AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEIZURE WARRANT

I, Aaron Stewart, Special Agent of the Federal Bureau of Investigation ("FBI"), being first duly sworn, hereby declare as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am an "investigative or law enforcement officer of the United States" within the meaning of Section 2510(7) of Title 18, United States Code, that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated against the United States.

2. I have been employed as a Special Agent of the FBI since October 2014 and am currently assigned to the San Francisco Division. While employed by the FBI, I have investigated federal criminal violations related to malicious cyber activity by state-sponsored actors and agents of foreign governments. I have gained experience through training at the FBI and everyday work relating to conducting these types of investigations. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. The facts in this affidavit are based on my personal participation in this investigation, my training and experience, the work of other agents and investigators, and documents, records, emails, and other types of information obtained during the investigation from other sources and witnesses. The FBI has, thus far, conducted open source research, received information from other government agencies, conducted interviews, and served legal process. 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.

4. The following domain names ("the Target Domains") to be seized are registered with U.S.-based domain registrars[1] and use top-level domains owned by U.S.-based registries as follows:

	Domain	**Registrar**	**Registry**	**Paragraph Numbers**
1	ababil.org	Namecheap	Public Internet Registry	54, 102, 107, 110, 111, 122, 126, 139, 142, 165, 168, 173, 180
2	ahtribune.com	n/a	Verisign	44, 72, 73, 75, 81, 83, 87, 89, 90, 178, 179
3	al-ahd.net	OnlineNIC	Verisign	54, 94, 102, 103, 105, 106, 107, 111, 122, 124, 126, 139, 142, 165, 168, 173, 179
4	al-naba.net	n/a	Verisign	54, 102, 108, 109, 148, 179
5	albabylon.com	OnlineNIC	Verisign	54, 102, 112, 113, 119, 127, 159, 179
6	aleppospace.com	TierraNet	Verisign	54, 102, 114, 115, 116, 161, 162, 179
7	alghadeer.tv	GoDaddy	Verisign	54, 102, 113, 117, 118, 119, 127, 159, 179
8	alharakah.net	OnlineNIC	Verisign	54, 102, 107, 111, 120, 121, 122, 126, 135, 139, 142, 165, 168, 173, 179
9	alhiwaraldini.com	n/a	Verisign	54, 94, 102, 105, 107, 111, 113, 119, 122, 123, 124, 125, 126, 127, 139, 142, 159, 165, 168, 173, 179
10	awdnews.com	n/a	Verisign	44, 54, 72, 73, 75, 91, 92, 93, 94, 97, 98, 105, 124, 133, 166, 178, 179
11	criticalstudies.org	Dynadot	Public Internet Registry	44, 72, 73, 75, 80, 99, 100, 101, 178, 180
12	darinews.com	n/a	Verisign	54, 102, 128, 129, 130, 131, 136, 151, 156, 157, 177, 179
13	elintelecto.com	Dynadot	Verisign	54, 98, 102, 132, 133, 179
14	farhang-press.com	n/a	Verisign	54, 102, 121, 131, 134, 135, 136, 151, 156, 177, 179
15	harkarmusulunci.org	n/a	Public Internet	54, 102, 107, 111, 122, 126, 137, 138, 139, 142, 165, 168, 173, 180

[1] The term "n/a" indicates that the registrar is based outside of the United States.

			Registry	
16	iircenter.net	n/a	Verisign	54, 102, 107, 111, 122, 126, 139, 140, 141, 142, 165, 168, 173, 179
17	iuvm-sy.net	TierraNet	Verisign	169, 179
18	iuvmpixel.com	n/a	Verisign	54, 102, 143, 144, 145, 169, 179
19	jordan-times.com	OnlineNic	Verisign	54, 102, 109, 147, 148, 179
20	kelkeen.com	n/a	Verisign	54, 102, 131, 136, 149, 150, 151, 156, 177, 179
21	kurdrudaw.com	n/a	Verisign	54, 102, 152, 153, 154, 179
22	mediaadil.com	n/a	Verisign	107, 111, 122, 126, 139, 142, 165, 168, 171, 172, 173, 179
23	roushd.com	n/a	Verisign	54, 102, 130, 131, 136, 151, 155, 156, 157, 177, 179
24	rpfront.com	Web.com	Verisign	44, 54, 72, 73, 75, 76, 77, 78, 79, 80, 83, 101, 178, 179
25	siampublic.com	OnlineNIC	Verisign	54, 102, 113, 119, 127, 158, 159, 179
26	studiesaf.com	n/a	Verisign	131, 136, 151, 156, 174, 177, 179
27	syria-victory.com	Web.com	Verisign	54, 102, 115, 116, 160, 161, 162, 179
28	voiceofwadi.com	NameBright	Verisign	54, 102, 107, 111, 122, 126, 139, 142, 163, 165, 168, 173, 179
29	yemenpress.org	OnlineNIC	Public Internet Registry	54, 102, 107, 111, 122, 126, 139, 142, 165, 166, 167, 168, 173, 180

5. [redacted] As outlined below, the FBI believes the Target Domains part of the Liberty Front Press network.

6. On October 2, 2020, the Honorable Joseph C. Spero authorized a separate seizure warrant for the seizure of 92 domain names linked to the Liberty Front Press network. Like the Target Domains described herein, those domains were found to be subject to civil and criminal forfeiture because they constituted or were derived from proceeds traceable to a violation of 50 U.S.C. § 1705 and 22 U.S.C. § 611 *et seq*. The FBI executed the seizure warrant on October 7, 2020. The affidavit supporting that warrant is attached hereto as Exhibit A.

7. As set forth below, there is probable cause to believe that the Target Domains constitute property used, or intended to be used, to commit or facilitate violations of 50 U.S.C. § 1705 and 22 U.S.C. § 611 *et seq*. (the **"**Subject Offenses"), and are accordingly subject to seizure and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) and 28 U.S.C. § 2461(c). I make this Affidavit for a warrant to seize the property described in Attachments A through B, the Target Domains.

8. The procedure by which the government will seize the Target Domains is described in Attachments A through B hereto and below.

BACKGROUND ON DOMAIN NAMES

9. Based on my training and experience and information learned from others, I am aware of the following:

10. 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").

11. 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.

12. 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, and the "example" second-level domain. The owner of a second-level domain assigns it to a particular web server to host the content of any associated website or other content.

13. Domain Name Servers: DNS servers are computers connected to the Internet that convert, or resolve, domain names into IP addresses.

14. 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. ("VeriSign"), which has its headquarters at 12061 Bluemont Way, Reston, Virginia; the registry for ".org" top-level domain is Public Internet Registry, which has its headquarters at 1775 Wiehle Avenue, Suite 200 Reston, Virginia 20190; and the registry for ".info" top-level domain is Afilias, Inc., which has its headquarters at 300 Welsh Road, Building 3, Suite 105, Horsham, Pennsylvania 19044.

15. 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 assign a domain name to another computer anywhere in the world. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

16. 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 12.145.67.0 - 12.145.67.99 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 12.145.67.0 - 12.145.67.99.

17. Web crawler. A web crawler is a generic term for any program (such as a robot or spider) that is used to automatically discover and scan websites by following links from one webpage to another. A web crawler copies webpages so that they can be processed later by a search engine, such as Google or Yahoo!, which indexes the downloaded pages. This allows users of the search engine to find webpages quickly.

RELEVANT STATUTES

International Emergency Economic Powers Act

18. The International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701–1706, authorizes the President of the United States to impose economic sanctions on a foreign country, individual, or organization in response to an unusual or extraordinary threat to the national security, foreign policy, or economy of the United States when the President declares a national emergency with respect to that threat.

19. Pursuant to the authority under IEEPA, the President of the United States and the executive branch have issued orders and regulations governing and prohibiting certain transactions by U.S. persons or involving U.S. goods. Title 50, United States Code, Section 1705 provides:

> A person who willfully commits, willfully attempts to commit, or willfully conspires to commit, or aids or abets in the commission of a violation of any license, order, or regulation issued under this chapter shall, upon conviction, be fined or may be imprisoned for not more than twenty years, or both; and any officer, director, or agent of any corporation who knowingly participates in such violation may be punished by a like fine, imprisonment, or both.

The Iranian Transactions and Sanctions Regulations

20. On March 15 and May 6, 1995, the President of the United States issued

Executive Orders Nos. 12957 and 12959, prohibiting, among other things, the exportation, reexportation, sale, or supply, directly or indirectly, to Iran of any goods, technology, or services from the United States or by a United States person, and on August 19, 1997, issued Executive Order No. 13059 clarifying the previous orders (collectively, the "Executive Orders"). The Executive Orders authorized the United States Secretary of the Treasury to promulgate rules and regulations necessary to carry out the Executive Orders. Pursuant to this authority, the Secretary of the Treasury promulgated the Iranian Transactions Regulations (renamed in 2013, the Iranian Transactions and Sanctions Regulations, the "ITSR") implementing the sanctions imposed by the Executive Orders.

21. The ITSR, Title 31, Code of Federal Regulations, Section 560.204, prohibits, among other things, the exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a United States Person, of goods, technology, or services to Iran or the GOI (with certain limited exceptions), including the exportation, reexportation, sale or supply of goods, technology or services to a third country knowing that such goods, technology or services are intended for Iran or the Government of Iran, without a license from the United States Department of the Treasury, Office of Foreign Assets Control ("OFAC").

22. The ITSR further prohibit transactions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate the ITSR. 31 C.F.R. § 560.203.

Sanctions Concerning the IRGC

23. *Executive Order 13224*. On September 23, 2001, under the authority of IEEPA and other authorities, the President of the United States issued Executive Order 13224 "Blocking

Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism." Although Executive Order 13224—issued two weeks after the September 11, 2001 attacks on the United States—targeted Al Qaeda, the United States has subsequently used it to target Iran.[2]

24. Section 1 of Executive Order 13224 states, in part, that: "…all property and interests in property of the following persons that are in the United States or that hereafter come within the United States, or that hereafter come within the possession or control of United States persons are blocked:

> (b) foreign persons determined by the Secretary of State, in consultation with the Secretary of the Treasury and the Attorney General, to have committed, or to pose a significant risk of committing, acts of terrorism that threaten the security of U.S. nationals or the national security, foreign policy, or economy of the United States."

25. Section 105 of the Countering America's Adversaries Through Sanctions Act ("CAATSA") mandated the imposition of Executive Order 13224 penalties on the Islamic Revolutionary Guard Corps ("IRGC") and its officials, agents, and affiliates by October 30, 2017.

26. On October 13, 2017, OFAC designated the IRGC as a Specially Designated National pursuant to Executive Order 13224 and consistent with CAATSA. OFAC designated the IRGC for its activities in support of the IRGC-Qods Force ("IRGC-QF"), which was

[2] *See* "Iran Sanctions," Congressional Research Service, RS20871, updated July 23, 2020.

designated pursuant to Executive Order 13224 on October 25, 2007, for providing support to a number of terrorist groups, including Hizballah, Hamas, and the Taliban.

27. The State Department has authority under Section 219 of the Immigration and Nationality Act (Title 8, United States Code, Section 1189) to designate an entity as a Foreign Terrorist Organization ("FTO"). On April 15, 2019, the United States designated the IRGC as an FTO.

28. *Executive Order 13848*. On September 12, 2018, under the authority of IEEPA and other authorities, the President of the United States issued Executive Order 13848 "Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election."

