UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Seizure of
13 DOMAIN NAMES FOR
VIOLATIONS OF 18 U.S.C. § 201

Case No. 26-sz-42

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE BY TELEPHONE

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property located in the jurisdiction of the District of Columbia be seized as being subject to forfeiture to the United States of America. The property is described as follows:

13 DOMAIN NAMES, FUTHER DESCRIBED IN ATTACHMENT A, HEREBY INCORPORATED BY REFERENCE.

I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property.

YOU ARE COMMANDED to execute this warrant and seize the property on or before 06/18/2026
(not to exceed 14 days)

☐ in the daytime – 6:00 a.m. to 10:00 p.m.

☑ at any time in the day or night, as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to United States Magistrate Judge G. Michael Harvey.
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 06/05/2026

Judge's signature

City and state: District of Columbia

G. Michael Harvey, United States Magistrate Judge
Printed name and title

Return		
Case No.: 26-sz-	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of:		
Inventory of the property taken:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-1: PROPERTY TO BE SEIZED

With respect to the domain names centrikglobalconsulting.com, rightinfoconsult.com, finnaclevesperconsulting.com, cydfconsulting.com, pulsewaveglobal.com, catalystglobalsolutions.com, thehorizzen.com, geoindopacific.com, safesec-group.com, thetruthinfo.com, and vandercons.com (**TARGET DOMAIN NAMES**), VeriSign, Inc. ("VeriSign"), which is the domain registry for the **TARGET DOMAIN NAMES**, shall take the following actions to effectuate the seizure of the **TARGET DOMAIN NAMES**:

1. Take all reasonable measures to redirect the **TARGET DOMAIN NAMES** to substitute servers at the direction of the Federal Bureau of Investigation, by associating the **TARGET DOMAIN NAMES** to the following authoritative name-servers:
    a. Ns1.fbi.seized.gov;
    b. Ns2.fbi.seized.gov; and/or
    c. Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including email, to VeriSign.
2. Prevent any further modification to, or transfer of, the **TARGET DOMAIN NAMES** pending transfer of all right, title, and interest in the **TARGET DOMAIN NAMES** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **TARGET DOMAIN NAMES** cannot be made absent court order or, if forfeited to the United States, without prior consultation with Federal Bureau of Investigation.
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.

The government will display a notice on the website to which the **TARGET DOMAIN NAMES** will resolve. That notice will consist of the following text (or substantially similar text):

This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued pursuant to 18 U.S.C. § 981(a)(1)(A), 18 U.S.C. § 982(a)(1), and 21 U.S.C. § 853, issued by the U.S. District Court for the District of Columbia as part of a joint law enforcement operation and action by:

The United States Attorney's Office for the District of Columbia;
National Security Division, Counterintelligence and Export Control Section; and
FBI Washington Field Office and FBI Norfolk Field Office.

If you have information concerning this website, please contact the FBI at 1-800-Call-FBI or online at tips@fbi.gov.

ATTACHMENT A-2: PROPERTY TO BE SEIZED

With respect to the domain names gpf-ina.org and gulfpeace.org (**TARGET DOMAIN NAMES**), Public Interest Registry ("PIR"), which is the domain registry for the **TARGET DOMAIN NAMES**, shall take the following actions to effectuate the seizure of the **TARGET DOMAIN NAMES**:

1. Take all reasonable measures to redirect the **TARGET DOMAIN NAMES** to substitute servers at the direction of the Federal Bureau of Investigation, by associating the **TARGET DOMAIN NAMES** to the following authoritative name-servers:
    a. Ns1.fbi.seized.gov;
    b. Ns2.fbi.seized.gov; and/or
    c. Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including email, to PIR.
2. Prevent any further modification to, or transfer of, the **TARGET DOMAIN NAMES** pending transfer of all right, title, and interest in the **TARGET DOMAIN NAMES** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **TARGET DOMAIN NAMES** cannot be made absent court order or, if forfeited to the United States, without prior consultation with Federal Bureau of Investigation.
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.

The government will display a notice on the website to which the **TARGET DOMAIN NAMES** will resolve. That notice will consist of the following text (or substantially similar text):

This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued pursuant to 18 U.S.C. § 981(a)(1)(A), 18 U.S.C. § 982(a)(1), and 21 U.S.C. § 853, issued by the U.S. District Court for the District of Columbia as part of a joint law enforcement operation and action by:

The United States Attorney's Office for the District of Columbia;
National Security Division, Counterintelligence and Export Control Section; and
FBI Washington Field Office and FBI Norfolk Field Office.

If you have information concerning this website, please contact the FBI at 1-800-Call-FBI or online at tips@fbi.gov.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEIZURE OF 13 DOMAIN NAMES FOR VIOLATIONS OF 18 U.S.C. § 201	**Case No.: 26-sz-42** **FILED UNDER SEAL**

Reference: USAO No. 2024R01683

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, [redacted], a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a seizure warrant for 13 domain names,[1] centrikglobalconsulting.com, rightinfoconsult.com, pulsewaveglobal.com, finnaclevesperconsulting.com, cydfconsulting.com, catalystglobalsolutions.com, thehorizzen.com, geoindopacific.com, gpf-ina.org, safesec-group.com, thetruthinfo.com, vandercons.com and gulfpeace.org (**TARGET DOMAIN NAMES 1-13**, respectively; collectively, the **TARGET DOMAIN NAMES**). The **TARGET DOMAIN NAMES** to be seized are described in the following paragraphs and in Attachment A-1 and A-2.

[1] A domain name is a string of text that maps to an IP address and serves as an easy-to-remember way for humans to identify devices on the Internet (e.g., "justice.gov"). Domain names are composed of one or more parts, or "labels," delimited by periods. When read right-to-left, the labels go from most general to most specific. The right-most label is the "top-level domain" ("TLD") (e.g., ".com" or ".gov"). To the left of the TLD is the "second-level domain" ("SLD"), which is often thought of as the "name" of the domain. The SLD may be preceded by a "third-level domain," or "subdomain," which often provides additional information about various functions of a server or delimits areas under the same domain. For example, in "www.justice.gov," the TLD is ".gov," the SLD is "justice," and the subdomain is "www," which indicates that the domain points to a web server.

2. A search of publicly available WHOIS[2] domain name registration records revealed that **TARGET DOMAIN NAMES 1-13** were registered on or about the listed date through the listed registrar,[3] believed to be headquartered at the listed address:

	Name	Registration Date	Registrar	Address
1	centrikglobalconsulting.com	11/29/2023	GoDaddy.com	100 S. Mill Ave Suite 1600 Tempe, AZ 85281
2	rightinfoconsult.com	8/30/2022	1API	Talstraße 27 66424 Homburg, Germany
3	finnaclevesperconsulting.com	06/21/2025	1API	Talstraße 27 66424 Homburg, Germany
4	cydfconsulting.com	10/12/2024	1API	Talstraße 27 66424 Homburg, Germany
5	pulsewaveglobal.com	05/30/2024	NameSilo	1300 E Missouri Ave Ste A-110 Phoenix, AZ 85014
6	catalystglobalsolutions.com	06/10/2024	NameCheap	4600 East Washington St Suite 300 Phoenix, AZ 85034
7	thehorizzen.com	06/10/2025	Wix.com	100 Gansevoort Street New York, NY 10014
8	geoindopacific.com	07/13/2023	NameCheap	4600 East Washington St Suite 300 Phoenix, AZ 85034
9	gpf-ina.org	08/01/2024	PDR Ltd.	1203 Hedon Road, Kingston Upon

[2] WHOIS is a protocol used for querying databases that store registration and other information about domains, IP addresses, and related Internet resources.

