture.

19. Neither a restraining order nor an injunction, with or without notice, is sufficient to guarantee the availability of the **SUBJECT DOMAIN NAMES** for forfeiture. These civil processes require notice and party compliance. Because the Ministry of Intelligence and Security ("MOIS") is an organ of the Islamic Republic of Iran and the individuals responsible for the **SUBJECT DOMAIN NAMES** are already violating U.S. law, it is unlikely that the potential defendants, which the FBI is still in the process of identifying, will comply with an order from this Court. Moreover, in response to such an order, the MOIS may simply remove or destroy the information the United States is trying to seize. It will then shift these criminal activities to other domains.

20. There is no expectation that those responsible for the **SUBJECT DOMAIN NAMES** would appear for an (expedited) hearing on a temporary restraining order given their overt and consistent efforts to mask their actions, which already violate U.S. law. Additionally, the information and statements on these domains are part of a continuing offense that victimizes the individuals who have been threatened and whose PII is publicly available. Temporarily removing or seizing this website is insufficient because once the temporary period ends the threats and sensitive information presently on the **SUBJECT DOMAIN NAMES** will be publicly displayed again.

21. Only by seizing and forfeiting the **SUBJECT DOMAIN NAMES** and redirecting the traffic to websites controlled by the government, can the Government prevent third parties from acquiring the domain names and using them to continue to commit the SUBJECT OFFENSES. Furthermore, seizure of the **SUBJECT DOMAIN NAMES** will prevent third parties from continuing to access the **SUBJECT DOMAIN NAMES** in their present form.

III. DEFINITIONS AND TERMS

22. Internet Protocol Address: An Internet Protocol address (IP address) is a unique numeric address used by computers on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address – it enables computers connected to the Internet to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by Internet Service Providers ("ISPs").

23. Domain Name: A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond with a particular IP address. For example, "usdoj.gov" and "cnn.com" are domain names.

24. Domain Name System: The domain name system ("DNS") is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or "labels," that are delimited by periods, such as "www.example.com." The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or

subdomain, of the domain on the right. The right-most label conveys the "top-level" domain. For example, the domain name "www.example.com" means that the computer assigned that name is in the ".com" top-level domain, the "example" second-level domain, and is the web server.

25. Domain Name Servers: DNS servers are computers connected to the Internet that convert, or resolve, domain names into Internet Protocol ("IP") addresses.

26. Registry: For each top-level domain (such as ".com"), there is a single company, called a "registry," that determines which second-level domain resolves to which IP address. For example, the registry for the ".com" and ".net" top-level domains are VeriSign, Inc., which has its headquarters at 12061 Bluemont Way, Reston, Virginia.

27. Registrar & Registrant: Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchasers of the domain name. The individual or business that purchases, or registers, a domain name is called a "registrant." Registrants control the IP address, and thus the computer, to which their domain name resolves. Thus, a registrant may easily move a domain name to another computer anywhere in the world. Typically, a registrar will provide a registrant with the ability to change which IP address a domain or computer resolves to through an online interface. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

28. Whois: A "Whois" search provides publicly available information as to which entity is responsible for a particular IP address or domain name. A Whois record for a particular IP address or domain name will list a range of IP addresses that that IP address falls within and

the entity responsible for that IP address range and domain name. For example, a Whois record for the domain name XYZ.COM might list an IP address range of 12.345.67.0- 12.345.67.99 and list Company ABC as the responsible entity. In this example, Company ABC would be responsible for the domain name XYZ.COM and IP addresses 12.345.67.0- 12.345.67.99.

IV. PROBABLE CAUSE

29. On or about July 15, 2022, the government of Albania reported that multiple government computer systems (hereinafter, the "Targeted Computer Servers") were targeted by an ongoing, large-scale cyber-attack. The attack resulted in multiple Albanian government computer servers being taken offline and the loss of significant amounts of sensitive data from those servers. According to open-source reporting, the cyber-attack entailed multiple phases between approximately May 2021 and August 2022, including: (1) probing the Targeted Computer Servers' infrastructure for vulnerabilities; (2) exploiting those vulnerabilities in order to infiltrate the Target Computer Servers and exfiltrate data; (3) implementing ransomware and destructive malware designed to delete data from the Targeted Computer Servers; and (4) acting without authorization to disclose data from the Targeted Computer Servers on the internet for the stated purpose of intimidating government personnel and forcing political change.