29. Section 2(a) of Executive Order 13848 states: "All property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in: any foreign person determined by the Secretary of the Treasury, in consultation with the Secretary of State, the Attorney General, and the Secretary of Homeland Security:

> (i) to have directly or indirectly engaged in, sponsored, concealed, or otherwise been complicit in foreign interference in a United States election;
>
> (ii) to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any activity described in subsection (a)(i) of this section or any person whose property and interests in property are blocked pursuant to this order; or
>
> (iii) to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property or interests in property are blocked pursuant to this order.

30. On October 22, 2020, OFAC designated the International Union of Virtual Media ("IUVM") as a Specially Designated National pursuant to Executive Order 13848.

31. The U.S. Department of Treasury designated the IRGC, the IRGC-QF, and Bayan Rasaneh Gostar Institute as Specially Designated Nationals pursuant to Executive Order 13848 for having directly or indirectly engaged in, sponsored, concealed, or otherwise been complicit in foreign interference in the 2020 U.S. presidential election. The IUVM was designated as a Specially Designated National pursuant to Executive Order 13848 for being owned or controlled by the IRGC-QF.

Foreign Agents Registration Act

32. The U.S. Department of Justice administers the Foreign Agent Registration Act ("FARA"). FARA establishes a registration, reporting, and disclosure regime for agents of foreign principals (which includes foreign non-government individuals and entities) so that the U.S. government and the people of the United States are informed of the source of information and the identity of persons attempting to influence U.S. public opinion, policy, and law. FARA requires, among other things, that persons subject to its requirements submit periodic registration statements containing truthful information about their activities and the income earned from them. Disclosure of the required information allows the federal government and the American people to evaluate the statements and activities of such persons in light of their function as foreign agents. Specifically,

a. FARA states that "[n]o person shall act as an agent of a foreign principal unless he has filed with the Attorney General a true and complete registration statement." 22 U.S.C. § 612(a).

b. FARA defines "foreign principal" to include "a government of a foreign country," a "foreign political party," and "a person outside of the United States" who is not a United States citizen. Id. § 611(b). The term "government of a foreign country" is defined to include any person "exercising sovereign de facto or de jure political jurisdiction over any country," including "any group or agency to which such sovereign de facto or de jury authority or functions are directly or indirectly delegated." *Id*. § 611(e).

c. FARA defines the term "agent of a foreign principal" to have two requirements. First, the person must either "act[] as an agent, representative, employee, or servant" of a foreign principal, or act "at the order, request, or under the direction or control, of a foreign principal," or be a person "any of whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in major part by a foreign principal." Id. § 611(c)(1). Second, the person must either "engage[] within the United States in political activities for or in the interests of such foreign principal," or "act[] within the United States as a public relations counsel, publicity agent, information-service employee or political consultant for or in the interests of such foreign principal," or "within the United States represent[] the interests of such foreign principal before any agency or official of the Government of the United States." *Id*.

d. The term "political activities" means any activity that the person engaging in believes will, or that the person intends to, in any way influence any agency or official of the Government of the United States or any section of the public within the United States with reference to formulating, adopting, or changing the domestic or foreign policies of the United States or with reference to the political or public interests, policies, or relations of a government of a foreign country or a foreign political party. *Id*. § 611(o).

e. An agent must also register if it acts within the United States as a publicity agent or information-service employee of a foreign principal. A "publicity agent" refers to "any person who engages directly or indirectly in the publication or dissemination of oral, visual, graphic, written, or pictorial information or matter of any kind, including publication by means of . . . broadcasts, motion pictures, or otherwise." Id. § 611(h). An "information-service employee" includes any person "who is engaged in furnishing, disseminating, or publishing accounts, descriptions, information, or data with respect to the political, industrial, employment, economic, social, cultural, or other benefits, advantages, facts, or conditions or any country other than the United States or of any government of a foreign country . . . ." *Id*. § 611(i).

f. The term "agent of a foreign principal" does not include any news or press service or association organized under the laws of the United States or any State or other place subject to the laws of the United States, or any newspaper, magazine, periodical, or other publication for which there is on file with the United States Postal Service information in compliance with Section 3611 of title 39, published in the United States, solely by virtue of any bona fide news or journalistic activities, including the solicitation or acceptance of advertisements, subscriptions, or other compensation therefor, so long it is at least 80 per centum beneficially owned by, and its officers and directors, if any, are citizens of the United States, and such news or press service or association, newspaper, magazine, periodical, or other publication, is not owned, directed, supervised, controlled, subsidized, or financed, and none of its policies are determined by any foreign principal. *Id*. § 611(d).

g. FARA imposes criminal penalties on any person who "willfully violates any provision" of the statute. 22 U.S.C. § 618(a)(1).

Statutory Basis for Seizure

33. Title 18, United States Code, Section 981(a)(1)(C) provides that any property, real or personal, which constitutes or is derived from proceeds traceable to, a violation of a specified unlawful activity, to wit: the International Emergency Economic Powers Act, Title 50, United States Code, Section 1705; and the Foreign Agents Registration Act, Title 22, United States Code, Section 611 *et seq*., or a conspiracy to commit such an offense, is subject to forfeiture.

34. Title 18, United States Code, Section 981(b)(2) authorizes seizure of property subject to civil forfeiture based upon a warrant supported by probable cause. Title 18, United States Code, Section 981(b)(3) permits the issuance of a civil seizure warrant by a judicial officer in any district in which a forfeiture action against the property may be filed pursuant to Title 28, United States Code, Section 1355(b). A forfeiture proceeding may be brought in this district because acts or omissions giving rise to forfeiture occurred in this district.

35. Title 21, United States Code, Section 853(f) (as incorporated by Title 18, United

States Code, Section 982(b)(1)) provides that a criminal seizure warrant for property subject to forfeiture may be sought in the same manner in which a search warrant may be issued under Federal Rule of Criminal Procedure 41. 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.

36. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the Target Domains for forfeiture. By seizing the Target Domains and redirecting each Target Domain to another website, the Government will prevent third parties from acquiring the name and using it to commit additional crimes. Furthermore, seizure of the Target Domains will prevent third parties from continuing to access the Target Domain websites in their present form. A restraining order or injunction will still render the Target Domains subject to entry and vulnerability to cyber-attacks, whereas seizure will ensure that the Target Domains cannot be used for any nefarious purpose

37. Title 18, United States Code, Section 981(h) provides that venue for civil forfeitures brought under this section lies in the district either where the defendant owning the property is located or in the judicial district where the criminal prosecution is brought.

38. Venue. Title 21, United States Code, Section 853(j), incorporating Title 21, United States Code, Section 881(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.

39. As defined above, a "web crawler" is a generic term for any program (such as a robot or spider) that is used to automatically discover and scan websites by following links from one webpage to another. According to support.google.com, Google's main crawler is called Googlebot. A web crawler copies webpages so that they can be processed later by the search engine, which indexes the downloaded pages. This allows users of the search engine to find webpages quickly. According to Google, when Googlebot finds a webpage, Google's systems render the content of the page, just as a browser does. Google takes note of key signals—from keywords to website freshness—and keeps track of it all in the Search index. The Google Search index contains hundreds of billions of webpages and is well over 100,000,000 gigabytes in size.

40. Although it can vary widely, once a website is on the internet, the indexing process can take as little as an hour or up to several weeks. Based on open source research by the FBI, the archived versions of the Target Domains show an online presence of months to years, thereby providing ample time for Googlebot to crawl and index the Target Domains to Google servers.

41. Moreover, the Target Domains are all accessible and viewable to Internet users in the Northern District of California. Various individuals employed by the FBI, including the undersigned, have accessed and seen the Target Domains in the Northern District of California.

42. As set forth below, there is probable cause to believe that the Target Domains are subject to civil and criminal forfeiture because they constitute or are derived from proceeds traceable to a violation of the Subject Offenses, namely, the use of U.S. domain registration services in violation of IEEPA and/or FARA. Specifically, Verisign and Public Internet

Registry, both located in the U.S., are the top-level domain name registries for the Target Domains. Verisign currently charges $7.85 per year for the registration or renewal of a ".com" domain, and Public Internet Registry currently charges $9.93 per year for the registration or renewal of a ".org" domain. As described below, each of the Target Domains was fraudulently registered because each is being used by or on behalf of the IRGC and this critical information was omitted from the registration, and because the source of funds emanated from entities violating IEEPA and FARA, to wit, individuals part of and/or associated with the IRGC and GOI. The Target Domains are accordingly subject to seizure pursuant to Title 18, United States Code, Section 981(b); and Title 21, United States Code, Section 853(f).

FACTS SUPPORTING PROBABLE CAUSE

Overview

43. As described throughout this application, the FBI believes that the Government of Iran, through the IRGC as well as individuals acting on behalf of the IRGC, is engaging in a covert influence campaign both inside the United States and elsewhere through the use of domains registered in the United States, in violation of IEEPA. This belief, as explained throughout, [redacted] content from the domains which is consistent with Iranian foreign policy and IRGC disinformation and misinformation tradecraft, open source reporting, and returns from legal process which indicate that the Target Domains were registered under false names and content hosted on the Target Domains originated in Iran. As a result, there is probable cause to seize

each of the Target Domains as property which constitutes or is derived from proceeds traceable to a violation of 50 U.S.C. § 1705, as described above.

44. In addition, Target Domains **rpfront.com, ahtribune.com, awdnews.com** and **criticalstudies.org,** described in detail below, have been used by the IRGC and those acting on behalf of the IRGC and the GOI to engage in the United States in political activities and disseminate information, as defined by FARA, without proper registration pursuant to FARA and without notifying the American public with a conspicuous label that the content of the domains was being published on behalf of the IRGC and the GOI. As a result, there is probable cause to seize these domains as property which constitutes, or is derived from proceeds traceable to, a violation of FARA.

Background on Iranian Foreign Policy

45. The February 11, 1979, fall of the Shah of Iran, who was a key U.S. ally, shattered U.S.-Iran relations. According to a February 2020 Congressional Service Report, Iran has since pursued policies that every successive U.S. Administration has considered inimical to U.S. interests in the Near East region and beyond. Iran's authoritarian political system and human rights abuses have further contributed to the U.S.-Iran rift.

46. On April 29, 2020, the Congressional Research Service published that the ideology of Iran's 1979 Islamic revolution still infuses Iran's foreign policy today. Iran's leaders assert that the political structure of the Middle East is heavily weighted in favor of the United States and its regional allies and against those who Iranian leaders describe as "oppressed peoples," such as Palestinians and Shia Muslims. Shias are politically and economically

disadvantaged minorities in many countries of the region. Iranian leaders claim that Western intervention and the creation of Israel have distorted the region's politics and economics. Iran's leadership has a history of taking advantage of regional conflicts to advance a broader goal of overturning a power structure in the Middle East that it asserts favors the United States, Israel, Saudi Arabia, and other Sunni Muslim Arab regimes.

Iranian Cyber Influence Operations

47. Several reputable sources have identified Iran as one of numerous countries that implement state-sponsored, malign foreign influence campaigns utilizing cyberspace. According to the Homeland Security Advisory Council Interim Report of the Countering Foreign Influence Subcommittee on May 21, 2019, Iran was alleged to be involved in malign foreign influence activities, whose aim is "designed to sow discord, manipulate public discourse, discredit the electoral system, bias the development of policy, or disrupt markets for the purpose of undermining the interests of the United States and its allies."

48. Further, the Iranian Action Group of the U.S. Department of State described Iran as a "leading threat actor in cyberspace, which uses cyberespionage, propaganda, and attacks to influence events, shape foreign perceptions, and counter perceived threats." Although the IRGC is oftentimes behind Iranian cyber-attacks or intrusions, it often uses individuals outside of the government to assist with these operations. Similarly, the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security reported that the U.S. intelligence community and various private sector threat intelligence organizations have identified the IRGC as a driving force behind Iranian state-sponsored cyberattacks—either through contractors in the

Iranian private sector or by the IRGC itself.