[3] A registrar is a company that has been accredited by the Internet Corporation for Assigned Names and Numbers ("ICANN") or a national country code top-level domain (such as .uk or .ca) to register and sell domain names. Registrars act as intermediaries between registries and registrants. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

				Hull, East Yorkshire, HU9 5LY, UK
10	safesec-group.com	08/02/2024	Wix.com	100 Gansevoort Street New York, NY 10014
11	thetruthinfo.com	08/20/2024	PDR Ltd.	1203 Hedon Road, Kingston Upon Hull, East Yorkshire, HU9 5LY, UK
12	vandercons.com	03/03/2025	Spaceship, Inc.	4600 E Washington St Suite 305 Phoenix, AZ 85034
13	gulfpeace.org	10/20/2025	GoDaddy.com	100 S. Mill Ave Suite 1600 Tempe, AZ 85281

3. The top-level domain for **TARGET DOMAIN NAMES 1-8** and **10-12** is ".com." VeriSign, Inc., a U.S. company, manages all ".com" domains and is the registry[4] for **TARGET DOMAIN NAMES 1-8** and **10-12**.

4. The top-level domain for the **TARGET DOMAIN NAMES 9 and 13** is ".org." Public Interest Registry (PIR), headquartered at 1191 Freedom Drive, Reston, Virginia, manages all ".org" domains and is the registry for the **TARGET DOMAIN NAMES 9 and 13**.

5. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(c), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a seizure warrant.

[4] A domain name registry is an organization that manages top-level domains, including by setting usage rules and working with registrars to sell domain names to the public.

6. I have been an FBI Special Agent since August 2021. I am one of the case agents in this investigation. I am assigned to the Washington, D.C. Field Office. As a Special Agent, I have experience investigating cases involving conspiracy, bribery, wire fraud, identity theft, and money laundering. During my career, I have received training and gained experience in interview and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, and various criminal laws and procedures. I have conducted or participated in surveillances, worked with cooperating witnesses, executed arrest and search warrants, debriefed informants, and reviewed taped conversations. Through my training, education, and experience, I have become familiar with how various federal offenses can be committed. Based on my training and experience, I am familiar with the methods of operation employed by subjects to obfuscate their involvement in transactions for the purpose of circumventing U.S. law.

PURPOSE OF AFFIDAVIT

7. The facts in this affidavit come from my personal observations, my training and experience, information obtained from both government and public records databases, information obtained from other agents, and review of records and documents. When I rely on statements made by others, such statements are set forth only in part and in substance unless otherwise indicated. In addition, many of the statements described herein are based on machine translations or draft English translations of communications that were not originally made in English, and are subject to revision. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. I submit only those facts believed to be relevant to the determination of probable cause, and this affidavit should not be construed as a complete statement of all the facts of this investigation. The dates, times, and amounts discussed herein are approximate.

8. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. §§ 201 (Bribery of public officials and witnesses), 641 (Public money, property or records), 1028 (Fraud and related activity in connection with identification documents, authentication features, and information), and 1956 (Laundering of monetary instruments) (the TARGET OFFENSES) have been committed by known and unknown individuals. There is also probable cause to seize the **TARGET DOMAIN NAMES** described in Attachments A-1 and A-2 as property subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A), 982(a)(1), and 21 U.S.C. § 853.

SUMMARY OF AFFIDAVIT

9. The United States is investigating unlawful activity conducted by actors believed to be working, wittingly and unwittingly, on behalf of the government of the People's Republic of China (PRC). Members of the conspiracy, including SUBJECT A and SUBJECT B, generally believed to be overseas, have used the **TARGET DOMAIN NAMES** to create and operate more than a dozen fake consulting companies to recruit individuals in the United States to obtain sensitive and possibly classified information in exchange for monetary payments. The conspirators have paid for webhosting and domain services provided by U.S. companies through debit and credit cards issued by foreign banks and cryptocurrency. The conspirators have also paid the various recruits at accounts located in the United States through payments originating from accounts located overseas. They have used the TARGET DOMAIN NAMES as part of a larger conspiracy to commit the TARGET OFFENSES.

10. The methods and means used by the conspirators include (1) the use of aliases, fictitious personas, and the stolen identities of actual persons (including Identity Theft Victim 1 and Identity Theft Victim 2); (2) the use of Artificial Intelligence (AI)-generated photographs; (3)

relatively large payments for research reports; (4) the use of Telegram and other encrypted applications; (5) pressure to provide "exclusive" or "insider" information; and (6) the transfer of money from places and accounts located overseas to places and accounts located in the United States.

11. The conspirators have recruited applicants through job postings, posted on LinkedIn and other job search platforms, including Upwork, Expertia AI, Hubstaff Talent, Wellfound, and Post Job Free, that relate to topics of interest to the PRC. The conspirators have targeted U.S. persons, including current and former security clearance holders with access to classified and sensitive U.S. government information, such as Recruits B, D, E, F, G, I, and J (all discussed below). They have recruited these individuals for phony positions such as Senior Analyst and International Affairs Consultant and pressured them to share confidential information and reports from "insider" sources. The conspirators have used contracts and confidentiality agreements to give their fake consulting companies an air of legitimacy. And they have denied any involvement by any foreign government. At the same time, the conspirators have encouraged applicants and recruits to share confidential and sensitive information in violation of their official duties and of particular interest to the People's Republic of China (PRC) government.

12. The conspirators have offered money to applicants and recruits in exchange for this information. They have paid for reports using PayPal accounts in the names of fictitious individuals and cryptocurrency to conceal the conspirators' identities and the true source of the payments. These payments have allowed for the flow of money from places outside the United States to places inside the United States in furtherance of the conspiracy.

RELEVANT LAWS

13. Section 201(b) of Title 18 provides, in pertinent part:

Whoever—

(1) directly or indirectly, corruptly gives, offers or promises anything of value to any public official or person who has been selected to be a public official, or offers or promises any public official or any person who has been selected to be a public official to give anything of value to any other person or entity, with intent—

(A) to influence any official act; or

(B) to influence such public official or person who has been selected to be a public official to commit or aid in committing, or collude in, or allow, any fraud, or make opportunity for the commission of any fraud, on the United States; or

(C) to induce such public official or such person who has been selected to be a public official to do or omit to do any act in violation of the lawful duty of such official or person;

(2) being a public official or person selected to be a public official, directly or indirectly, corruptly demands, seeks, receives, accepts, or agrees to receive or accept anything of value personally or for any other person or entity, in return for:

(A) being influenced in the performance of any official act;

(B) being influenced to commit or aid in committing, or to collude in, or allow, any fraud, or make opportunity for the commission of any fraud, on the United States; or

(C) being induced to do or omit to do any act in violation of the official duty of such official or person …

shall be fined under this title or not more than three times the monetary equivalent of the thing of value, whichever is greater, or imprisoned for not more than fifteen years, or both.