30. In response to the cyber-attack, the FBI deployed personnel to Albania to assist with incident response, data recovery, and technical analysis. The FBI investigation verified the attack timeline and offered additional insights into how the attack took place. According to FBI technical analysis of the Targeted Computer Servers, the attackers likely acquired initial access to the Government of Albania's computer network on or about May 2021 via exploitation of an internet facing Microsoft SharePoint server. The attackers maintained continuous network access

after that point, periodically accessing and exfiltrating e-mail content and other materials from the servers. In or about May 2022, the attackers shifted towards an "attack posture." During this phase, the attackers scanned the Targeted Computer Servers for additional vulnerabilities, tested accesses, and sought additional accesses in preparation for the destructive phase of the attack. On or about July 15, 2022, the actors initiated a destructive attack against the Targeted Computer Servers, employing a ransomware style attack coupled with a disk-wiping utility.

31. At the time of the cyber-attack, the Targeted Computer Servers contained, among other things, communications between Albanian government officials and U.S. government officials about various diplomatic, national security, and intelligence matters. These communications were among the information that was exfiltrated from and destroyed on the Targeted Computer Servers during the attack.

32. During and after the attack, a group calling themselves "Homeland Justice" and alternatively "Justice Homeland," claimed credit for the attack online. Homeland Justice posted a video on its website – initially homelandjustice.ru, then www.homelandjustice.top, then www.homelandjustice.cx, and now justicehomeland.org (**SUBJECT DOMAIN NAME-1**) – of the ransomware being executed, and it published images of documents ostensibly belonging to Albanian government organizations. **SUBJECT DOMAIN NAME-1** currently hosts this information. Based on the ransomware message that was used and information posted online by Homeland Justice, the motivation for the attack appears to be the Albanian government's decision to support an Iranian dissident group called Mujahedeen e-Khalq or "MEK." MEK has, in the past, openly advocated for the overthrow of the Iranian government.

A. **The Aliases Justice Homeland, Handala Hack, and Karma Below Are Operated as Part of the Same Conspiracy**

33. In the public domain, the threat actor group that uses the cyber persona "Homeland Justice/Justice Homeland" is known by various commercial cyber security firms and cyber security researchers as "Banished Kitten," "Void Manticore," "Dune," "Red Sandstorm" and other names to attribute and describe their activity. Each commercial cyber security firm often creates its own unique naming convention to track malicious cyber activity perpetrated by the same group. Other cyber personas that have been linked to the same actor group as "Homeland Justice/Justice Homeland" are "Karma Below" and "Handala Hack."[2] According to open-source reporting conducted by cybersecurity and threat intelligence firms, [redacted] "Handala Hack," "Karma Below," and "Homeland Justice/Justice Homeland" are [redacted] operated by [redacted] Iran's MOIS.

34. Publicly available research [redacted] identified Homeland Justice, Handala Hack, and Karma Below as interconnected personas belonging to the same coordinated Iranian MOIS actors. As one example, [redacted] the Homeland Justice entity that hacked the Government of Albania in 2022 (described above) was the same as Handala Hack and Karma Below because all three actors

[2] A cyber persona is a moniker usually created by the threat actor itself to broadcast or claim responsibility for its malicious cyber activity.
[3] *See* https://research.checkpoint.com/2024/bad-karma-no-justice-void-manticore-destructive-activities-in-israel/
[4] *See* https://www.kelacyber.com/blog/handala-hack-telegram-breach-israeli-officials/
[5] *See* https://x.com/NarimanGharib/status/1829856651769250017

conducted virtually identical hacking activity and psychological operations targeting enemies of Iran.[6] In the case of Handala Hack and Karma Below, [redacted] observed incidents in which Karma Below claimed credit for hacking activity on a victim's systems (for example a ransom note) but then stolen data was ultimately posted on Handala Hack's website. [redacted] it evaluated hacks conducted by Karma Below and Homeland Justice and found identical [redacted] used by both entities in their hacks [redacted].

35. [redacted] the 2022 Albania hack and subsequent targeting of Israeli entities between 2023 and 2024 [redacted] used the same unique attack method (CVE-2019-0604 (a naming convention for a vulnerability, like a serial number)).

36. [redacted]

[6] *See* https://research.checkpoint.com/2026/handala-hack-unveiling-groups-modus-operandi/

37. As set forth more fully below, the conspiracy perpetrated by the Iranian MOIS actors includes among its objectives the fraudulent destruction and theft of identity information and means of authentication as well as the fraudulent and intentional access of computers without authorization to damage those computers, and information held on the computers. The conspiracy is continuous, ongoing, and has affected individuals globally and in Maryland as recently as last week.