49. A June 25, 2019, assessment of Iran's cyber power by the Center for Strategic and International Studies Senior Vice President James Andrew stated that Iran's cyber operations are conducted primarily by the IRGC, the Basij, and Iran's Passive Defense Organization. According to the assessment, the IRGC is behind a series of incidents against American targets, Israeli critical infrastructure, Saudi Arabia, and other Gulf States.

50. Known Iranian cyber operations have typically focused on "soft" targets. More specifically, expert witness Philip Howard from Oxford Internet Institute at the Open Hearing on Foreign Influence Operations' Use of Social Media Platforms Before the Select Committee on Intelligence of the U.S. Senate on August 1, 2018, described Iran as one of several studied countries that has organized dedicated disinformation campaigns, and, in particular, had a recently exposed social media manipulation operation. Iran's use of inauthentic social media accounts, which garnered more than one million followers, "focused on promoting particular policy interests that are aligned with the Iranian government," according to Park Advisors in a report produced with the support of the U.S. Department of State's Global Engagement Center.

51. Iranian state-sponsored foreign influence and information operations have been far-reaching and targeted. For example, in the written testimony of Joseph M. Humire regarding Iran's Strategic Penetration of Latin America before the U.S. House of Representatives Committee on Foreign Affairs, Subcommittee on the Western Hemisphere, Subcommittee on the Middle East & North Africa, Mr. Humire wrote:

> While subtle and often under the radar, Iran's 'cultural' outreach has been significant over the last decade and is only growing in both size and scope. One

> of the most visible outcomes of this outreach is their Spanish language 24-hour news broadcast, HispanTV, that is operated by the larger, state-owned Islamic Republic of Iran Broadcaster ('IRIB'). Launched in 2012, this Iranian network has grown to broadcast in at least 16 countries throughout Latin America, often in conjunction with what is known as counter-hegemonic news media in the region, namely the Venezuela-based TeleSUR. This media network provides Iran with a large megaphone to enhance its influence and information operations in the region.

52. Targeted influence topics have included messaging against the current U.S. President, U.S. withdrawal from the Joint Comprehensive Plan of Action ("JCPOA"), anti-Israeli narratives, and condemnation of Saudi Arabia, an Iranian adversary. Similarly, Iranian actors have produced pro-GOI, inauthentic news media imitating authentic news sources posted on websites that are prominent in search results for authentic news media.

53. The above demonstrates a history of intent, capability, and tactics by the GOI and the IRGC in creating inauthentic electronic content for use in mass, coordinated disinformation campaigns, for the purpose of influencing public opinion regarding U.S. politics and foreign policy.

Iran's Current Covert Influence Campaign

54. [redacted] the following Target Domains were operated by or on behalf of the IRGC: **ababil.org, al-ahd.net, al-naba.net, albabylon.com, aleppospace.com, alghadeer.tv, alharakah.net, alhiwaraldini.com, awdnews.com, darinews.com, elintelecto.com, farhang-press.com, harkarmusulunci.org, iircenter.net, , iuvmpixel.com,**

jordan-times.com, kelkeen.com, kurdrudaw.com, roushd.com, rpfront.com, siampublic.com, syria-victory.com, voiceofwadi.com and **yemenpress.org**. This information, as described below, is consistent with information that the FBI has obtained from open sources, U.S. service providers, and through the use of criminal process indicating that the GOI, and the IRGC in particular, is behind this covert influence and disinformation campaign, and has violated the Subject Offenses to advance this campaign. Additionally, as described below, the FBI identified the remainder of the Target Domains as being used, accessed, and/or registered by the same user(s) as the Target Domains [redacted] and note that the content of the these remaining Target Domains is consistent with the GOI tradecraft observed throughout this investigation. The FBI, therefore, assesses that all of the Target Domains are being used by or on behalf of the GOI and the IRGC in violation of IEEPA.

55. [redacted]

56. [redacted]

[redacted]

Liberty Front Press

57. [redacted]

FireEye first publicly reported on Liberty Front Press activity in a report dated August 21, 2018, entitled "Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East." FireEye provided supplemental reporting regarding Liberty Front Press on September 7, October 19, November 15, and December 6, 2018; and February 1, March 18, and April 23, 2019. [redacted] As outlined in this Affidavit, the FBI believes the Target Domains to be part of the Liberty Front Press network.

58. According to FireEye reporting, Liberty Front Press activity originated from Iran and was aimed at audiences in the U.S., U.K., Latin America, and the Middle East. The Liberty Front Press operation leverages a network of inauthentic news sites and clusters of associated accounts across multiple social media platforms to promote political narratives in line with Iranian interests. These narratives included anti-Saudi, anti-Israeli, and pro-Palestinian themes, as well as support for specific U.S. policies favorable to Iran, such as the JCPOA.

59. FireEye assessed that Liberty Front Press originated from Iran-based actors based on a combination of indicators, including website registration data, social media accounts linked to Iranian phone numbers, and the promotion of content consistent with Iranian political interests.

60. For example, registrant emails for two inauthentic news sites included in the Liberty Front Press network, libertyfrontpress.com and institutomanquehue.org, were associated with advertisements for website designers in Tehran and with the Iran-based site gahvare.com, respectively. Furthermore, FireEye identified multiple Twitter accounts directly affiliated with the sites, as well as other associated Twitter accounts, that were linked to phone numbers with the +98 Iranian country code. Finally, FireEye observed inauthentic social media personas, masquerading as American liberals supportive of a current U.S. Senator and former candidate for U.S. President, heavily promoting Quds Day, a holiday established by Iran in 1979 to express support for Palestinians and opposition to Israel, and which takes place on the last Friday of Ramadan.

61. According to FireEye, the namesake of the Liberty Front Press network, libertyfrontpress.com, publishes primarily political news stories related to the U.S., and language used by social media accounts affiliated with the site portray it as operated by individuals based in the United States. Much of the content on the site has been appropriated from legitimate news sources, including Politico, RawStory, and CNN. Content that appears to be original to libertyfrontpress.com contains poorly written English.

62. FireEye reported that the registration email for domain libertyfrontpress.com was

associated with several advertisements for website designers in Tehran from 2014. The registration email for libertyfrontpress.com links the website to at least one other site identified as part of the Liberty Front Press network. Furthermore, fake personas and social media accounts linked to other websites identified as part of the Liberty Front Press network have promoted libertyfrontpress.com

63. FireEye reported that libertyfrontpress.com has maintained social media accounts on multiple platforms, including Twitter, Facebook, Instagram, Google Plus, and YouTube. Most of these Twitter accounts are linked to phone numbers with the Iranian +98 country code, despite listing their locations as being within the U.S. Many were created on the same day as at least one other account, evidencing an organized and coordinated effort to promote the fake news site. Most of libertyfrontpress.com's affiliated social media accounts appear orientated toward particular countries or regions. For example, of the accounts focused on the Middle East, three of the Twitter accounts identified by FireEye focused on Palestinian themes, and others focused on Yemen, Syria, Bahrain, and potentially Qatar. These accounts have pushed content in line with Iranian interests.

64. FireEye reported that the site's original Twitter accounts, @libertyfrontpr and @libertyfrontp, began tweeting content in April 2017 that included American-themed material, such as photographs of the Statue of Liberty. The two accounts, which linked to libertyfrontpress.com in their bios, also used language to suggest U.S. origins, such as the use of "our country" in reference to the United States. In mid-July 2018, FireEye observed these two accounts drop their direct affiliation with libertyfrontpress.com and rebrand under the pretense of

being operated by American liberals.

65. FireEye reported that the rebranded accounts heavily promoted Quds Day and also tweeted general opposition to the current U.S. Presidential Administration. In July 2018, two other Palestine-focused libertyfrontpress.com-affiliated accounts, @LFPressPalestin and @QudsPalestine, changed their account names to @PalestinianRes (display name: "Palestinian Resistance") and @VoiceofQuds (display name: "Voice of Quds"), respectively. Collectively, pro-Palestine, anti-Israel, anti-Saudi and anti-U.S. President themes appear to be common across most of the libertyfrontpress.com-affiliated social media accounts, irrespective of their purported regions and areas of focus.

66. Based on a tip from FireEye, Facebook started its own investigation into Liberty Front Press and identified additional accounts and pages from the network. Facebook reported that some of the accounts attempted to conceal their location and primarily posted political content focused on the Middle East, as well as the UK, U.S., and Latin America. Beginning in 2017, the accounts increased their focus on the UK and U.S. Facebook reported that accounts and pages linked to Liberty Front Press typically posed as news and civil society organizations sharing information in multiple countries, without revealing their true identity, and promoted a pro-Iranian agenda. Based on the tip from FireEye, Facebook reported on August 21, 2018 that it removed 652 pages, groups and accounts for coordinated inauthentic behavior that originated in Iran and targeted people across multiple internet services in the Middle East, Latin America, UK and U.S.

67. Facebook was able to link the Liberty Front Press network to Iranian state media

through publicly available website registration information, as well as the use of related IP addresses and Facebook pages sharing the same admins. For example, according to Facebook, one part of the network, "Quest 4 Truth," claimed to be an independent Iranian media organization, but is in fact linked to Press TV, an English-language news network affiliated with Iranian state media.

68. Consistent with Facebook's finding, Liberty Front Press's activities are indicative of a state-sponsored influence campaign. The anti-U.S., anti-Saudi and anti-Israeli material being promoted is in line with Iranian foreign policy and similar to previously identified Iranian covert influence campaigns. Also consistent with known Iranian covert influence campaigns, the network accomplishes Iranian propaganda objectives by manipulating U.S. public discourse and sowing discord in the American people through use of U.S. social media platforms and inauthentic news media outlets. [redacted], there is probable cause to believe the IRGC is directing this campaign and that the domains associated with the Liberty Front Press activities are registered on behalf of the IRGC.

69. Furthermore, based on my training and experience, the breadth and sophistication of the network is consistent with GOI state-sponsored influence campaigns carried out by the IRGC. Liberty Front Press represents a widespread, orchestrated and coordinated effort utilizing potentially thousands of inauthentic domains and social media accounts to promote pro-GOI political interests. For example, in its investigation of Liberty Front Press to date, the FBI has identified well over 1,000 domains, email accounts and social media accounts from Twitter,

Facebook, Instagram and YouTube, and the FBI believes that many more exist. In addition, many of the personas used by the network appear well-crafted and detailed. For example, persona "Liam Jay Campbell" claims to be "a journalist and English MA graduate from Sacramento," claims to have attended California State University, and maintains social media accounts on Twitter and Reddit. It is unlikely that any Iran-based group or entity other than the GOI–or an organization supported by the GOI, like the IRGC–would have the resources to pursue an influence campaign as broad and sophisticated as Liberty Front Press.

70. As described above, on October 7, 2020, the FBI seized 92 domains (the "October 7 Seizure") that the FBI had identified as inauthentic news sites that were operated by or on behalf of the IRGC and linked to the Liberty Front Press campaign. The domains were seized pursuant to a federal seizure warrant issued on October 2, 2020 by the U.S. District Court for the Northern District of California. The affidavit supporting that warrant is attached hereto as Exhibit A.

Additional Investigative Activity

71. As part of its investigation, the FBI conducted searches of publicly available WHOIS domain name registration records. The FBI also obtained subscriber and transaction records from the U.S.-based registrars for the Target Domains, as well as additional relevant subscriber and transaction records from other U.S.-based service providers. As further outlined below, subscriber and transaction records from Cloudflare, a U.S.-based company providing internet infrastructure and security services, revealed that many of the Target Domains–as well as domains seized in the October 7 Seizure–were accessed and/or referenced by the same

Cloudflare user ID number, evidencing a broad and interconnected network.