14. Section 201(a)(1) of Title 18 provides, in pertinent part:

The term "public official means… an officer or employee or person acting for or on behalf of the United States, or any department, agency or branch of Government thereof."

15. Section 641 of Title 18 provides, in pertinent part:

> Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or
>
> Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted—
>
> Shall be fined under this title or imprisoned ... or both.

16. Section 1028(a) of Title 18 provides, in pertinent part:

> Whoever, in a circumstance described in subsection (c) of this section—.
>
> . . .
>
> (7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law ... shall be punished as provided in subsection (b) of this section.

17. Section 1028(c)(3)(A) of Title 18 permits a prosecution where "the production, transfer, possession, or use prohibited by this section is in or affects interstate or foreign commerce, including the transfer of a document by electronic means."

18. Regarding money laundering, sections 1956(a)(2) and (c)(7)(B)(v)(II) provide, in pertinent part:

> (a)(2) Whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States—
>
> (A) with the intent to promote the carrying on of specified unlawful activity . . .
>
> shall be sentenced to a fine of not more than $500,000 or twice the value of the monetary instrument or funds involved in the transportation, transmission, or transfer, whichever is greater, or imprisonment for not more than twenty years, or both.
>
> (c) As used in this section—

(7) the term "specified unlawful activity" means--

. . .

(A) any act or activity constituting an offense listed in section 1961(1) of this title except an act which is indictable under subchapter II of chapter 53 of title 31; [and]

. . .

(D) an offense under . . . section 641 (relating to public money, property, or records).

19. Section 1961(1) of Title 18 includes the following crimes, among others: Bribery of public officials and witnesses, in violation of 18 U.S.C. § 201; Fraud and related activity in connection with identification documents, authentication features, and information, in violation of 18 U.S.C. § 1028; and Laundering of monetary instruments, in violation of 18 U.S.C. § 1956.

JURISDICTION AND VENUE

20. This Court has jurisdiction to issue the requested warrant. Section 853(f) of Title 21 of the U.S. Code authorizes the government to obtain a seizure warrant from the court in the same manner as a search warrant under Federal Rule of Criminal Procedure 41. Further, Section 853(l) provides that a federal court has "jurisdiction to enter orders as provided in this section *without regard to the location of any property which may be subject to forfeiture*" (emphasis added). Section 853(f) provides that 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. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the **TARGET DOMAIN NAMES** for forfeiture. By seizing the **TARGET DOMAIN NAMES** and redirecting traffic, the government will prevent third parties from controlling or acquiring

TARGET DOMAIN NAMES and using it to commit additional violations of the TARGET OFFENSES.

21. This affidavit also is being submitted in support of a civil seizure warrant for the property pursuant to 18 U.S.C. § 981(b)(2). Such a warrant requires a finding of probable cause and may be obtained on an *ex parte* basis. Section 981(b) applies to all property subject to civil forfeiture under § 981(a). Under § 981(a)(1)(A), property subject to forfeiture to the United States includes "[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of [18 U.S.C. §1956]." Section 1956(a)(2)(A) of Title 18 criminalizes "transport[ing], transmit[ing], or transfer[ing], or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States with the intent to promote the carrying on of specified unlawful activity." Violations of 18 U.S.C. §§ 201, 641, 1028, and 1956 qualify as specified unlawful activity under the statute. Section 1956(h) of Title 18 criminalizes the conspiracy to commit money laundering, as defined in Section 1956(a). As discussed below, there is probable cause to believe that violations of 18 U.S.C. §§ 201, 641, 1028, and 1956(a)(2)(A), (h) have been committed by members of the conspiracy.

22. Further, the criminal offenses under investigation began or were committed upon the high seas, or elsewhere out of the jurisdiction of any particular State or district, and no offender is known to have, or have had, residence within any United States district. *See* 18 U.S.C. § 3238.

PROBABLE CAUSE

23. As explained below, there is probable cause to believe that known and unknown conspirators have used Centrik Global Consulting, centrikglobalconsulting.com (CENTRIK) (**TARGET DOMAIN NAME 1**); Rightinfo Consulting, rightinfoconsult.com (RIGHTINFO)

(**TARGET DOMAIN NAME 2**); Finnacle-Vesper Consulting (FV), finnaclevesperconsulting.com (**TARGET DOMAIN NAME 3**); CYDF Consulting, cydfconsulting.com (CYDF) (**TARGET DOMAIN NAME 4**); Pulse Wave Global, pulsewaveglobal.com (PWG) (**TARGET DOMAIN NAME 5**); Catalyst Global Solutions, catalystglobalsolutions.com (CGS) (**TARGET DOMAIN NAME 6**); Horizzen, thehorizzen.com (HORIZZEN) (**TARGET DOMAIN NAME 7**); GeoIndopacific, geoindopacific.com (GEOINDOPACIFIC) (**TARGET DOMAIN NAME 8**); Global Peace Foundation – Indonesia, gpf-ina.org (GPFI) (**TARGET DOMAIN NAME 9**); SafeSec Group, safesec-group.com (SAFESEC) (**TARGET DOMAIN 10**); The TruthInfo, thetruthinfo.com (TRUTHINFO) (**TARGET DOMAIN NAME 11**); Vandercons.com (**TARGET DOMAIN NAME 12**); and Gulf Peace Foundation, gulfpeace.org (GULF PEACE) (**TARGET DOMAIN NAME 13**), in their conspiracy to commit bribery of current and former public officials, identity theft, and international money laundering.

24. The probable cause section of this affidavit is organized as follows: (a) background on the People's Republic of China Intelligence Services (PRCIS); (b) the PRCIS's use of LinkedIn to spot, assess, and recruit U.S. persons; (c) background on LinkedIn in China; (d) the conspirators' use of phony "consulting" websites; (e) the conspirators' use of stolen identities belonging to actual U.S. Persons; (f) evidence of Chinese state sponsored activity and the use of fictitious personas; (g) SUBJECT A's targeting of current and former U.S. government officials through CENTRIK From August to November 2024; and (h) evidence that the **TARGET DOMAIN NAMES** conduct targeting on behalf of the PRC.[5]

[5] On October 8, 2024, U.S. Magistrate Judge Lawrence R. Leonard issued search warrants in 24-sw-176 targeting accounts associated with **TARGET DOMAIN NAME 2**. On November 22, 2024, U.S. Magistrate Judge G. Michael Harvey issued search warrants in 24-sc-2334 targeting multiple accounts related to this investigation, including eight accounts associated with **TARGET**

A. People's Republic of China Intelligence Services

25. The PRCIS encompass both civilian and military components of Chinese intelligence programs. Among other things, the PRCIS and their various components are focused on identifying and influencing the foreign policy of other countries, including the United States, and obtaining sensitive and confidential information from those countries. The PRCIS seek to obtain information on foreign intelligence operations directed at the People's Republic of China ("PRC" or "China"), corporate and industrial information that could benefit China, biographical profiles of foreign politicians and intelligence officers, and the political, economic, and security policies of other countries that might affect China.