38. In summary, these groups are widely attributed to a specific cyber unit within Iran's MOIS, tracked by researchers under monikers such as Void Manticore (Check Point), Storm-0842 (Microsoft), and Banished Kitten (KELA). This unified state control is evidenced by significant overlaps in technical infrastructure and shared Tactics, Techniques, and Procedures (TTPs). For example:

a. Shared Infrastructure: The leak sites and Telegram bots for each persona have been traced back to the same backend servers and Iranian IP ranges.

b. Destructive Tooling: The groups deploy similar custom-built malware, including the BiBi Wiper—a destructive tool named after Israeli Prime Minister Benjamin Netanyahu.

c. Psychological Operations: Each persona is used to amplify the impact of breaches through "faketivist" influence operations, including data leaks and high-volume SMS "bombing" campaigns designed to harass and intimidate citizens.

d. Geographic Specialization: While sharing resources, the personas are often deployed for specific theaters. Homeland Justice typically targets Albanian infrastructure, while Karma Below and Handala focus on high-value targets within Israel.

B. **Implanting Malware on [redacted] System**

39. [redacted] a Journalist for [redacted] a United Kingdom-based Farsi language news organization, was contacted by a Telegram account [redacted]

40. The FBI analyzed the file and determined it was the first stage of a malware. When the file was activated, it would download additional stages from a malicious endpoint. Based on my training and experience, malicious cyber actors often masquerade malware as a popular program, so an unsuspecting victim is more likely to download and open the file, thus infecting the victim's device. A subsequent stage of the malware downloaded a file titled "RuntimeSSH.exe." [redacted]

[7] [redacted]

[redacted]

41. The Government obtained domain registration records for the Handala Hack domain, handala.to, from Namecheap. These records show that on or about December 12, 2023, the registrant of the domain handala.to deposited Litecoin to a Namecheap address through the cryptocurrency payment processor BitPay.

42. Blockchain analysis indicates that the Litecoin used for this payment originated from a cryptocurrency wallet attributed to [redacted] an automated cryptocurrency exchange service based in Hong Kong and registered in St. Kitts and Nevis. [redacted] facilitates cross-chain swaps (e.g., Bitcoin to Litecoin) without requiring users to operate accounts on multiple platforms. Further analysis of [redacted] transaction records show that prior to purchasing **SUBJECT DOMAIN NAME-2** with Litecoin, a [redacted] user received cryptocurrency from several virtual asset service providers (VASPs), including Ramzinex. Ramzinex is a prominent Iranian cryptocurrency exchange headquartered in Tehran. Blockchain tracing therefore demonstrates that funds used to purchase the domain were sourced, through intermediary transactions, from an Iranian cryptocurrency exchange. The deliberate use of multiple cryptocurrency conversions and intermediary transfers reflects an effort to obfuscate the original source of funds used to facilitate the underlying criminal scheme.

C. March 2025 Undercover Purchase of Data from Homeland Justice

43. On or about February 25, 2025, an FBI employee acting in a covert capacity engaged the "Homeland Justice" persona via the Telegram social messaging application to obtain a copy of data that persona claimed to possess. On February 26, 2025, the Homeland Justice

[8] [Host Name] is the redacted device name that was disseminated in the Telegram message.

persona responded and claimed to possess "…e-albania and other databases covering Albanian ID cards and other sensitive information" and offered the information for sale. On March 1, 2025, the Homeland Justice persona said "…the information for sale contain much more sensitive information than the free stuff we have posted publicly." This conversation is illustrated in the following screenshot of the text message chain:

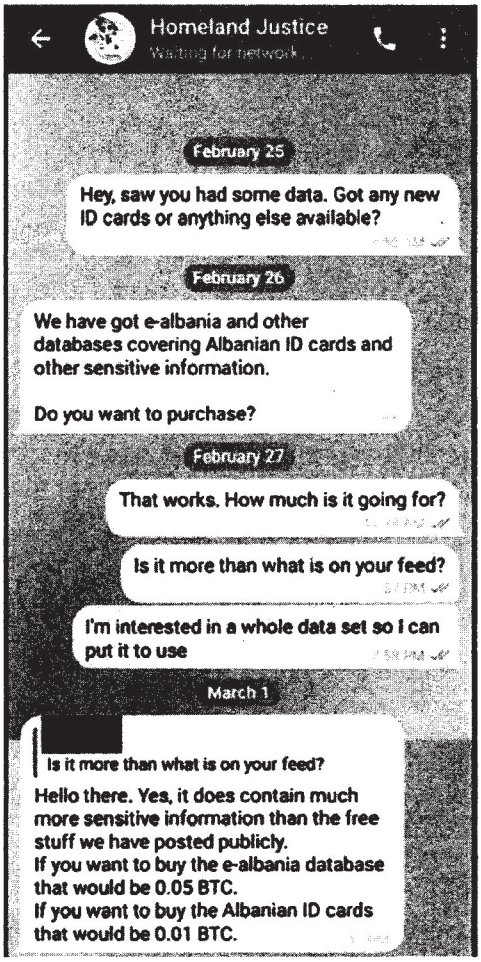


Figure 1: February 25-26, 2025, Chat with Homeland Justice Persona. The identifier used by the FBI employee was redacted.