The Target Domains

72. There is probable cause to believe that each of the Target Domains is property which constitutes or is derived from proceeds traceable to violations of IEEPA, as they are used by or on behalf of the IRGC, a component of the Government of Iran. Had the registrants of the domains truthfully registered the domains as being used by or on behalf of the IRGC, the U.S. service providers would not have been permitted to provide domain name registration services as it is prohibited by U.S. sanctions targeting the IRGC (described above). Target Domains **rpfront.com, ahtribune.com, awdnews.com,** and **criticalstudies.org** are also subject to seizure as those domains are property that constitutes or is derived from proceeds traceable to violations of FARA.

The Target Domains are Property Constituting or are Derived from Proceeds Traceable to Violations of IEEPA and FARA.

73. As described below, there is probable cause to believe that Target Domains **rpfront.com, ahtribune.com, awdnews.com,** and **criticalstudies.org** are property which constitutes or is derived from proceeds traceable to violations of IEEPA (because they are used by or on behalf of the IRGC and the GOI) as well as FARA. Neither the IRGC, nor any individual or entity on the IRGC's behalf, has registered with the Department of Justice for the activities taking place using Target Domains **rpfront.com, ahtribune.com, awdnews.com,** and **criticalstudies.org.** Furthermore, these Target Domains are not properly labeled pursuant to FARA.

74. First, both the GOI and the IRGC are "Foreign Principals" as defined by FARA.

The term "government of a foreign country" includes any person or group of persons exercising sovereign de facto or de jure political jurisdiction over any country, other than the United States, or over any part of such country, and includes any subdivision of any such group and any group or agency to which such sovereign de facto or de jury authority of functions are directly or indirectly delegated. 22 U.S.C. § 611(e).

75. Second, the operators of these domains are acting as agents of the GOI and the IRGC under several theories of agency as defined by FARA. First, they are acting as agents by engaging in political activities, *i.e.*, by attempting to influence any section of the public within the United States with reference to formulating, adopting, or changing the domestic or foreign policies of the United States, or with reference to the political or public interests, policies, or relations of Iran. Second, they are acting as agents by acting as information-service employees by furnishing, disseminating, or publishing accounts, descriptions, information, or data with respect to the political, industrial, employment, economic, social, cultural, or other benefits, advantages, facts, or conditions or any country other than the United States or of any government of a foreign country. Finally, they are acting as publicity agents by engaging, directly or indirectly, in the publication or dissemination of oral, visual, graphic, written, or pictoral information or matter of any kind. As these activities are taking place in the United States, in that they are being published in English and targeting a United States audience, and without the required registration with the Department of Justice,[3] the user(s) of Target Domains

[3] Registration pursuant to FARA does not require a foreign agent to alter the content of its publications in any manner; indeed, if registered as required, a foreign agent would be free to facilitate the production, publication, and dissemination of any content it chooses. Registration would simply allow the American public consuming

rpfront.com, ahtribune.com, awdnews.com, and **criticalstudies.org** are violating FARA.

76. **Rpfront.com**. [redacted], **rpfront.com** is operated by or on behalf of the IRGC.

77. According to FireEye, Target Domain **rpfront.com** describes itself as "a progressive NGO that aims to support people's movements for freedom, peace and justice, reaffirm civil rights and reduce the influence of money in politics—among other things—through a government of the people, by the people and for the people." The **rpfront.com** website publishes English-language political news stories pertaining primarily to the U.S. and Middle East, including both plagiarized and original content, consistent with GOI propaganda. The content reflects narratives in line with GOI political stances. The FBI assesses that by disseminating this material in English, and directing it toward a U.S. audience, the user(s) of this domain are violating FARA by engaging in political activities. For example, articles featured on the site have included op-eds protesting a new Israeli law declaring Israel to be "the historic homeland of the Jewish people… [who] have the exclusive right to national self-determination in it" and pieces depicting the current U.S. Presidential administration negatively, such as those criticizing the administration's immigration policies, which the FBI assesses to be an attempt to influence some portion of the U.S. public to change U.S. foreign or domestic policies to benefit the GOI.

78. The **rpfront.com** website was registered on May 8, 2017, using the email address

---

such content to be fully informed regarding the foreign principal behind it.

realprogressivefront@gmail.com. The domains rpfront.org and rpfront.us were also registered using this email. The registrant name provided was "realprogressive front," and the address provided—a street in Houston, Texas— appears to have been falsified based on an incorrect ZIP code. The phone number provided included the U.S. country code of "+1" but did not have the appropriate number of digits for a U.S. phone number.

79. According to FireEye, while the primary Twitter account for **rpfront.com**, @RPFront, lists its location as the United States, it was registered with a +98 Iran country code phone number. Also, additional social media accounts affiliated with the site focus on the UK, Saudi Arabia, Palestine, Bahrain, and Syria. Twitter account @VoiceOfQuds, discussed above as being associated with libertyfrontpress.com, promoted **rpfront.com** material. **Rpfront.com** also claims some individuals as contributors to its site that were also listed as contributors for usjournal.net, which was seized in the October 7 Seizure. The **rpfront.com** site content includes some material authored by genuine individuals.

80. Subscriber and transaction records from Cloudflare for **rpfront.com** revealed that User ID 7335792 was used to access **rpfront.com** and **criticalstudies.org,** as well as Liberty Front Press domain usjournal.net, which was seized in the October 7 Seizure. As a result, the FBI assesses that **rpfront.com** is used by or on behalf of the IRGC in violation of U.S. sanctions.

81. **Ahtribune.com**. Target Domain **ahtribune.com** is an English-language news site featuring the following sections: US, World, Opinion, In Depth, Politics, Religion, History, Youth, and Human Rights. The bottom of the main page also lists the following regional news categories: Africa, Americas, Asia & Pacific, Europe, and North Africa & South West Asia.

According to the site, "American Herald Tribune is a genuinely independent online media outlet. AHTribune is dedicated to strengthening and supporting independent journalism, and to improving the public's access to independent information sources. AHTribune aim is to inspire action and advocacy on the human rights, social justice, media, spirituality and religion, contemporary history, youth issues and more. Funding for AHTribune comes from site advertising, individual donors, and private foundations. AHTribune publishes grassroots success stories and inspirational narratives alongside hard-hitting critiques of policies, and in-depth reports, encouraging critical thinking and civic action on a diverse range of issues affecting individuals and their communities."

82. As of October 19, 2020, trending topics featured on the site included Covid-19, #IsraelGate, Palestine, and the 2020 U.S. election. Narratives of content featured on the home page include anti-Israel, anti-US, anti-Semitic, and pro-Hizbollah sentiments consistent with GOI policies. Content featured on the "2020 Election" page presents narratives critical of the U.S. election process and candidates. For example, content on the "2020 Election" webpage insinuates that particular candidates for U.S. President and U.S. Vice President were pro-Zionist; that mail-in voting could lead to violence; and that the U.S. election is susceptible to foreign interference. The FBI assesses that these articles constitute political activities, as defined by FARA, as they are designed to influence any section of the public within the United States with reference to formulating, adopting, or changing the domestic or foreign policies of the United States, or with reference to the political or public interests, policies, or relations of Iran. Of note, the interview of an American progressive writer by American Herald Tribune was also featured

in this section. The columnists page identified 200 authors and/or contributors for American Herald Tribune.

83. FireEye identified **ahtribune.com** as part of the Liberty Front Press network. According to FireEye, while American Herald Tribune claims to be "a genuinely independent online media outlet" involved in journalism, associated Twitter account @AHTribune was linked to a phone number with the +98 Iranian country code. In addition, American Herald Tribune was hosted on Iranian domain name servers. American Herald Tribune articles and social media were promoted by Target Domain **rpfront.com**, indicating that these domains are part of the same network of users.

84. FireEye reported that a U.S. person ("U.S. Person 1") was associated with American Herald Tribune. According to FireEye's observations of U.S. Person 1's Facebook page, U.S. Person 1 states that s/he is a "columnist at American Herald Tribune" and is also a contributor and analyst at Press TV, an Iranian state-owned media outlet. FireEye also noted U.S. Person 1's articles published on whatsupic.com, which was seized by the FBI in the October 7 Seizure.

85. The FBI believes, however, that U.S. Person 1 and other genuine journalists that have contributed to American Herald Tribune may be unwitting and unaware of the true nature and origins of the inauthentic news site. On January 24, 2020, a U.S. Media Outlet ("U.S. Media Outlet 1") published an article titled "Exclusive: This site pays Americans to write 'news' articles. Signs indicate it originates in Iran," by a U.S. Journalist of U.S. Media Outlet 1. The U.S. Media Outlet 1 article reported that American Herald Tribune publishes in English and pays

Americans to write articles. The article reported that, U.S. Person 1, an American who lives in Salem, Oregon and claims to be a writer with a long career in media, wrote an article critical of the current U.S. President for American Herald Tribune and was paid a couple hundred dollars for an article by the people who run the American Herald Tribune website. According to U.S. Media Outlet 1, U.S. Person 1 is a critic of American foreign policy and says that Iran is "misunderstood" in the U.S. Although U.S. Person 1 admitted to knowingly working with Iranian media in the past, U.S. Person 1 stated that he did not believe that American Herald Tribune was run by Iran.

86. U.S. Media Outlet 1 reported, however, that multiple investigations by American tech companies pointed to the site originating in Iran. A Facebook spokesperson told a subsidiary of U.S. Media Outlet 1 that company staff who looked into the website's Facebook page say it was linked to Iranian state media. Facebook removed the page in 2018. Additionally, Google confirmed to a subsidiary of U.S. Media Outlet 1 that American Herald Tribune was part of a takedown by Google that shut down Gmail and Google ad accounts linked to a malicious network of sites. An employee of FireEye told a subsidiary of U.S. Media Outlet 1 that "indicators, both technical and behavioral," point to American Herald Tribune being linked to an operation run from Iran.

87. Further undermining American Herald Tribune's credibility, American Herald Tribune used a subsidiary of U.S. Person 1's name and his ex-wife ("U.S. Person 2")'s contact information to register **ahtribune.com**, unbeknownst to either. In late 2016, U.S. Person 2 was contacted by a writer complaining that American Herald Tribune had been plagiarizing his work.

The writer told U.S. Person 2 he had found her contact details through the site's registration data. U.S. Person 2 confirmed to U.S. Media Outlet 1 that U.S. Person 1's name and her telephone number had been used to register **ahtribune.com** without her knowledge or consent.

88. The U.S. Media Outlet 1 article also reported that while American Herald Tribune pays some contributors like U.S. Person 1 for original content, it also republishes articles from elsewhere and then lists the people who wrote those articles as contributors to its site.

89. Historical WHOIS records show that on November 29, 2018, **ahtribune.com** listed "irPowerWeb" as a reseller of the domain. Open source research by the FBI revealed that irPowerWeb is a company that provides web hosting and domain registration services in Iran and to more than 300,000 Persian-language websites. Also, on August 23, 2015, **ahtribune.com** utilized irpowerweb.com for its name servers. Historical WHOIS records for irpowerweb.com from September 21, 2016 show a registrant country of Iran and a registrant phone number beginning with Iran-based country code "+98", indicating that **ahtribune.com** was utilizing an Iran-based name server.