26. Additionally, the PRCIS and their various components are tasked with conducting clandestine and overt human source operations, of which the United States is a principal target. Human sources or assets are people who agree to help a foreign intelligence service by providing information to that service in response to taskings from foreign intelligence officers or agents. PRCIS human source operations use PRCIS trained intelligence officers, as well as non-professional collectors called "cut-outs" or "co-optees," to recruit, operate, and obtain information from human sources. A cut-out or co-optee is a person trusted by both an intelligence officer and the officer's human source, who helps to provide a layer of insulation between the intelligence officer and the source to increase operational security. Cut-outs or co-optees can operate under a variety of covers, posing as diplomats, journalists, academics, or businesspeople both at home and abroad. These individuals are tasked with spotting, assessing, targeting, collecting, and handling

---

DOMAIN NAME 1. On December 13, 2024, U.S. Magistrate Judge Lawrence R. Leonard issued search warrants in 24-sw-219 targeting accounts associated with **TARGET DOMAIN NAME 2**. On June 20, 2025, U.S. Magistrate Judge Moxila A. Upadhyaya issued search warrants in 25-sc-1002 targeting additional accounts related to this investigation, including all accounts using **TARGET DOMAIN NAME 1**. Relevant evidence collected from these search warrants is discussed below.

sources or assets with access to classified, open-source, proprietary, or sensitive information that the PRC government can use for economic, political, or military decision-making or advantage. Sources or assets are people who agree to help a foreign intelligence service by providing information to that service in response to taskings from foreign intelligence officers or agents.

27. PRCIS source operations tend to originate inside China, where the PRCIS prefers to meet with its sources or assets. To facilitate continued meetings inside China, the PRCIS will arrange and/or pay for travel and expenses. The PRCIS are known to pay their sources not only in cash, but also through other means, including business considerations or other types of assistance within China.

28. Based on my training and experience, I am aware that PRCIS officers and agents employ various forms of intelligence tradecraft to protect themselves and their operations. Intelligence tradecraft includes the use of aliases, codenames and false identities, the use of encrypted forms of communication, and meetings with sources and assets in private locations. PRCIS officers and agents often use aliases or false identities when initially communicating with potential intelligence assets.

B. The PRCIS's Use of LinkedIn to Spot, Assess, and Recruit U.S. Persons

29. Based on my training and experience, I also know that the PRCIS use job networking websites like LinkedIn to target and recruit intelligence assets in the United States. According to open-source news articles, for many years the PRCIS used LinkedIn and other social media platforms to solicit and try to recruit U.S. persons with access or knowledge of U.S. government or commercial secrets, including current and former U.S. government officials.

30. The prosecution of Jun Wei Yeo, also known as Dickson Yeo ("Yeo"), illustrates this tradecraft. According to a June 18, 2020 information filed in the U.S. District Court for the

District of Columbia,[6] Yeo acted in the United States as an agent of the PRC government without providing prior notice to the Attorney General, in violation of 18 U.S.C. § 951. On July 15, 2020, Yeo signed a statement of facts to establish that he was guilty of the charged offense.[7]

31. According to the statement of facts, around 2015, while Yeo was a doctoral student in Singapore, he was recruited by PRCIS operatives. These PRCIS individuals claimed to represent PRC-based think tanks, but in reality, at least four of these individuals were intelligence operatives for the PRC government. Yeo was tasked by his PRCIS handlers with obtaining and providing non-public information from the United States about international political, economic, and diplomatic relations.

32. Using the internet and various social media sites, Yeo worked to spot and assess U.S. persons with access to valuable non-public information, including U.S. military and government employees with security clearances. Yeo recruited these individuals and paid them to write reports. Yeo told the individuals that the reports were intended for clients in Asia, without revealing that the reports were being sent to the PRC government.

33. Yeo also met with PRC operatives in various locations across China. Although the PRCIS operatives used pseudonyms in their interactions with Yeo, they were open about their affiliation with the PRC government. During one meeting, Yeo was instructed by his PRCIS handlers to obtain non-public information about the U.S. Department of Commerce, artificial intelligence, and the trade war between China and the United States.

---

[6] *United States v. Yeo*, Case No. 20-CR-00087 (D.D.C.).

[7] The statement of facts is publicly available at the following website: justice.gov/usao-dc/press-release/file/1297451/dl, and additional information can be found at: https://www.justice.gov/opa/pr/Singaporean-national-pleads-guilty-acting-united-states-illegal-agent-chinese-intelligence.

34. To accomplish his taskings, Yeo used [redacted] to identify individuals with resumes and job descriptions that suggested they were likely to have access to valuable nonpublic information.[8] More specifically, Yeo used [redacted] social networking algorithm to identify targets. For each contact with a potential recruit, [redacted] would then suggest additional contacts with similar experience. Yeo used these suggestions to identify, and communciate with, additional potential recruits.

35. After contacting these individuals [redacted], Yeo attempted to recruit them to write reports and provide information using recruitment strategies he had learned from his PRCIS handlers. Yeo would ask recruits to write reports for a fake consulting company that Yeo had created.

C. LinkedIn in China

36. According to open source information, LinkedIn first entered China in February 2014 with a localized version of its main application, which allowed access to LinkedIn's global social media platform. LinkedIn offered direct access to western markets, making it possible for PRCIS to use LinkedIn as a recruitment and communications platform.

37. In October 2021, LinkedIn announced that it would sunset the localized version of its application, instead launching a standalone jobs application for China that would not include social media features. Then, in May 2023, LinkedIn announced that it would be phasing this out on August 9, 2023, essentially ending significant LinkedIn access for China-based users.[9]

---

[8] The public statement of facts [redacted]

[9] Additional information can be found at LinkedIn's website: https://www.linkedin.com/pulse/linkedin-china-timeline-teamedupchina (last accessed on April 6, 2026).

D. The Conspirators' Use of Phony "Consulting" Websites (TARGET DOMAIN NAMES 1-13)

38. Starting in or around November 2023, the conspirators have created at least 13 fake "consulting" company websites using fraudulent or stolen identities, AI-generated photos, and stock language. The websites and their associated job postings advertise generic "consulting" jobs and include implicit and explicit statements indicating their purpose is to recruit current or former U.S. government and U.S. military employees to provide expertise to unspecified clients. These websites are often linked or referenced within the entities' job postings on LinkedIn and other hiring platforms. These websites are discussed in the following paragraphs. Table 1 shows the respective indicators of illicit activity for each website with the websites identified by their **TARGET DOMAIN NAME** number.