44. Based on the characteristics of the data that was stolen from the 2022 Albanian data breach, and the fact that an alias with the name "Homeland Justice" was trying to sell this data,

there is probable cause to believe that the data purchased includes data taken from Albanian government computers during the July 15, 2022 and September 9, 2022 cyber-attacks.

45. As a result of the text messages, on or about March 4, 2025, the Homeland Justice persona sold a database to an FBI employee acting in a covert capacity and located in the district of Maryland. A review of the database sold to the FBI employee indicated it contained [redacted] Albanian national ID numbers, names, dates of birth, addresses, and other sensitive personally identifiable information (PII). The resulting information exposed Albanian citizens' sensitive PII, which could be used to steal identities.

D. **Heavygram-KeePass-Malware**

46. [redacted]

Between [redacted] and [redacted]

48. [redacted]

49. On or about [redacted] the FBI notified US VICTIM-1, a resident of [redacted], that malware believed to be associated with an Iranian intelligence service may have infected US VICTIM-1's laptop and/or desktop computer. On or about [redacted], US VICTIM-1 consented to an FBI examination of the affected devices. Upon forensic examination, the FBI observed several suspicious files that included RuntimeSSH.exe (hereinafter the "Heavygram-RuntimeSSH.exe-Malware") and winappx.exe (hereinafter the "Heavygram-Winappx.exe-Malware"). Both programs used file names that attempted to make a user think they were standard computer programs. The Heavygram-RuntimeSSH.exe-Malware masqueraded as a Powershell program[9], and the Heavygram-Winappx.exe-Malware masqueraded as Windows Remote desktop

[9] A PowerShell program refers to a script or set of commands written in the PowerShell scripting language, designed to manage and control nearly every aspect of an operating system and its integrated applications.

software.[10] The FBI's analysis also revealed that a file named "RuntimeSSH" was part of the second stage of the Heavygram malware [redacted]

50. [redacted]

E. [redacted]

51. On or about July 8, 2025, Confidential Source-3 shared with the FBI that the Handala Hack Telegram channel posted a message where Handala Hack claimed responsibility for hacking [redacted] Confidential Source-3 indicated Handala Hack hacked the [redacted]

52. In September 2025, a trusted partner shared information with the FBI that contained details about a set of posts made on the Handala Hack website, handala-hack.to (**SUBJECT**

[10] Windows Remote desktop software allows a user to connect to and control a computer from a different physical location, as if they were sitting directly in front of it. To enable remote connections on the host PC, the host must turn on the feature in the system settings and ensure the computer is powered on and connected to the network.

DOMAIN NAME-2). [redacted]

[redacted] The FBI performed open-source research and corroborated Handala Hack made these posts on [redacted], which are illustrated below:

53. In the same posts, Handala Hack included a screen shot of [redacted] from [redacted] perspective. The screen shot illustrated [redacted] the alleged meeting [redacted] The screenshot included the superimposed text "www.handala-hack.to" in red letters.

54. Based upon my training and experience, in this [redacted]. Handala Hack actors illustrated their ability to exfiltrate data from [redacted] computer, [redacted] As a result, I have probable cause to believe the perpetrators gained access to [redacted] computer via a Heavygram malware infection that targeted [redacted] computer as described above.

F. **Hack of [redacted]**

55. On March 11, 2026, Handala Hack, via the Handala-hack[.]to domain, claimed credit for hacking [redacted] – a major American multinational medical technologies firm based in [redacted]. The Handala Hack persona claimed the hack was retaliation for "ongoing cyber assaults against the infrastructure of the Axis of Resistance." The Handala Hack persona

claimed the operation extracted [redacted]

[redacted] Below is part of the post Handala Hack placed on the Handala-hack[.]to domain:

[redacted]

56. [redacted] has provided information through counsel to the FBI regarding a [redacted] victim of the Handala Hack cyberattack. On [redacted] contacted [redacted] to notify the company that the employee's work computer had been wiped. In fact, on March 16, 2026, the affected [redacted] have information restored to the computer.