90. Historical WHOIS records for **ahtribune.com** further revealed registrant email address PaulCraigRoberts@mail.com. Subscriber and transaction records for PaulCraigRoberts@mail.com showed login activity in September 2020 from IP address 217.218.67.254, and WHOIS searches regarding IP address 217.218.67.254 revealed that it belongs to an Iran-based IP network range named "presstv-ir." In addition, the alternate email for PaulCraigRoberts@mail.com was listed as whatsupicer@gmail.com, which is substantially similar to domain whatsupic.com, seized in the October 7 Seizure.

91. **awdnews.com**. [redacted], **awdnews.com** is operated by or on behalf of the IRGC.

92. According to FireEye, **awdnews.com**, known as "Another Western Dawn News" or "AWD News," describes itself as a journalistic website and appears to have content consistent with GOI interests. For example, **awdnews.com** published material critical of Saudi-led efforts and the Israeli state. The FBI assesses that these articles constitute political activities, as defined by FARA, as they are designed to influence any section of the public within the United States with reference to formulating, adopting, or changing the domestic or foreign policies of the United States, or with reference to the political or public interests, policies, or relations of Iran because they were published in English and directed toward an American audience. FireEye also noted mainstream media outlets The Guardian and U.S. Media Outlet 2 as having recognized AWD News as an inauthentic news site, and as having been attributed to causing a "tense Twitter exchange between Pakistan and Israel," which included a false news article where Israeli defense prime minister supposedly threatened Pakistan with a nuclear attack.

93. Further, FireEye reported that Twitter account @fairobservers–linked to a phone number with the +98 Iranian country code–promoted content on both **awdnews.com** and whatsupic.com, which was seized in the October 7 Seizure.

94. FireEye further reported that **awdnews.com** used the same IP address–67.205.99.12–as Target Domains **al-ahd.net** and **alhiwaraldini.com** and Liberty Front Press domains niletenonline.com and haghighah.com, both of which were seized in the October 7 Seizure.

95. In December 2016, a story appeared in The Guardian, a British news and media outlet, titled "Fake news story prompts Pakistan to issue nuclear warning to Israel" by Emma Graham-Harrison. The Guardian reported that an AWD News article "mis-identified Moshe Ya'alon as the Israeli defence minister when he actually resigned in May, changed the title of a senior official from the Pakistan government and was dotted with grammatical errors and strange syntax." The Guardian further reported that, as a result of the article by AWD News, "Pakistan's defence minister, Khawaja Mohammad Asif, apparently read the article as a genuine threat of a pre-emptive nuclear strike and took to Twitter to warn Israel that 'Pakistan is a nuclear state too.'" The Guardian identified, through a fact-checking organization, that AWD News is a fake news site.

96. Similarly, in December 2016, U.S. Media Outlet 2 reported similar information in an article titled "Fake news sets off Twitter confrontation between Pakistan and Israel." U.S. Media Outlet 2 also reported that it had identified AWD News as a fake news site based on reports from a fact-checking organization.

97. Historical WHOIS records for **awdnews.com** revealed registrant email address kelvinmiddelkoop@hotmail.com, which was used to register Liberty Front Press domains sachtimes.com and whatsupic.com, both of which were seized in the October 7 Seizure.

98. Subscriber and transaction records from Cloudflare revealed that User ID 7967863 was used to access **awdnews.com**, Target Domain **elintelecto.com**, and domains pergiustizia.com and whatsupic.com, both of which were seized in the October 7 Seizure. In addition, Cloudflare records revealed that User ID 3084320 was used to access **awdnews.com**

and Liberty Front Press domain jamekurdi.com, which was seized in the October 7 Seizure.

99. **Criticalstudies.org**. According to an archived version of the website from August 4, 2020, **criticalstudies.org** is an English-language site that claims to have several prominent U.S. person writers, including a former candidate for U.S. President and well-known activist ("U.S. Person 3"), a former candidate for U.S. President and current U.S. Senator ("U.S. Person 4"), and a well-known philosopher and political activist ("U.S. Person 5"). Much of the content of **criticalstudies.org** is critical of the U.S. and U.S. foreign policy and the narratives of several articles on the site include anti-Israel sentiments and views against the current presidential administration. Quds Day 2020 is also featured in its own section on the page. The FBI assesses that these articles constitute political activities, as defined by FARA, as they are designed to influence any section of the public within the United States with reference to formulating, adopting, or changing the domestic or foreign policies of the United States, or with reference to the political or public interests, policies, or relations of Iran.

100. Historical WHOIS records for **criticalstudies.org** showed a legitimate registrant address in Los Angeles, California that open source research revealed is currently the location of a Hilton hotel. The same WHOIS record showed a registration phone number with a +98 Iran country code. Other historical WHOIS records revealed a registrant state and country location of California, U.S. and, nonsensically, California, Iran. Historical WHOIS records further revealed that **criticalstudies.org** used Iran-based name servers ns81.iranhost.com and ns82.iranhost.com as authoritative name servers for resolving its domain name to the appropriate web server.

101. Subscriber and transaction records from Cloudflare revealed that User ID

7335792 was used to access **criticalstudies.org,** Target Domain **rpfront.com,** and Liberty Front Press domain usjournal.net, which was seized in the October 7 Seizure.

[redacted]

102. [redacted] a number of domains were being operated by or on behalf of the IRGC. The IRGC is a Specially Designated National pursuant to OFAC's regulatory authority, meaning that their assets are blocked and U.S. persons are prohibited from doing business with them.[4] [redacted] The domains **al-ahd.net, al-naba.net, ababil.org, albabylon.com, aleppospace.com, alghadeer.tv, alharakah.net, alhiwaraldini.com, darinews.com, elintelecto.com, farhang-press.com, harkarmusulunci.org, iircenter.net, iuvmpixel.com, jordan-times.com, kelkeen.com, kurdrudaw.com, roushd.com, siampublic.com, syria-victory.com, voiceofwadi.com** and **yemenpress.org** are therefore subject to seizure as property which constitutes or is derived from proceeds traceable to violations of IEEPA.

103. **al-ahd.net**. According to an archived and Google-translated version of the website from June 8, 2020, **al-ahd.net** is an Arabic-language news site with the following description at the bottom of the page: "The Yemeni Covenant Agency is concerned with all

[4] IEEPA is content-neutral and does not seek to prohibit or influence speech. It does, however, prohibit the provision of services to sanctioned entities and individuals.

developments and events in the local, Arab, Islamic and international arenas and seeks to promote tolerant culture and promote the values of freedom."

104. Google translations of this website indicate that several news articles featured on June 8, 2020 were critical of Saudi Arabia, the U.S., and Israel. Several articles also appear to have titles sympathetic to Islamic Jihad leadership, such as "Islamic Jihad in Palestine mourns its former Secretary General, Dr. Ramadan Shallah." Middle East regional conflict and Coronavirus were also covered according to observed translations. Open source research by the FBI revealed linked Twitter account "ahdyemenia," which was suspended by Twitter, and YouTube channel UCEpBoAGWcouTUMM2f4RLWLw, which was terminated for a violation of YouTube's Terms of Service.

105. According to FireEye, **al-ahd.net** describes itself as an independent Yemeni news agency and has content consistent with Iranian interests, for example, anti-U.S. President, anti-Israel, and anti-Saudi messaging. FireEye also noted that **al-ahd.net** registrant email address domain@sepehrict.ir is associated with Iranian company Sepehr ICT located in Tehran, which was confirmed in open source research by the FBI. Further, FireEye noted that former registrant email address abdullatifmansour@hotmail.com was used to register several other sites, including nilenetonline.com, which was seized by the FBI in the October 7 Seizure. FireEye also reported that IP address 67.205.99.12 was used by Target Domains **al-ahd.net**, **awdnews.com**, and **alhiwaraldini.com**, as well as domains whatsupic.com, nilenetonline.com, and haghighah.com, which were seized by the FBI in the October 7 Seizure.

106. Historical WHOIS records for **al-ahd.net** revealed a registrant location of Qom,

Iran, a registrant phone number with a +98 Iran country code, and a registrant email address ending in ".ir", the internet country code top-level domain for Iran.

107. Subscriber and transaction records from Cloudflare revealed that User ID 7070033 was used to access **al-ahd.net,** Target Domains **alhiwaraldini.com, iircenter.net, ababil.org, alharakah.net, harkarmusulunci.org, mediaadil.com, voiceofwadi.com** and **yemenpress.org,** and domains 3adalah.com, aden-alyoum.com, adentimes.net, ageofpakistan.com, al-sufia.com, almasirahpress.com, almasirahtv.com, altanzil.net, haghighah.com, libyaalmokhtar.com, nthnews.net, puketnews.com, qudspal.com and yemaniate.net, which were seized in the October 7 Seizure.

108. **al-naba.net**. According to an archived and Google-translated version of the website from March 20, 2020, **al-naba.net** describes itself as "[a] comprehensive news site where you follow the latest developments in Yemeni, Arab and international events around the clock, and continuous coverage of military and political news." Translations also indicated the site featured articles with anti-Saudi and anti-Israel sentiments and references to "The Zionist enemy," coronavirus, and conflicts in Yemen.

109. Subscriber and transaction records from Cloudflare revealed that User ID 6325113 was used to access **al-naba.net**, Target Domain **jordan-times.com**, and domains aftruth.com, ageofpakistan.com, al-hadath24.com, alsudanalyoum.com, altanzil.net, raitunisia.com and theleadersnews.com, which were seized in the October 7 Seizure. As described throughout, the FBI's investigation has revealed that the user(s) of the Target Domains and the domains subject to the October 7 Seizure frequently had overlapping subscriber

information and user access information, which is indicative of multiple domains being accessed by a set of common users. The FBI assesses that this is consistent with a group of IRGC actors operating multiple domains as part of a concerted effort, which is reflected in the consistency in the content supporting GOI policies across all of the Target Domains. The FBI assesses that, given the state-sponsored nature of the IRGC's covert influence campaign, it is extremely unlikely that the IRGC would allow an individual not involved with the campaign to access multiple domains used in furtherance of the campaign, and that a common User ID accessing multiple Target Domains is, therefore, a major indicator that all domains accessed by that User ID are being used by or on behalf of the IRGC. As a result, there is probable cause that **al-naba.net** is used by or on behalf of the IRGC because the content of the domain is consistent with the IRGC covert influence campaign and User ID 6325113.

110. **ababil.org**. According to an archived and Google-translated version from April 19, 2020, **ababil.org** is a Spanish-language news site that claims to represent a non-governmental Palestinian organization. According to **ababil.org**, "[t]he ABABIL Site is a non-governmental Palestinian organization that works in the dissemination of culture, history, traditions, news and the Palestinian cause. It is a non-profit organization, financed through the contribution and work of its own members." A webpage included a phrase translating to "Stop Palestinian Holocaust" and a banner containing the hashtag "#RESISTENCIA_ES_VISTORIA"–translated to "resistance is victory"–next to an image of raised fists above the text "Palestina" or "Palestine" in Spanish. Another **ababil.org** webpage contained the text "The peoples of Latin America and the Caribbean in solidarity with Palestine"

and the url "Historiadepalestina.com." Featured content includes anti-Israel, anti-U.S., and pro-Palestine narratives.

111. Subscriber and transaction records from Cloudflare revealed that User ID 7070033 was used to access **ababil.org,** Target Domains **al-ahd.net, alhiwaraldini.com, iircenter.net, alharakah.net, harkarmusulunci.org, mediaadil.com, voiceofwadi.com** and **yemenpress.org**, and domains 3adalah.com, aden-alyoum.com, adentimes.net, ageofpakistan.com, al-sufia.com, almasirahpress.com, almasirahtv.com, altanzil.net, haghighah.com, libyaalmokhtar.com, nthnews.net, puketnews.com, qudspal.com and yemaniate.net, which were seized in the October 7 Seizure.