Table 1: Links Among TARGET DOMAIN NAMES

	1	2	3	4	5	6	7	8	9	10	11	12	13
Registered using Identity Theft Victim 1's name	X	X											
Shared a domain hosting IP address		X	X	X									
Posted vague consulting job(s)	X	X	X	X	X	X	X	X	X	X	X	X	X
Job post(s) contained identical text or substantially similar idiosyncratic text to another entity in the list	X	X	X	X		X	X		X		X		
Website with stock or AI-generated photos	X	X	X	X	X		X	X	X	X	X	X	X
Purported location of entity does not match job post(s) or records	X				X	X		X		X		X	
Associated with [redacted]" persona	X	X				X			X			X	X
Associated with SUBJECT B					X			X					
Exchanged Emails with a CENTRIK persona					X								

Subject of a suspicious activity report to the FBI	X	X								X			
Website appears to have been built by Chinese language user											X		
Job post(s) showed template language that was not deleted						X							
Impersonated real entity who flagged job post(s) as a scam									X				

1. TARGET DOMAIN NAME 1 (centrikglobalconsulting.com)

39. One of the target websites (www.centrikglobalconsulting.com, **TARGET DOMAIN NAME 1**, last visited in or around June 2025)[10] is that of Centrik Global Consulting (CENTRIK). **TARGET DOMAIN NAME 1** has described CENTRIK as a consulting firm and a "leading provider of innovative and impactful solutions to businesses across various industries." **TARGET DOMAIN NAME 1** claim that CENTRIK has a physical address of 128 City Road, London, United Kingdom. Open-source searches of the address 128 City Road, London, United Kingdom, indicate that it may be a building with multiple commercial tenants. One company that listed this address was Your Company Formations LTD.

40. According to its website, Your Company Formations LTD is a company formation agent that helps clients set up limited companies in the United Kingdom (UK) [URL: https://www.yourcompanyformations.co.uk]. The website states that its clients do not need to live in the UK to register a UK company and only need a registered UK office address for the company. The website also states that if clients wish to keep their details private, they can pay to use the Your Company Formations LTD company address and the Your Company Formations LTD director's privacy address in company incorporation filings.

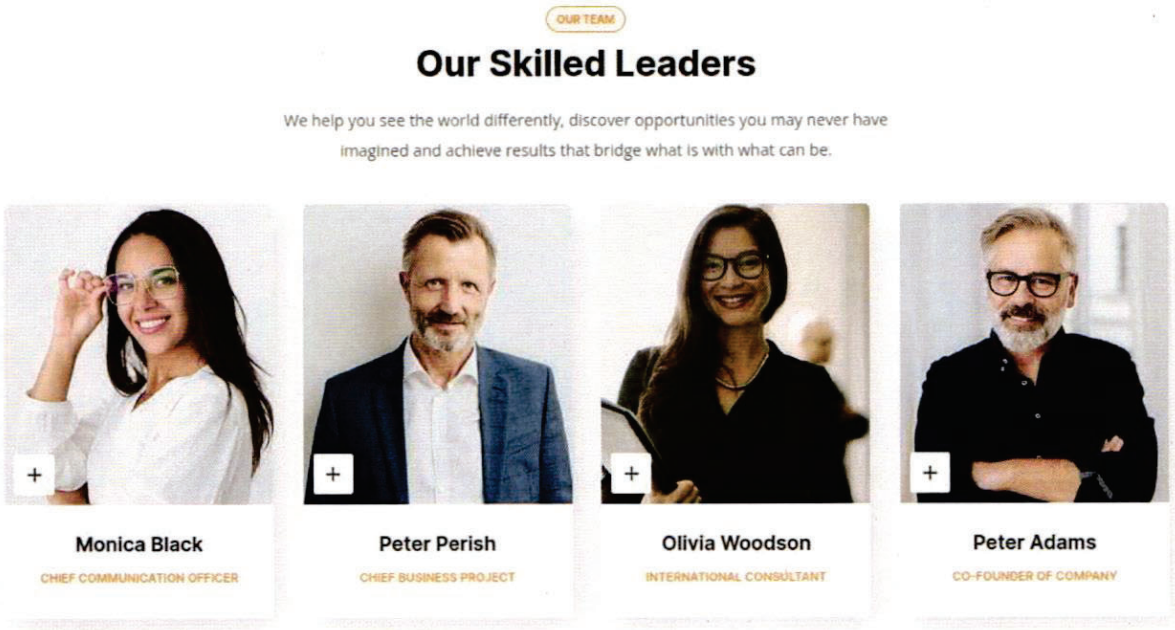
[10] As of April 17, 2026, this website is inactive. Nevertheless, seizure of **TARGET DOMAIN NAME 1** is appropriate to prevent the subjects from using it in the future.

41. According to records obtained from New Fold Digital, Inc., **TARGET DOMAIN NAME 1** was registered on or about November 29, 2023, by someone using Identity Theft Victim 1's name; Identity Theft Victim 1's address in [redacted], Florida;[11] and email address [redacted]@gmail.com, through a reseller, Hosteons Pte. Ltd. According to Google records, a user of [redacted]@gmail.com logged into the account on January 17, 2024, from the IP Address 113.52.104.7. Open-source search of this IP address shows it resolves to Macau. Account [redacted]@gmail.com also was logged into on the following dates from IP addresses resolving to Macau: January 16, 2024; December 5, 2023; and November 24, 2023.

42. According to records obtained from Hosteons Pte. Ltd., someone using Identity Theft Victim 1's name and address purchased web hosting services for CENTRIK from Hosteons Pte. Ltd. on or about November 29, 2023, from IP Address 43.198.215.165. An open-source search of this IP Address resolves to Hong Kong. According to Hosteons Pte. Ltd., in or around October 2025, CENTRIK's Hosteons account (with **TARGET DOMAIN NAME 1**) was last logged into on or about June 24, 2025, from IP address 118.248.211.114. An open-source search of this IP Address came back to the Internet Service Provider Chinanet Hunan Province Network, location Changsha, China. According to Hosteons Pte.Ltd., as of in or around June 2025, CENTRIK's Hosteons account appears to have been logged into by IP Addresses that resolve to cloud service providers, indicating possible virtual private network (VPN) usage.

[11] As discussed below, the FBI's investigation has revealed that Identity Theft Victim 1 is an actual U.S. person who was not involved in any of the **TARGET DOMAIN NAMES** or illicit activity.

43. The About Us section of **TARGET DOMAIN NAME 1**[12] included images of a diverse leadership team. Specifically:



44. A reverse image search of the above photograph posted on **TARGET DOMAIN NAME 1** for the company's Chief Communications Officer, "[redacted]," returned an exact match from the website of a Nigeria-based human resources company called MacTay that advertises background check services.[13] The portion of the MacTay website advertising the background check services appeared to use a template similar to **TARGET DOMAIN NAME 1** and displayed the same photos, names, and titles for its leadership team as those displayed on **TARGET DOMAIN NAME 1**. While MacTay appears to be a legitimate company, due to the exact matches of the photos and names and the similarity of the layout of the two websites, investigators have concluded that either **TARGET DOMAIN NAME 1** copied content from the

[12] https://centrikglobalconsulting.com/about-us.html/ (last accessed on April 17, 2026; no longer active).