57. On March 11, 2026, [redacted] issued an internal memo that the cyber-attack on [redacted] had a direct impact on emergency medical services ("EMS") and hospitals within Maryland. [redacted] reported that certain

[redacted] computer systems may have been affected by a "global network disruption," which prompted some hospitals to temporarily suspend their connections to [redacted] The [redacted] Protocols for EMS require the transmission [redacted] enable timely clinical decision-making. As a result of the disruption to [redacted] systems, [redacted] clinicians were instructed to rely on radio consultation and verbal description [redacted] This disruption to required clinical communication systems demonstrates that the cyber-attack on [redacted] in some cases interfered with the delivery of emergency medical care in Maryland hospitals.

G. **handala-redwanted.to**

58. On or about October 29, 2025, investigators learned of the domain handala-redwanted.to ("**SUBJECT DOMAIN NAME-4**"). Open-source research indicates handala-redwanted.to and handala-hack.to are likely operated by the same actors. A query of handala-hack.to generated an article titled "Ignite Chaos at Your Own Risk: [redacted]." The article included the same logo as the handala-redwanted.to website, and the website listed beneath the logo was handala-hack.to. In November 2025, handala-hack.to posted "wanted" reports on behalf of handala.redwanted.to. The reports provided photos of Israelis that Handala considered "wanted" and listed a reward amount for the individuals' apprehension. Furthermore, the handala-hack.to website noted Handala would unveil a new chapter in exposing those complicit in the

machinery of the Zionist regime through their Handala/Redwanted platform. The screenshot also provided the link for handala-redwanted.to, connecting both sites to one another.

H. Karmabelow80.org

59. The group Karma Below is associated with the website karmabelow80.org ("**SUBJECT DOMAIN NAME-3**"). Information obtained during my investigation indicates Karma Below is a persona used by Iranian MOIS to claim responsibility for destructive cyberattacks, primarily targeting Israeli organizations. It is linked to Handala Hack and Homeland Justice through shared infrastructure, centralized command within MOIS, and a common operational "playbook." Open-source research of the karmabelow80.org website illustrated what appeared to be malicious cyber activity against Israeli entities, including claims of hacking the [redacted], Israeli police websites, and [redacted] data infrastructure.

I. Handala Hack Used the SUBJECT DOMAIN NAMES and Associated Accounts to Issue Death Threats and Dox Iranian Dissidents and Government Adversaries

60. Handala Hack has used, and continues to use, internet domains associated with the group to publish data obtained through unauthorized hacking and exploitation activities. After obtaining sensitive information from compromised systems and illicitly accessed accounts, Handala Hack posts this information on publicly accessible websites under the actor's control, namely **SUBJECT DOMAIN NAME-2** and **SUBJECT DOMAIN NAME-4**. **SUBJECT DOMAIN NAME-2** also mirrored information that was posted on the Handala Hack telegram channel. The material published on these domains included personally identifiable information (PII) associated with targeted individuals, such as names, addresses, telephone numbers, employment information, and other private data. The domains function as platforms for the

systematic release and amplification of this stolen information. In addition to "doxxing" victims and exposing personal information, the postings frequently contain harassing and intimidating language, including threats of violence directed toward the identified individuals. In the affiant's training and experience, the public dissemination of stolen personal data in this manner is consistent with doxxing and intimidation tactics intended to harass victims, place them in fear for their safety, and increase pressure on them through the widespread exposure of their private information. For example:

a. In or about March 2024, the Handala Hack telegram channel, which states that it is operated by the same group that operates the Handala-Hack.to domain, posted [redacted] visitor logs. [redacted] is an Israeli defense industry firm. In addition to posting the logs, the Telegram Account included language encouraging followers to target individuals on the logs. In that list were two executives of [redacted], a defense firm based in [redacted], Maryland. Given that the only two pieces of information on the "targets list" were the individuals' names and employers, my training and experience tells me that the individuals behind Handala Hack wanted its followers and sympathizers to target these individuals at their places of work. In the case of the two [redacted] executives, that was in the District of Maryland.

b. On March 6, 2026, Handala Hack, via the Handala-hack.to domain, posted names and confidential data corresponding to individuals Handala Hack claimed worked for the Israeli Defense Force ("IDF"). The post stated, in part, "Your iPhone 12 Pro Max holds no security

for us: we even know your exact location...," and urged "People of the Axis of Resistance! See these names and respond to these Zionist pigs yourselves."