112. **albabylon.com**. According to an archived and Google-translated version of the website from May 11, 2019, **albabylon.com** is an Arabic-language site with a copyright for the "Christian Movement in Iraq." According to Google translations, the content of the site is pro-Popular Mobilization Forces ("PMF"). PMF is an Iraqi state-sponsored organization that various open sources indicate is backed by Iran.

113. Subscriber and transaction records from Cloudflare revealed that User ID 5914850 was used to access **albabylon.com,** Target Domains **alhiwaraldini.com, alghadeer.tv** and **siampublic.com**, and domains alsudanalyoum.com, beritadunia.net, hindkhabar.com, iraqnewsservice.com, libyaalmokhtar.com and raitunisia.com, which were seized in the October 7 Seizure.

114. **aleppospace.com**. According to an archived and Google-translated version of the website from June 28, 2020, **aleppospace.com** is an Arabic-language site that hosts news content

primarily critical of the U.S. and Saudi Arabia. Of note, the Caesar Syria Civilian Protection Act–United States legislation that sanctions the Syrian government–was criticized and associated with the "starvation of Syrians under the umbrella of freedoms." Open source research by the FBI identified associated Facebook profile "aleppo.space.new2020," which included political cartoons criticizing the U.S., the current POTUS, and Israel.

115. Subscriber and transaction records from Cloudflare revealed that User ID 10098098 was used to access **aleppospace.com,** Target Domain **syria-victory.com**, and domain syria-scope.com, which was seized in the October 7 Seizure.

116. Historical WHOIS records show that Target Domain **aleppospace.com** registrant emails aminbaik88@gmail.com and m.h.memo1992@gmail.com were used to register Target Domain **syria-victory.com**, showing that these accounts were accessed by the same user(s).

117. **alghadeer.tv**. According to an archived and Google-translated version of the website from August 26, 2020, en.alghadeer.tv is the English-language news site for **alghadeer.tv**. The site covers various topics, mainly centering on Middle East and world events. Some articles were critical of the current U.S. President and U.S. foreign policy, while anti-Israel narratives were also observed. A page banner included political cartoons regarding the current-U.S. President and the U.S. At least three articles appeared to have pro-Iran sentiments regarding oil and sanctions, specifically, opposition to U.S. sanctions on Iran. The English-language version of **alghadeer.tv** identifies itself as an "Iraqi Arab media commission seeking to spread the noble principles, values and promote the culture of unity among people and spread the spirit of tolerance and dialogue between different cultures."

118. Historical WHOIS records for **alghadeer.tv** revealed a registrant location of Tehran, Iran and a registrant phone number with a +98 Iran country code.

119. Subscriber and transaction records from Cloudflare revealed that User ID 5914850 was used to access **alghadeer.tv,** Target Domains **albabylon.com, alhiwaraldini.com** and **siampublic.com**, and domains alsudanalyoum.com, beritadunia.net, hindkhabar.com, iraqnewsservice.com, libyaalmokhtar.com and raitunisia.com, which were seized in the October 7 Seizure.

120. **alharakah.net**. According to an archived and Google-translated version of the website from March 31, 2019, **alharakah.net** is an Arabic-language website that supports Ibrahim Zakzaky, an imprisoned outspoken and prominent Shi'a Muslim leader who desired to establish an Islamic state in Nigeria.

121. Historical WHOIS records for **alharakah.net** revealed a registrant location of Qom, Iran and a registrant phone number with a +98 Iran country code. These records further revealed a registrant email address of walasr5@yahoo.com, which was also used in a historical registration of Target Domain **farhang-press.com**. Historical WHOIS records further revealed a registrant contact of "getpanel.ir." A WHOIS search for "getpanel.ir" revealed a location of Qom, Iran as well as additional Iranian contact information.

122. Subscriber and transaction records from Cloudflare revealed that User ID 7070033 was used to access **alharakah.net,** Target Domains **al-ahd.net, alhiwaraldini.com, iircenter.net, ababil.org, harkarmusulunci.org, mediaadil.com, voiceofwadi.com** and **yemenpress.org**, and domains 3adalah.com, aden-alyoum.com, adentimes.net,

ageofpakistan.com, al-sufia.com, almasirahpress.com, almasirahtv.com, altanzil.net, haghighah.com, libyaalmokhtar.com, nthnews.net, puketnews.com, qudspal.com and yemaniate.net, which were seized in the October 7 Seizure.

123. **alhiwaraldini.com**. According to an archived and Google-translated version of the website from March 31, 2020, **alhiwaraldini.com** was an Arabic-language site that included language translating to "Association for Religious Dialogue for Unity." Associated Facebook profile "alhiwaraldini" identified the association as a non-governmental organization with Iranian phone number +98 25 1775 8015.

124. FireEye reported that **alhiwaraldini.com** used the same IP address–46.4.69.232–as Liberty Front Press domains libyaalmokhtar.com and qudspal.com, both of which were seized in the October 7 Seizure. FireEye further reported that **alhiwaraldini.com** used the same–IP address 5.9.137.45–as Liberty Front Press domains libyaalmokhtar.com, raitunisia.com and alsudanalyoum.com, all of which were seized in the October 7 seizure. In addition, **alhiwaraldini.com** used the same IP address–67.205.99.12–as Target Domains **al-ahd.net** and **awdnews.com** and Liberty Front Press domains niletenonline.com and haghighah.com, both of which were seized in the October 7 Seizure.

125. Historical WHOIS records for **alhiwaraldini.com** revealed registrant locations of the cities of Qom, Tehran and Mashhad, Iran; a registrant phone number with a +98 Iran country code; Iran-based name server pasargad.irandns.com; and a registrant email address ending in ".ir", the internet country code top-level domain for Iran.

126. Subscriber and transaction records from Cloudflare revealed that User ID

7070033 was used to access **alhiwaraldini.com,** Target Domains **al-ahd.net, iircenter.net, ababil.org, alharakah.net, harkarmusulunci.org, mediaadil.com, voiceofwadi.com** and **yemenpress.org**, and domains 3adalah.com, aden-alyoum.com, adentimes.net, ageofpakistan.com, al-sufia.com, almasirahpress.com, almasirahtv.com, altanzil.net, haghighah.com, libyaalmokhtar.com, nthnews.net, puketnews.com, qudspal.com and yemaniate.net, which were seized in the October 7 Seizure.

127. Also discussed above, subscriber and transaction records from Cloudflare revealed that User ID 5914850 was used to access **alhiwaraldini.com,** Target Domains **albabylon.com, alghadeer.tv** and **siampublic.com**, and domains alsudanalyoum.com, beritadunia.net, hindkhabar.com, iraqnewsservice.com, libyaalmokhtar.com and raitunisia.com, which were seized in the October 7 Seizure.

128. **darinews.com**. Target Domain **darinews.com** features news articles from July 2020 and is a Persian-language news site according to Google translate. Topics covered include: Middle East conflicts and events; coronavirus (U.S. cases; Russia accused of stealing a vaccine from the UK); an Indiana steel plant explosion in the U.S.; and U.S. and European views and policies regarding Hizbollah.

129. Historical WHOIS records for **darinews.com** revealed a registrant location of Mashhad, Iran and a registrant phone number with a +98 Iran country code. Historical WHOIS records further revealed that the website used name servers ns14.vatandata.com and ns15.vatandata.com as authoritative name servers for resolving its domain name to the appropriate web server. Open source research revealed that Vatan Data is an Iran-based web

hosting company.

130. Historical WHOIS records show that Target Domain **darinews.com** registrant email moosavi.2010@gmail.com was used to register Target Domain **roushd.com**, indicating they were registered by the same user.

131. Subscriber and transaction records from Cloudflare revealed that User ID 10120699 was used to access **darinews.com,** Target Domains **farhang-press.com, roushd.com, kelkeen.com,** and **studiesaf.com**, and domain risolattj.com, which was seized in the October 7 Seizure.

132. **elintelecto.com**. According to an archived and Google-translated version of the website from September 19, 2018, Target Domain **elintelecto.com** targets a Spanish-speaking audience and has content in line with Iranian messaging. For example, it includes anti-Israeli articles titled and translated to "The beginning of the end of Netanyahu's political life" and "Israeli youth watch and applaud the killing of Palestinians in Gaza."

133. Subscriber and transaction records from Cloudflare revealed that User ID 7967863 was used to access **elintelecto.com**, Target Domain **awdnews.com**, and domains pergiustizia.com and whatsupic.com, which were seized in the October 7 Seizure.

134. **farhang-press.com**. According to an archived and Google-translated version of the website from March 3, 2020, **farhang-press.com** is a Persian-language site that centers on culture and the arts as they relate to Afghanistan.

135. Historical WHOIS records for **farhang-press.com** revealed a registrant location of Qom, Iran and a registrant phone number with a +98 Iran country code. Historical WHOIS

records further revealed a registrant email address of walasr5@yahoo.com, which was also used in a historical registration of Target Domain **alharakah.net**.

136. Subscriber and transaction records from Cloudflare for **farhang-press.com** revealed Iran-based IP addresses 5.114.176.54, 5.113.16.102 and 185.212.192.209. In addition, Cloudflare records revealed that User ID 10120699 was used to access **farhang-press.com,** Target Domains **roushd.com, darinews.com, kelkeen.com,** and **studiesaf.com**, and domain risolattj.com, which was seized in the October 7 Seizure.

137. **harkarmusulunci.org**. According to an archived and Google-translated version of the website from August 8, 2020, **harkarmusulunci.org** is a Hausa-language site that contains some English, with the target audience likely being Nigeria. English text in a banner menu included the hashtag #FreeZakzaky. According to open source research, Ibrahim Zakzaky is an imprisoned outspoken and prominent Shi'a Muslim leader in Nigeria who desired to establish an Islamic state in Nigeria. The content of **harkarmusulunci.org** mainly centers on Islam, Quds Day and Ghadeer Day, which commemorates a sermon delivered by the Islamic prophet Muhammad and celebrated by Shi'ite Muslims.

138. Historical WHOIS records for **harkarmusulunci.org** revealed registrant locations of Tehran, Iran and Mashhad, Iran; a registrant phone number with a +98 Iran country code; and a registrant email address ending in ".ir", the internet country code top-level domain for Iran.

139. Subscriber and transaction records from Cloudflare revealed that User ID 7070033 was used to access **harkarmusulunci.org,** Target Domains **al-ahd.net, alhiwaraldini.com, iircenter.net, ababil.org, alharakah.net, mediaadil.com,**

voiceofwadi.com and **yemenpress.org**, and domains 3adalah.com, aden-alyoum.com, adentimes.net, ageofpakistan.com, al-sufia.com, almasirahpress.com, almasirahtv.com, altanzil.net, haghighah.com, libyaalmokhtar.com, nthnews.net, puketnews.com, qudspal.com and yemaniate.net, which were seized in the October 7 Seizure.

140. **iircenter.net**. As of October 22, 2020, **iircenter.net** returned a page indicating that the site's IP address may have changed, the server may be misconfigured, or the site may have a new server. Notwithstanding its inability to resolve, website operators can reconstitute websites at any time to display content. An excerpt of **iircenter.net** in search results displayed Arabic text that translated to: "Dr. Iqbal Center for Research and Studies" and "The Office of the Supreme Religious Authority, Mr. Ali Al-Hussaini Al-Sistani, sent a message to the Iraqi people due to the great spread of Corona in the country."