[13] https://www.mactay.com/backgroundchecks/our-team/ (last accessed on April 6, 2026).

MacTay website or both websites were built from website templates that included stock photos and names of personnel.

45. According to LinkedIn records and open-source research, someone using Identity Theft Victim 2's name created a LinkedIn account on or about December 4, 2023, from an IP address that resolved to Shanghai, China.[14] CENTRIK's use of Identity Theft Victim 2's identity and various fictitious personas to recruit former members of the U.S. military and U.S. intelligence community with security clearances to provide non-public information is elaborated in sections G. and H. below.

2. TARGET DOMAIN NAME 2 (rightinfoconsult.com)

46. According to legal returns from Monster Megs, a web hosting services company, Identity Theft Victim 1 is included on the domain registration information for another website, https://rightinfoconsult.com (**TARGET DOMAIN NAME 2**, last visited on April 6, 2026), which was registered on or about August 30, 2022, with some of the same information used to register **TARGET DOMAIN NAME 1**, including Identity Theft Victim 1's name and the address in [redacted], Florida. As elaborated below, the FBI interviewed Identity Theft Victim 1, who stated she/he has never registered an internet domain and had never heard of MonsterMegs, Hosteons, RightInfo Consulting, or Centrik Global Consulting.

47. A review of **TARGET DOMAIN NAME 2** in April 2026 indicated the website contained generic descriptions of consulting services offered by RIGHTINFO. **TARGET DOMAIN NAME 2** contained a section titled "Clients Words," which contained reviews of the consulting firm from individuals named Ron Burgundy, Brick Tamland, and Brian Fontana—all

[14] It is unclear how this account was opened from an IP address resolving to China given that LinkedIn officially ceased operating in China in August 2023 (*see* paras. 36-37).

names of characters from the movie "Anchorman: The Legend of Ron Burgundy."

48. As of in or around October 2023, **TARGET DOMAIN NAME 2** also included biographies of company personnel with their photographs.[15] A reverse image search of the photograph included for the company's CEO, "[redacted]" (assessed to be a fictitious persona), revealed significant similarities to the photograph of an executive at an identified U.S. accounting firm. Reverse image searches of photographs for the remaining employees listed on **TARGET DOMAIN NAME 2** revealed three exact matches for stock images.

49. In or around September and October 2023 and as recent as April 2026, the FBI identified multiple job postings by RIGHTINFO on various job search platforms for analyst and consultant jobs which indicated ideal candidates would have government or military experience. As of April 2026, **TARGET DOMAIN 2** also contained a job advertisement for "International Affairs Analysts (Remote)" which stated "[e]xperience in Government/Military or NATO institutions" and "[d]eep understanding of geopolitical, security and military policies" were preferred and noted the responsibilities would include "[m]onitoring developments related to Russian-Ukranian conflict, Israeli-Palestinian conflict and other international hotspot issues."

50. As detailed below, the FBI conducted open-source searches and found the text from CENTRIK and RIGHTINFO job postings was reproduced by other suspected fake companies on various job search platforms, specifically on job postings posted by **TARGET DOMAIN NAMES 4, 9,** and **11**.

3. & 4. TARGET DOMAIN NAMES 3 and 4 (finnaclevesperconsulting.com and cydfconsulting.com)

51. The FBI has identified two additional consulting websites, among other unrelated

[15] As of at least April 2026, these biographies are no longer on **TARGET DOMAIN NAME 2**.

websites, hosted on the same IP address as **TARGET DOMAIN NAME 2**. This IP address resolves to an Internet Service Provider that operates a Content Delivery Network (CDN). A CDN is a geographically distributed group of servers that caches content, significantly reducing latency and speeding up website performance. Based on my training and experience, actors who set up domains often use the same server infrastructure or CDN infrastructure because they have existing accounts with these providers, making the set up easier. The two websites identified as using the same IP address were Finnacle Vesper Consulting, using www.finnaclevesperconsulting.com (**TARGET DOMAIN NAME 3**, last visited on April 6, 2026), and CYDF Consulting, using www.cydfconsulting.com (**TARGET DOMAIN NAME 4**, last visited on April 6, 2026). A review of both websites revealed almost identical designs. Open-source searches for excerpts from **TARGET DOMAIN NAME 3** identified only two results, which were for **TARGET DOMAIN NAME 3** and **TARGET DOMAIN NAME 4**. Notably, the thumbnail logo for both **TARGET DOMAIN NAME 3** and **TARGET DOMAIN NAME 4** in the search results appeared to be identical.

52. Both **TARGET DOMAIN NAME 3** and **TARGET DOMAIN NAME 4** have posted similar generic "consulting" jobs. One of the **TARGET DOMAIN NAME 4** job postings had portions that were identical to a September 2024 LinkedIn job posting by **TARGET DOMAIN NAME 2**. Reverse image searches of the photos for the four employees listed on **TARGET DOMAIN NAME 4** returned results suggesting they were stock photos.

53. Open-source searches revealed a business registration for **TARGET DOMAIN NAME 3** in Canada that shows it was incorporated in 2017 and updated in April 2025 with an address that appears to be a co-working space, a business that provides a shared workspace environment to individuals and companies on a paid basis. Based on the similarities in content and

the generic appearance of these two websites, I believe **TARGET DOMAIN NAME 3** was registered in Canada to look legitimate and hide its true location, similar to how **TARGET DOMAIN NAME 1** was registered in the UK for the same reason.

5. TARGET DOMAIN NAME 5 (pulsewaveglobal.com)

54. In approximately December 2024, the FBI identified a company on LinkedIn called Pulse Wave Global (PWG) that had a LinkedIn job posting for a "Defense and Geopolitical Analyst." The job posting requested individuals provide "special reports about assigned topics as required by our clients" and stated that candidates must have knowledge of global military trends, security policies, and proficiency in open-source intelligence. This PWG job posting hyperlinked to a PWG company LinkedIn profile, which linked to the PWG website, https://pulsewaveglobal.com (**TARGET DOMAIN NAME 5**, last visited on April 6, 2026). According to its LinkedIn page,[16] PWG describes itself as "providing strategic insights on global defense and geopolitical developments," claims to be "committed to providing professional consulting service[s] to client enterprise," and further claims to "work with governments, organizations, and defense institutions."

55. According to LinkedIn records, PWG's LinkedIn page was created on or about November 28, 2024, by SUBJECT B, who is believed to be a real person from a country in the Caribbean that is living or lived in China, based on a review of government records. In approximately November 2024, SUBJECT B posted the PWG defense and geopolitical analyst job referenced above. Billing information showed SUBJECT B paid for the job posting charges to LinkedIn based in the United States with a credit card issued by a French bank.

56. SUBJECT B registered a personal LinkedIn account on or about July 25, 2021, with

[16] https://www.linkedin.com/company/pulse-wave-global/ (last accessed on April 7, 2026).