c. On March 6, 2026, Handala Hack, via the Handala-hack.to domain, claimed it stole 851 gigabytes of confidential data from members of the Sanzer Hasidic Jewish community, including "documents of financial cooperation, witchcraft ceremonies, and secret correspondences with Netanyahu ..." The post continued "We warn the leaders and members of the Sanzer Hasidic community: No place is safe for you. Betrayal of the oppressed leads to nothing but disgrace and shame. Expect more documents to be revealed. Handala Hack[.]"

d. As of March 9, 2026, Handala Hack, via the Handala-redwanted.to domain, posted the names, photos, and sensitive PII of approximately 190 individuals associated with or employed by the Israeli military and/or government. The Handala Hack posting contained threats indicating the individuals were being monitored, their residences were known, and that consequences would soon follow.

61. Investigators also believe Handala Hack used the email account "Handala_Team@outlook.com" to send death threats to Iranian dissidents and journalists living abroad in the United States [redacted]. In those posts, Handala Hack offered bounties and openly called for Mexican cartel "partners" to commit acts of violence against Handala Hack's targets. There is probable cause to conclude that Handala Hack created and used this account because the address bears a close resemblance to **SUBJECT DOMAIN NAME-2** and **SUBJECT DOMAIN NAME-4**, and the messaging is consistent with Handala Hack's established modus operandi of issuing threats to dissidents and journalists. Furthermore, an email sent from the account identified Handala Hack as the account owner. Specifically, on or about March 1, 2026, the

Handala_Team@outlook.com account was used to email victims [redacted]. In an email with the subject line "Death to [redacted]", the sender [redacted] wrote:

> We the Handala Hack team, the loyal followers of the supreme leader Ali Hosseini Khamenei, declare war on all the enemies of Islam in the West. Our partners, the CJNG [Jalisco New Generation Cartel] cartel in America [redacted] have been given a list of our enemies who are responsible for our great leaders [sic] death. [redacted] you laughed like hyenas during the [redacted] show. We have hacked and revealed your home addresses in [redacted U.S. city] [redacted] to our partners in the CJNG who are in [redacted U.S. state] [redacted] now. Both of you will be executed soon, and we have offered a reward of $250.000 for the operatives who kills [sic] and beheads both of you. ALLAHU AKBAR[.]

62. Based on the foregoing, there is probable cause to believe that Handala Hack used the **SUBJECT DOMAIN NAMES** and associated accounts to identify, harass, and issue death threats against Iranian dissidents and government adversaries.

J. SUBJECT DOMAIN NAME-1

63. As described above, **SUBJECT DOMAIN NAME-1** was used by the threat actor group to commit or facilitate violations of the SUBJECT OFFENSES. A search of publicly available WHOIS domain name registration records revealed that **SUBJECT DOMAIN NAME-1** was registered on or about February 1, 2023, through the registrar Tucows Domains, Inc. ("Tucows"), which is headquartered at 96 Mowat Avenue, Toronto, Ontario, M6K 3M1 Canada. Tucows allows website owners to keep their publicly-viewable contact details private during the domain name registration process.

64. The top-level domain registry for **SUBJECT DOMAIN NAME-1** is Public Interest Registries ("PIR") headquartered at 11911 Freedom Drive, 10th Floor, Suite 1000, Reston, Virginia 20190. PIR currently manages all .org domains.

K. SUBJECT DOMAIN NAME-2

65. As described above, **SUBJECT DOMAIN NAME-2** was used by the threat actor group to commit or facilitate violations of the SUBJECT OFFENSES. A search of publicly available WHOIS domain name registration records revealed that **SUBJECT DOMAIN NAME-2** was registered on or about July 24, 2024, through the registrar Namecheap, which has its headquarters at 4600 East Washington Street, Suite 300, Phoenix, Arizona 85034. Namecheap provides services that allow website owners to keep their publicly viewable contact details private during the domain name registration process.

L. SUBJECT DOMAIN NAME-3

66. As described above, **SUBJECT DOMAIN NAME-3** was used by the threat actor group to commit or facilitate violations of the SUBJECT OFFENSES. A search of publicly available WHOIS domain name registration records revealed that **SUBJECT DOMAIN NAME-3** was registered on or about February 4, 2025, through the registrar Tucows, which has its headquarters at 96 Mowat Avenue, Toronto, Ontario, M6K 3M1 Canada. Tucows provides services that allow website owners to keep their publicly-viewable contact details private during the domain name registration process.

67. The top-level domain for **SUBJECT DOMAIN NAME-3** is Public Interest Registry ("PIR"), headquartered at 11911 Freedom Drive, 10th Floor, Suite 1000, Reston, Virginia 20190. PIR currently manages all .org domains.