141. Subscriber and transaction records from Cloudflare for **iircenter.net** revealed that a user attempted to change their password from Iran-based IP address 5.160.10.11 and login from Iran-based IP address 5.160.10.72. Further, Cloudflare records for **iircenter.net** revealed user account registrant email iuvmdev@gmail.com. Historical WHOIS records revealed that iuvmdev@gmail.com was used to register IUVM domains iuvmdaily.com and iuvmdaily.net, indicating that **iircenter.net** and IUVM domains are controlled by the same user(s).

142. Subscriber and transaction records from Cloudflare revealed that User ID 7070033 was used to access **iircenter.net,** Target Domains **al-ahd.net, alhiwaraldini.com, ababil.org, alharakah.net, harkarmusulunci.org, mediaadil.com, voiceofwadi.com** and **yemenpress.org**, and domains 3adalah.com, aden-alyoum.com, adentimes.net,

ageofpakistan.com, al-sufia.com, almasirahpress.com, almasirahtv.com, altanzil.net, haghighah.com, libyaalmokhtar.com, nthnews.net, puketnews.com, qudspal.com and yemaniate.net, all of which were seized in the October 7 Seizure.

143. **iuvmpixel.com**. According to the Atlantic Council's Digital Forensic Research Lab ("DFRLab") on atlaniccouncil.org, the International Union of Virtual Media ("IUVM") posted exclusively pro-Iranian content as it "laundered content from Iranian state media, lending it an air of credibility by stripping the affiliation, thereby enabling it to be passed to less discerning readers as (ostensibly) credible." DFRLab reported that IUVM offered links to dozens of "member" websites, all of which were clearinghouses for Iranian propaganda. IUVM regularly tweaked and republished official Islamic Republic of Iran Broadcasting ("IRIB") stories, only to have its articles republished, in turn, by other Iranian propaganda mills.

144. FireEye reported IUVM is a "network of websites and social media accounts that appears to promote Iranian state messaging and other material directly in line with Iranian interests." FireEye identified **iuvmpixel.com** as part of the IUVM and Liberty Front Press networks, as well as domains iuvmpress.com, iuvmtech.com, iuvmtv.com and iuvm.org, all of which were seized in the October 7 Seizure. According to FireEye, **iuvmpixel.com** was used by the IUVM network to "convey photos and breaking news to the public." In an April 2020 report, Graphika, a U.S.-based social network analysis company, provided an in-depth look at certain IUVM sites titled "Iran's IUVM Turns to Coronavirus." The article featured **iuvmpixel.com**, as well as iuvmpress.com and iuvmtv.com, both of which were seized in the October 7 Seizure.

145. Subscriber and transaction records from Cloudflare for **iuvmpixel.com** revealed

logins from Iran-based IP addresses 185.212.192.225 and 5.114.176.54. Moreover, its name indicates its association with the broader IUVM network.

146. As discussed above, IUVM was designated as a Specially Designated National pursuant to Executive Order 13848 for being owned or controlled by the IRGC-QF.

147. **jordan-times.com**. FireEye identified **jordan-times.com** as part of the Liberty Front Press network. According to FireEye, **jordan-times.com** ("Jordan Times") has media content focused on Jordan, but provides anti-Israel, pro-Palestinian, anti-ISIS, and anti-Trump messaging in line with Iranian interests. FireEye noted that Jordan Times associated Twitter Account @Jjordantimes was linked to a phone number with the +98 Iran country code, although it claims its location is in Jordan.

148. Subscriber and transaction records from Cloudflare for **jordan-times.com** revealed logins from Iran-based IP addresses 2.178.184.9, 5.112.206.108 and 2.178.26.17. Cloudflare records further revealed that User ID 6325113 was used to access **jordan-times.com**, Target Domain **al-naba.net**, and domains aftruth.com, ageofpakistan.com, al-hadath24.com, alsudanalyoum.com, altanzil.net, raitunisia.com and theleadersnews.com, which were seized in the October 7 Seizure.

149. **kelkeen.com**. According to an archived and Google-translated version of the website from February 13, 2020, **kelkeen.com** is a Persian-language news site. Narratives of featured articles included anti-Saudi and pro-Iran sentiments and were critical of the U.S. and Israel. The site described itself as "[t]he socio-cultural foundation of Afghans living in the Islamic Republic of Iran, since its establishment, thanks to God and with a young, committed and

valuable staff, has taken great steps towards creating a new Islamic civilization with the help of faithful, committed and professional Afghan youth."

150. Historical WHOIS records for **kelkeen.com** revealed a registrant phone number with the +98 Iran country code and Iran-based name server directi1.irandns.com.

151. Subscriber and transaction records from Cloudflare revealed that User ID 10120699 was used to access **kelkeen.com,** Target Domains **farhang-press.com, roushd.com, darinews.com** and **studiesaf.com**, and domain risolattj.com, which was seized in the October 7 Seizure.

152. **kurdrudaw.com**. According to an archived and Google-translated version of the website from February 4, 2020, **kurdrudaw.com** is likely a Persian-language site that provides news related to Iraq and Iran.

153. Historical WHOIS records for **kurdrudaw.com** revealed a registrant location of Mashhad, Iran, a registrant phone number with the +98 Iran country code, and Iran-based nameserver directi1.irandns.com and directi2.irandns.com.

154. Subscriber and transaction records from Cloudflare revealed that User IDs 10169714 and 15095444 were used to access **kurdrudaw.com** and jamekurdi.com, which was seized in the October 7 Seizure.

155. **roushd.com**. Historical WHOIS records for **roushd.com** revealed a registrant location of Qom, Iran and a registrant phone number with the +98 Iran country code. Historical WHOIS records further revealed that the website used name servers ns1.vatandata.com and ns2.vatandata.com as authoritative name servers for resolving its domain name to the appropriate

web server. Open source research revealed that Vatan Data is an Iran-based web hosting company.

156. Subscriber and transaction records from Cloudflare for **roushd.com** revealed logins from Iran-based IP addresses 5.160.10.72, 5.114.176.54 and 185.212.192.209. Cloudflare records further revealed that User ID 10120699 was used to access **roushd.com,** Target Domains **farhang-press.com, darinews.com, kelkeen.com** and **studiesaf.com**, and domain riolattj.com, which was seized in the October 7 Seizure.

157. Historical WHOIS records show that Target Domain **roushd.com** registrant email moosavi.2010@gmail.com was used to register Target Domain **darinews.com**, indicating they were registered by the same user.

158. **siampublic.com**. Open source research by the FBI on Target Domain **siampublic.com** reveals through an March 10, 2018 archive and machine translation that it purports itself as a "Thai News Agency." Content includes anti-Israeli and anti-U.S. content consistent with Iranian messaging. For example, it includes an article titled, according to machine translation "The Special Report 'No Death, No Life' is Israel's policy against the Gaza people" and "Analysis of the world: why the US must be the enemy of Iran's Islamic revolution?"

159. Subscriber and transaction records from Cloudflare revealed that User ID 5914850 was used to access **siampublic.com,** Target Domains **albabylon.com, alhiwaraldini.com** and **alghadeer.tv**, and domains, alsudanalyoum.com, beritadunia.net, hindkhabar.com, iraqnewsservice.com, libyaalmokhtar.com and raitunisia.com, which were

seized in the October 7 Seizure.

160. **syria-victory.com**. Open source research by the FBI revealed that Target Domain **syria-victory.com** targeted a Syrian audience. According to a machine translation of an archived record of the website from April 27, 2019, several articles in line with Iranian interests were messaged; for example, articles titled "Russia ... America is still supporting terrorists in Syria until now" and "Iran ... US forces in West Asia are on the terrorist list."

161. Historical WHOIS records show that Target Domain **syria-victory.com** registrant emails aminbaik88@gmail.com and m.h.memo1992@gmail.com were used to register Target Domain **aleppospace.com**, showing that these accounts were accessed by the same user(s).

162. Subscriber and transaction records from Cloudflare revealed that User ID 10098098 was used to access **syria-victory.com,** Target Domain aleppospace.com, and domain syria-scope.com, which was seized in the October 7 Seizure.

163. **voiceofwadi.com**. Open source research by the FBI revealed that Target Domain **voiceofwadi.com** ("Voice of Wadi") has news targeting the Kashmir region. Open source research by the FBI identified associated Facebook account voiceofwadi. The "About" section for Facebook account voiceofwadi states that "Voiceofwadi is a non-profit organisation that collects unbiased news from Kashmir and around the world" and lists itself as a "News & Media website." While much of the news reported revolved around the Kashmir region, there was also content in line with Iranian interests. For example, the Facebook account featured an article from **voiceofwadi.com** regarding Iran's Press TV anchor Marsieh Hashemi regarding an event where she was detained by the FBI, stating that she was "jailed in #US, denied halal food, #hijab

removed against her will." Press TV is an Iranian state-owned news company.

164. There was also a video on this website from Islamic Pulse that esteemed prominent Iranian leaders, including quotes from Ayatollah Knoei, Ayatollah Sistani, Ayatollah Khomeini, and Imam Khamenei. Further, the Facebook account featured a picture captioned, "From the most militarized zone of world Kashmir, to the biggest open-air prison of world Palestine, [sic] opperssors are same" and a picture of a helicopter titled "US Helicopter Kills 7 Iraqi Civilians in Al-Anbar [and] US helicopter gunship had targeted several civilian vehicles in the al-Baghdadi neighborhood of Ramadi."

165. Subscriber and transaction records from Cloudflare revealed that User ID 7070033 was used to access **voiceofwadi.com,** Target Domains **al-ahd.net, alhiwaraldini.com, iircenter.net, ababil.org, alharakah.net, harkarmusulunci.org, mediaadil.com** and **yemenpress.org**, and domains 3adalah.com, aden-alyoum.com, adentimes.net, ageofpakistan.com, al-sufia.com, almasirahpress.com, almasirahtv.com, altanzil.net, haghighah.com, libyaalmokhtar.com, nthnews.net, puketnews.com, qudspal.com and yemaniate.net, which were seized in the October 7 Seizure.

166. **yemenpress.org**. According to FireEye, Target Domain **yemenpress.org** ("Yemen Press") is a news site focused on Yemeni issues but has content in line with Iranian interests, including reporting on "American-Saudi aggression" in Yemen. Additionally, FireEye noted that associated Twitter account @Yemenpress_org–which also promoted material from Target Domain **awdnews.com–**was linked to a phone number with an Iranian country code.

167. According to an archived and Google-translated version of the website from

August 20, 2020, **yemenpress.org** is an English-language news site that claimed to focus on Yemen. The site's description sates, "The Yemen Press brings its readers the best in breaking news and analysis on politics. With in-depth news coverage, diligent investigative reporting and thoughtful commentary, we'll make sure you're always in the know about Yemen's latest exploits." The content on the site included anti-U.S., anti-Israel, and anti-Saudi narratives. One article depicted the U.S. as disregarding humanitarian crises in Yemen, while another claimed that Wikileaks proved Hilary Clinton sold weapons to ISIS. One article also centered on mistrust of the U.S. election system and was titled, "US election: Round 1 of voter suppression a draw." On Israel and Saudi Arabia, articles primarily centered on their aggressions in the region and towards Yemen.

168. Subscriber and transaction records from Cloudflare revealed that User ID 7070033 was used to access **yemenpress.org,** Target Domains **al-ahd.net, alhiwaraldini.com, iircenter.net, ababil.org, alharakah.net, harkarmusulunci.org, mediaadil.com** and **voiceofwadi.com**, and domains 3adalah.com, aden-alyoum.com, adentimes.net, ageofpakistan.com, al-sufia.com, almasirahpress.com, almasirahtv.com, altanzil.net, haghighah.com, libyaalmokhtar.com, nthnews.net, puketnews.com, qudspal.com and yemaniate.net, which were seized in the October 7 Seizure.