IP address 45.135.186.25, which resolves to Hong Kong. On or about December 18, 2024, SUBJECT B added the email address career@geoindopacific.com (related to **TARGET DOMAIN NAME 8**, as detailed below) to his/her LinkedIn account. This is similar to how SUBJECT A, described later in this affidavit, registered PRC front company CENTRIK's LinkedIn page on or about August 15, 2024, and shortly after, on or about August 29, 2024, added a CENTRIK email account, [redacted]@centrikglobalconsulting.com [**TARGET DOMAIN NAME 1**], to SUBJECT A's LinkedIn account. "[redacted]" is a fictitious persona that has been used by CENTRIK, as detailed below.

57. From approximately November 30, 2024, through January 15, 2025, SUBJECT B made multiple credit card purchases for LinkedIn Jobs, all paid to LinkedIn based in the United States with a credit card issued by a French bank. According to NameSilo records, **TARGET DOMAIN NAME 5** registered its domain, through a domain reseller, to a user of a ProtonMail email account with phone number 212-355-XXXX and an address on [redacted] New York, NY 10022. According to open-source research, there is a legitimate dental office located at this location. Of note, as discussed below, **TARGET DOMAIN NAME 8** was registered by the same user with the same ProtonMail email account, address, and phone number.

58. According to **TARGET DOMAIN NAME 5**, as of April 3, 2025, email address [redacted]@gmail.com is listed under the Contact Us section of **TARGET DOMAIN NAME 5**. According to transaction records provided by Google, on or about December 13, 2024, an email address associated with CENTRIK ([Identity Theft Victim 2]@gmail.com, discussed in more detail below) exchanged an email with [redacted]@gmail.com. According to Google records, [redacted]@gmail.com is registered to "[redacted]" and associated with an Android device for which the locale of the device is en-US (referring to English-United States) with time zone set to

Asia/Shanghai. The Android device has a current cell operator MCC+MNC: 46000 and a current SIM operator (MCC+MNC): 45407. According to MCC-MNC research, the Android's SIM operator resolves to Hong Kong, specifically China Unicom (Hong Kong) Limited and the Android's cell operator resolves to China, specifically China Mobile.

59. Like CENTRIK, PWG describes itself as a consulting company on LinkedIn. Similar to CENTRIK, the account that registered **TARGET DOMAIN NAME 5** appears to be different than the account that is the administrator of their LinkedIn company page. While CENTRIK listed the address of a UK based incorporation company, PWG listed the address of an apparently legitimate New York dental office.

6. TARGET DOMAIN NAME 6 (catalystglobalsolutions.com)

60. The FBI conducted open-source searches and found the text from CENTRIK job postings was reproduced by other purported consulting companies on various job search platforms. The identical text contained portions with the same grammatical errors. One of these was Catalyst Global Solutions (CGS). One of the CGS jobs posted to LinkedIn was linked to a company profile on LinkedIn of the same name. This CGS company profile included a website, www.catalystglobalsolutions.com (**TARGET DOMAIN NAME 6**, last visited on July 16, 2024).[17] **TARGET DOMAIN NAME 6** was registered on June 10, 2024, less than two weeks after **TARGET DOMAIN NAME 5** was registered.

61. In approximately July 2024, the FBI reviewed **TARGET DOMAIN NAME 6** and found that its homepage contained information about CGS being "among DC's top firms," its advocacy work, and its access on "Capitol Hill." At the same time, it listed an office location in "Jaranwala road Faisalabad [Pakistan]" but did not indicate any physical presence in Washington,

[17] As of April 17, 2026, this website is inactive. Nevertheless, seizure of **TARGET DOMAIN NAME 6** is appropriate to prevent the subjects from using it in the future.

DC. The contact us page of **TARGET DOMAIN NAME 6** included an office address in Lahore, Pakistan. A review of the domain registration information showed that **TARGET DOMAIN NAME 6** was registered to a user who provided an address in Pakistan. A review of the jobs posted by CGS on LinkedIn and on an Australian job search platform indicated they were for job roles such as "International Relations and Geopolitics Analyst" and "International Affairs Consultant." One of the job postings, seen in July 2024 on LinkedIn, included bracketed text that appeared to have been left in a template to be filled in later. A portion of this job posting is produced below:

> **How to Apply:** Please submit your resume, cover letter, and a sample of your previous work related to international relations or geopolitical analysis via [Indeed/Upwork] by [application deadline]. Include specific examples of successful analysis and relevant outcomes.
>
> **Contact Information:** For questions or more information, please contact [Your Contact Name] at [Your Contact Email] or [Your Contact Phone Number].
>
> [Your Company Name] is an equal opportunity employer and values diversity at our company. We do not discriminate on the basis of race, religion, color, sex, gender identity, sexual orientation, age, non-disqualifying physical or mental disability, national origin veteran status, or any other basis covered by appropriate law. All employment is decided on the basis of qualifications, merit, and business need.

62. Additionally, the FBI found language taken verbatim from a **TARGET DOMAIN NAME 6** job posting on LinkedIn that also was used on a **TARGET DOMAIN NAME 7** job posting, discussed in further detail below. The FBI also found that idiosyncratic language used in a **TARGET DOMAIN NAME 6** job posting was used in a **TARGET DOMAIN NAME 9** job posting, discussed in further detail below.

7. TARGET DOMAIN NAME 7 (thehorizzen.com)

63. In approximately July 2025, the FBI identified a company called Horizzen (HORIZZEN), with website www.thehorizzen.com (**TARGET DOMAIN NAME 7**, last visited on April 6, 2026), which indicated the company was based in Australia. HORIZZEN posted

several jobs to job recruitment platforms and included **TARGET DOMAIN NAME 7** in one of the postings.

64. One of its job postings included a "Next Steps" section, which had language that was taken verbatim from one of the CGS (**TARGET DOMAIN NAME 6**) job postings on LinkedIn and even included a reference to "CGS:"

> Qualified candidates will be invited to participate in a paid assessment test to better understand their expertise and alignment with our needs. Successful candidates will establish a formal relationship with CGS, with opportunities for ongoing projects and professional growth.

65. **TARGET DOMAIN NAME 7** included other indicators that it was phony, such as generic language, grammatical errors, and a section containing website template language, indicating that **TARGET DOMAIN NAME 7** was incomplete and hastily created. The company advertised jobs for "Defense and security policy specialist" and "Cross-border investment risk advisor" on **TARGET DOMAIN NAME 7**.

8. TARGET DOMAIN NAME 8 (geoindopacific.com)

66. As noted above, on or about December 18, 2024, SUBJECT B, who posted job advertisements for PWG (**TARGET DOMAIN NAME 5**), also added an email address with career@geoindopacific.com to his/her LinkedIn profile. In approximately May 2025, the FBI identified an entity using the name "GeoindoPacific" (GEOINDOPACIFIC) that made a LinkedIn job posting for a "Defense and Geopolitical Analyst – GeoindoPacific" that was visible in Google search results. The job was no longer visible on LinkedIn. This excerpt was visible in the Google search results: "Provide analytical articles about recent hot security and geopolitical issues which would have profound influence on as required by our routine…"

67. Open source searches identified a website for GEOINDOPACIFIC, https://www.geoindopacific.com (**TARGET DOMAIN NAME 8,** last visited on April 6, 2026).