M. SUBJECT DOMAIN NAME-4

68. As described above, **SUBJECT DOMAIN NAME-4** was used by the threat actor group to commit or facilitate violations of the SUBJECT OFFENSES. A search of publicly

available WHOIS domain name registration records revealed that **SUBJECT DOMAIN NAME-4** was registered on or about July 12, 2025, through the registrar Namecheap, which has its headquarters at 4600 East Washington Street, Suite 300, Phoenix, Arizona 85034. Namecheap provides services that allow website owners to keep their publicly-viewable contact details private during the domain name registration process.

69. As set forth above, there is probable cause to believe that the **SUBJECT DOMAIN NAMES** are subject to criminal forfeiture because they were used in the commission of violations of the SUBJECT OFFENSES.

V. SEIZURE PROCEDURE

70. As detailed in Attachment A, upon execution of the seizure warrant, the registry for the top-level domain or registrar for the subject domain will be served in the following manner:

a. Public Interest Registry ("PIR"), headquartered at 11911 Freedom Drive, 10th Floor, Suite 1000, Reston, Virginia 20190, shall be directed to restrain and lock **SUBJECT DOMAIN NAME**-1 pending transfer of all right, title, and interest in **SUBJECT DOMAIN NAME**-1 to the United States upon completion of forfeiture proceedings, to ensure that changes to **SUBJECT DOMAIN NAME**-1 cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or DOJ. In addition, upon seizure of **SUBJECT DOMAIN NAME**-1 by the FBI, PIR will be directed to associate **SUBJECT DOMAIN NAME**-1 to a new authoritative name server(s) to be designated by a law enforcement agent. The Government will display a notice on the website to which **SUBJECT DOMAIN NAME**-1 will resolve indicating that

the site has been seized pursuant to a warrant issued by this court.

b. Namecheap, headquartered at 4600 East Washington Street, Suite 300, Phoenix, Arizona 85034, shall be directed to restrain and lock **SUBJECT DOMAIN NAME**-2 pending transfer of all right, title, and interest in **SUBJECT DOMAIN NAME**-2 to the United States upon completion of forfeiture proceedings, to ensure that changes to **SUBJECT DOMAIN NAME**-2 cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or DOJ. In addition, upon seizure of **SUBJECT DOMAIN NAME**-2 by the FBI, Namecheap will be directed to associate **SUBJECT DOMAIN NAME**-2 to a new authoritative name server(s) to be designated by a law enforcement agent. The Government will display a notice on the website to which **SUBJECT DOMAIN NAME**-2 will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

c. PIR, headquartered at 11911 Freedom Drive, 10th Floor, Suite 1000, Reston, Virginia 20190, shall be directed to restrain and lock **SUBJECT DOMAIN NAME**-3 pending transfer of all right, title, and interest in **SUBJECT DOMAIN NAME**-3 to the United States upon completion of forfeiture proceedings, to ensure that changes to **SUBJECT DOMAIN NAME**-3 cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or DOJ. In addition, upon seizure of **SUBJECT DOMAIN NAME**-3 by the FBI, PIR will be directed to associate **SUBJECT DOMAIN NAME**-3 to a new authoritative name server(s) to be designated by a law enforcement agent. The Government will display a notice on the website to which **SUBJECT DOMAIN NAME**-3 will resolve indicating that the site has been seized

pursuant to a warrant issued by this court.

a. Namecheap, headquartered at 4600 East Washington Street, Suite 300, Phoenix, Arizona 85034, shall be directed to restrain and lock **SUBJECT DOMAIN NAME-4** pending transfer of all right, title, and interest in **SUBJECT DOMAIN NAME-4** to the United States upon completion of forfeiture proceedings, to ensure that changes to **SUBJECT DOMAIN NAME-4** cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or DOJ. In addition, upon seizure of **SUBJECT DOMAIN NAME-4** by the FBI, Namecheap will be directed to associate **SUBJECT DOMAIN NAME-4** to a new authoritative name server(s) to be designated by a law enforcement agent. The Government will display a notice on the website to which **SUBJECT DOMAIN NAME-4** will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