Additional Domains Identified by the FBI as Used by the IRGC Covert Influence Campaign and which are Property Constituting or Derived from Proceeds Traceable to Violations of IEEPA

169. **iuvm-sy.net**. In an April 2020 report, Graphika, a U.S.-based social network analysis company, provided an in-depth look at IUVM sites iuvmpress.com and iuvmtv.com, both of which were seized in the October 7 Seizure, and Target Domain **iuvmpixel.com**.

Graphika reported that YouTube channel IUVM Syria, which has been suspended by YouTube, also appeared to belong to the IUVM network. Open source research revealed that YouTube channel IUVM Syria is likely associated with **iuvm-sy.net** based on comparisons between videos posted on the channel and the titles of articles featured on **iuvm-sy.net**. In addition, an archived version of the homepage for **iuvm-sy.net** displayed a logo with the words "IUVM Syria." Open source research by the FBI revealed messaging in line with Iranian interests. For example, **iuvm-sy.net** displays an image of a U.S. flag showing silhouettes of officers demonstrating aggressive police tactics and captioned "'I cannot breathe,' is the word of all those who have been victims of American politics in the world." Other images include a picture of a Saudi Leader superimposed on an Israeli Star of David and a picture with an Iranian flag next to an upside-down U.S. flag.

170. As previously discussed, IUVM was designated as a Specially Designated National pursuant to Executive Order 13848 for being owned or controlled by the IRGC-QF. Accordingly, and as noted above, websites associated with IUVM are subject to seizure as property constituting or traceable to the proceeds of a violation of IEEPA.

171. **mediaadil.com**. Open source research by the FBI regarding Target Domain mediaadil.com ("Media Adil") revealed a target Malaysian audience. The website posted articles in line with Iranian interests; for example, an article titled, "The opening of an Iranian supermarket in Venezuela disrupted the Trump administration." Further, **mediaadil.com** has an associated Facebook account @mediaadil which identifies as a news and media website. The Facebook account posts **mediaadil.com** articles and anti-Trump, anti-Saudi, and anti-Israeli

messaging, consistent with Iran propaganda. For example, several images posted by the Facebook account include the hashtag "#deleteIsrael."

172. Historical WHOIS records for **mediaadil.com** revealed registrant email address jeddoub_21@yahoo.com, which was also used to register domain hpiiran.com. Additional open source research by the FBI identified hpiiran.com-associated Facebook page @hpiiran, which listed its location as Qom, Iran, indicating an Iran-based origin for **mediaadil.com**.

173. As discussed above, subscriber and transaction records from Cloudflare revealed that User ID 7070033 was used to access **mediaadil.com,** Target Domains **al-ahd.net, alhiwaraldini.com, iircenter.net, ababil.org, alharakah.net, harkarmusulunci.org, voiceofwadi.com** and **yemenpress.org**, and domains 3adalah.com, aden-alyoum.com, adentimes.net, ageofpakistan.com, al-sufia.com, almasirahpress.com, almasirahtv.com, altanzil.net, haghighah.com, libyaalmokhtar.com, nthnews.net, puketnews.com, qudspal.com and yemaniate.net, which were seized in the October 7 Seizure. As this domain (i) has overlapping subscriber/transaction information with other identified Target Domains and domains seized in the October 7 Seizure, and (ii) engages in activities consistent with the IRGC covert influence campaign, the FBI assesses that this domain is used by or on behalf of the IRGC.

174. **studiesaf.com**. According to an archived and Google-translated version of the website from August 11, 2020, **studiesaf.com** stated in Persian that "The Afghanistan Studies Collection is a network of multinational researchers whose goal is to provide specific, up-to-date and scientific analysis of the situation and issues in Afghanistan." Google translations also identified content as generally in line with Iranian interests.

175. For example, Iran's role in peace talks and diplomacy in the region was portrayed positively while that of the U.S. was criticized. Regarding Iran, the site stated that "Afghanistan's neighborhood, as well as its location in the sphere of Iranian civilization, makes Tehran play an important and influential role in the Afghan peace process through active diplomacy." Regarding the U.S., the site asked "Was the agreement between the Taliban and the United States due to the inability of the United States to defeat the group, or was the United States unwilling to eliminate the Taliban?"

176. Reporting that was likely meant to sow discord and disinformation regarding the U.S. abroad was also observed in an archived and Google-translated version of the website from August 11, 2020: "Russia's foreign minister says US and NATO planes are smuggling narcotics from Afghanistan" and "With the withdrawal of some US troops from Afghanistan, the issue of their war crimes has been brought to the attention of the media and legal circles in the world, and it is believed that the time has come to investigate the various crimes of US and NATO troops in Afghanistan."

177. Subscriber and transaction records from Cloudflare revealed that User ID 10120699 was used to access **studiesaf.com,** Target Domains **farhang-press.com, roushd.com, darinews.com** and **kelkeen.com**, and domain risolattj.com, which was seized in the October 7 Seizure. As this domain (i) has overlapping subscriber/transaction information with other identified Target Domains and at least one domain seized in the October 7 Seizure, and (ii) engages in activities consistent with the IRGC covert influence campaign, the FBI assesses that this domain is used by or on behalf of the IRGC.

Conclusion

178. As described throughout, there is probable cause to believe that the Target Domains are being used by or on behalf of the GOI and the IRGC to conduct a covert influence and disinformation campaign both within and without the United States to the benefit of the GOI. The services provided by U.S. domain name registration service providers for each of the Target Domains is a violation of IEEPA because the services provided are prohibited by U.S. sanctions targeting the GOI and the IRGC. As described above, each of the domains was fraudulently registered because each is being used by or on behalf of the IRGC and this critical information was omitted from the registration if any of the U.S. service providers had known that the domains were to be used by or on behalf of the IRGC, they would not have been able to provide the domain name registration services due to U.S. sanctions. Additionally, Target Domains **criticalstudies.org, awdnews.com, ahtribune.com** and **rpfront.com** are also subject to seizure as they are property that constitutes or is derived from proceeds traceable to violations of FARA. As a result, there is probable cause to believe that the Target Domains are subject to civil and criminal forfeiture because they constitute or are derived from proceeds traceable to a violation of the Subject Offenses, namely, the use of U.S. domain registration services in violation of IEEPA and/or FARA.

SEIZURE PROCEDURE

179. As detailed in Attachment A, upon execution of the seizure warrant, the registry for Target Domains **ahtribune.com, al-ahd.net, al-naba.net, albabylon.com, aleppospace.com, alghadeer.tv, alharakah.net, alhiwaraldini.com, awdnews.com,**

darinews.com, elintelecto.com, farhang-press.com, iircenter.net, iuvm-sy.net, iuvmpixel.com, jordan-times.com, kelkeen.com, kurdrudaw.com, mediaadil.com, roushd.com, rpfront.com, siampublic.com, studiesaf.com, syria-victory.com and **voiceofwadi.com,** VeriSign, Inc., headquartered at 12061 Bluemont Way, Reston, Virginia, shall be directed to restrain and lock the relevant Target Domains pending transfer of all right, title, and interest in the Target Domains to the United States upon completion of forfeiture proceedings, to ensure that changes to the Target Domains cannot be made absent court order or, if forfeited to the United States, without prior consultation with the U.S. Department of Justice.

180. As detailed in Attachment B, upon execution of the seizure warrant, the registry for Target Domains **ababil.org, criticalstudies.org, harkarmusulunci.org** and **yemenpress.org**, Public Internet Registry, headquartered at 1775 Wiehle Avenue, Suite 200 Reston, Virginia 20190, shall be directed to restrain and lock the relevant Target Domains pending transfer of all right, title, and interest in the relevant Target Domains to the United States upon completion of forfeiture proceedings, to ensure that changes to the relevant Target Domains cannot be made absent court order or, if forfeited to the United States, without prior consultation with the U.S. Department of Justice.

CONCLUSION

181. For the foregoing reasons, I submit that there is probable cause to believe that the Target Domains are used in and/or intended to be used in facilitating and/or committing the Subject Offenses. Accordingly, the Target Domains are subject to forfeiture to the United States pursuant to 21 U.S.C. § 853, and 18 U.S.C. § 981, as incorporated by 28 U.S.C. § 2461(c), and I

respectfully request that the Court issue seizure warrants for the Target Domains. Because the warrant will be served VeriSign and the Public Internet Registry, which control the Target Domains and, thereafter, at a time convenient, will transfer control of the Target Domains to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night. Finally, and in order to protect the ongoing investigation and in consideration that much of the information set forth above is not otherwise publicly available, I respectfully request that this Affidavit be filed and kept under seal until further order of this Court.

ATTACHMENT A

With respect to SUBJECT DOMAIN NAMES **ahtribune.com, al-ahd.net, al-naba.net, albabylon.com, aleppospace.com, alghadeer.tv, alharakah.net, alhiwaraldini.com, awdnews.com, darinews.com, elintelecto.com, farhang-press.com, iircenter.net, iuvm-sy.net, iuvmpixel.com, jordan-times.com, kelkeen.com, kurdrudaw.com, mediaadil.com,, roushd.com, rpfront.com, siampublic.com, studiesaf.com, syria-victory.com**and **voiceofwadi.com**, VERISIGN, who is the top-level domain registry for the SUBJECT DOMAIN NAMES, shall take the following actions to effectuate the seizure of SUBJECT DOMAIN NAME:

1) Take all reasonable measures to redirect the domain names to a substitute server at the direction of the U.S. GOVERNMENT LAW ENFORCEMENT, by updating the authoritative nameservers for the SUBJECT DOMAIN NAMES to any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to the Registry.

2) Prevent any further modification to, or transfer of, SUBJECT DOMAIN NAMES pending transfer of all right, title, and interest in SUBJECT DOMAIN NAMES to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN NAMES cannot be made absent court order or, if forfeited to the United States, without prior consultation with U.S. GOVERNMENT LAW ENFORCEMENT.

3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.

4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

5) The Government will display a notice on the website to which the SUBJECT DOMAIN NAMES will resolve. That notice will consist of law enforcement emblems and the following, or similar, text:

"The domain for SUBJECT DOMAIN NAME has been seized by the United States Government in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981, 982, and 50 U.S.C. 1701-1705 as part of a law enforcement action by the U.S. Department of Justice."

ATTACHMENT B

With respect to SUBJECT DOMAIN NAMES **ababil.org, criticalstudies.org, harkarmusulunci.org** and **yemenpress.org**, PUBLIC INTERNET REGISTRY, who is the top-level domain registry for the SUBJECT DOMAIN NAMES, shall take the following actions to effectuate the seizure of SUBJECT DOMAIN NAMES:

1) Take all reasonable measures to redirect the domain names to a substitute server at the direction of the U.S. GOVERNMENT LAW ENFORCEMENT, by updating the authoritative nameservers for the SUBJECT DOMAIN NAMES to any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to the Registry.

2) Prevent any further modification to, or transfer of, SUBJECT DOMAIN NAMES pending transfer of all right, title, and interest in SUBJECT DOMAIN NAMES to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN NAMES cannot be made absent court order or, if forfeited to the United States, without prior consultation with U.S. GOVERNMENT LAW ENFORCEMENT.

3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.

4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

5) The Government will display a notice on the website to which the SUBJECT DOMAIN NAMES will resolve. That notice will consist of law enforcement emblems and the

following, or similar, text:

"The domain for SUBJECT DOMAIN NAME has been seized by the United States Government in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981, 982, and 50 U.S.C. 1701-1705 as part of a law enforcement action by the U.S. Department of Justice."