VI. CONCLUSION

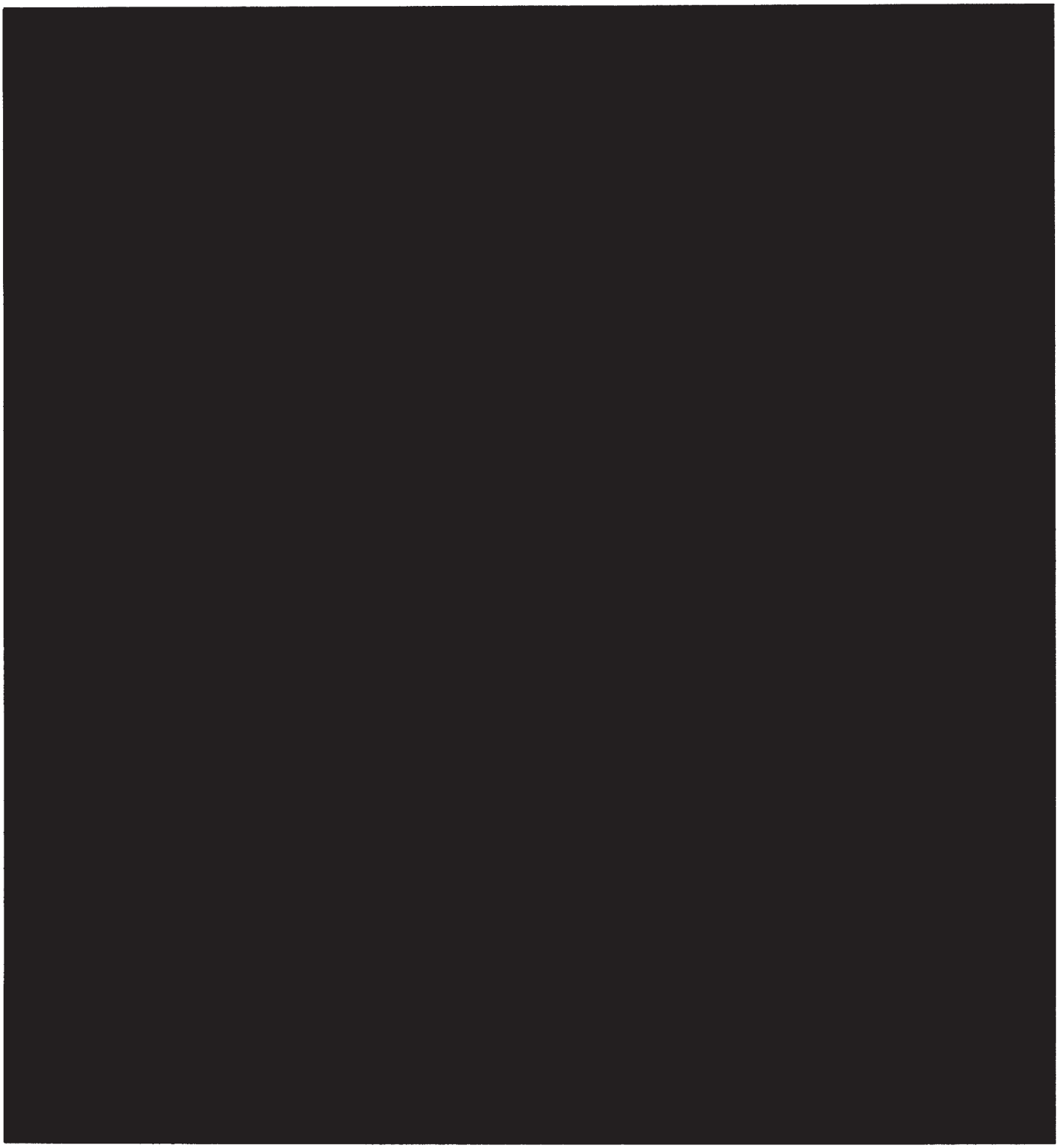
71. For the foregoing reasons, I submit that there is probable cause to believe that the **SUBJECT DOMAIN NAMES** are used in and/or intended to be used in facilitating and/or committing the SUBJECT OFFENSES. Accordingly, the **SUBJECT DOMAIN NAMES** are subject to forfeiture to the United States pursuant to 21 U.S.C. § 853(f) and 18 U.S.C. § 982(a)(2)(B), and I respectfully request that the Court issue a seizure warrant for the **SUBJECT DOMAIN NAMES**.

72. Because the warrant will be served on the Registry or Registrar that controls the **SUBJECT DOMAIN NAMES**, and at a time convenient to it, the relevant Registry or Registrar will transfer control of the **SUBJECT DOMAIN NAMES** to the Government, there exists

reasonable cause to permit the execution of the requested warrant at any time in the day or night.

VII. REQUEST FOR SEALING

73. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into criminal organizations and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the internet and disseminate them to other online criminals as they deem appropriate. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.



1:26-mj-0683-CDA