As of April 2026, **TARGET DOMAIN NAME 8** included a graphic stating that the company was hiring "professionals" to "join now and earn money online." The job posting included the following position types, presumably as targets for the advertisement: "Writers, Defense Analyst, Geo Political Analyst, Jobs for Ex - Military Personnel, Job for Ex-Diplomats." **TARGET DOMAIN NAME 8** also contained numerous news articles, many of which were focused on U.S. or China-related geopolitical topics, and which appeared to be copied from other news outlets, such as Nikkei Asia. A picture of the homepage as of April 6, 2026, is below:

68. Additional open-source searches identified various profiles for GEOINDOPACIFIC on social media platforms that posted jobs, including through videos with narration that sounded computer generated. One of these videos, which appeared to be computer-generated, was of a woman standing in a news studio encouraging prospective job applicants to apply to jobs at career@geoindopacific.com.

69. According to domain registration information for **TARGET DOMAIN NAME 8**, the domain was registered under the name "NYC Dental Hospital." The domain registration lists

the same physical address and phone number that were listed in the registration information for **TARGET DOMAIN NAME 5** (discussed above), which appear to be associated to a legitimate dental office, along with the same email address used in **TARGET DOMAIN NAME 5**'s registration that appears unrelated to the legitimate dental office.

9. TARGET DOMAIN NAME 9 (gpf-ina.org)

70. In approximately September 2024, the FBI identified an entity purporting to be located in Indonesia called Global Peace Foundation Indonesia (GPFI) with the website, https://gpf-ina.org (**TARGET DOMAIN NAME 9**, last visited on April 6, 2026), registered on August 1, 2024. This entity made several job postings to hiring platforms with the following titles: "International Affairs and Economic Consultant," "Freelance Writer," and "Political Analyst." Some of the job postings included either **TARGET DOMAIN NAME 9** or an email address @**TARGET DOMAIN NAME 9**.

71. One of the job postings contained substantial sections of text that were identical to job postings by CENTRIK and CGS (**TARGET DOMAIN NAME 1** and **TARGET DOMAIN NAME 6**, respectively). Specifically, a job post for GPFI made to Hubstaff Talent in or around September 2024 used the following in a list of responsibilities: "Keep track of international hot issues, and have unique opinions and convincing evidence." Additionally, the job post noted "We look forward to shaping the future of success together!" This same text was found verbatim in a CENTRIK job post on Jobsoid that the FBI viewed in or around July 2024. It was also found in a CGS job post on an Australian job recruitment platform that was viewed by the FBI in or around July 2024.

72. A review of **TARGET DOMAIN NAME 9** in or around September 2024 indicated it appeared to use stock photos and content copied from other entities' websites. Some of its links

redirected back to existing pages on the website and did not appear to be functioning. Furthermore, **TARGET DOMAIN NAME 9's** "User Registration" page contained Chinese characters that translate to "User Registration." The domain registrant contact information listed a location of Shanghai, CN [China]. Of note, the FBI identified another entity called the [redacted] that is a well-documented U.S.-based non-profit entity. Some of the GPFI job postings linked back to the legitimate [redacted] website.

73. In approximately September 2024, the FBI identified a LinkedIn posting for a "Freelance Writer" posted by GPFI with a listed location of Nigeria. The posting contained a link to a LinkedIn profile with the display name "[redacted]," which appears to be a legitimate registered entity in Indonesia affiliated with the legitimate [redacted] non-profit organization. Also in September 2024, this legitimate LinkedIn profile had a post that contained text in English and Indonesian, which stated "Beware of job scam impersonating [redacted]. Currently, [redacted] is not hiring. The official email address for [redacted] is [redacted].org. If you are contacted using any other email, please disregard it." The post contained screenshots of two GPFI LinkedIn job posts with the word "FAKE" printed across them.

10. TARGET DOMAIN NAME 10 (safesec-group.com)

74. In approximately October 2024, the FBI identified an entity using the name Safe Sec Group (SAFESEC) and website www.safesec-group.com (**TARGET DOMAIN NAME 10,** last visited on April 6, 2026), which purported to be a UAE-based consulting firm. **TARGET DOMAIN NAME 10** was registered on August 2, 2024, one day after **TARGET DOMAIN NAME 9** was registered.

75. In or around March 2025, SAFESEC made job postings to multiple job hiring platforms for jobs that generally included vague descriptions and were targeted to individuals with experience in the government or military. One of these job postings on LinkedIn included email address hr@**TARGET DOMAIN NAME 10**. A LinkedIn Profile of the same name that was included in one of the LinkedIn job postings also included **TARGET DOMAIN NAME 10**. One of SAFESEC's job postings for a Security Operations Specialist listed the role would conduct geopolitical analysis and "[w]ork closely with the Trump Cabinet to ensure alignment of security strategies with organizational objectives." The job posting also listed "Bitcoin Payment" under "Desired Skills and Experience." One job posting noted SAFESEC was a company with over ten years of experience, headquartered in Dubai with branch operations in Honolulu. The FBI has been unable to substantiate the existence of a SAFESEC presence in Hawaii through open source and law enforcement database searches.

76. In or around June 2025, an identified U.S. person (Recruit A) who worked at an identified geopolitical analysis firm in Washington, D.C., reported a suspicious interaction with SAFESEC to the FBI. Recruit A applied to a job posted by SAFESEC on LinkedIn and was contacted by a "[redacted]" with an email address at **TARGET DOMAIN NAME 10**. Recruit A understood SAFESEC to be a UAE-based company, but in one email interaction, Recruit A saw Chinese characters next to the time and date headers. Additionally, when Recruit A sent a redacted sample report, Recruit A was asked for an unredacted version, which was unusual in Recruit A's experience in applying for similar positions.

11. TARGET DOMAIN NAME 11 (thetruthinfo.com)

77. In approximately September 2024, through open source research, the FBI identified an entity purporting to be a United Arab Emirates (UAE)-based think tank called The TruthInfo

(TRUTHINFO), which made postings on freelancing platforms to recruit a "Risk Strategy Advisor" and a "Senior Consultant/Director Policy & Public Affairs." The job postings linked to a website, www.thetruthinfo.com (**TARGET DOMAIN NAME 11**, last visited on April 6, 2026).

78. As of April 2026, jobs advertised on **TARGET DOMAIN 11** were for remote and part-time work with job titles such as "International Affairs Analyst," "Risk Strategy Advisor," and "Public affairs and strategic communication advisor," including responsibilities such as "Identify potential risks and develop mitigation strategies on the Middle East region or the Indo-Pacific region to address challenges and ensure project success." One job role indicated the "advisor" would conduct research "to grasp the latest trend of hotspots" and would be "required to obtain the most valuable information from reliable channels."

79. **TARGET DOMAIN NAME 11** was registered on August 20, 2024, less than three weeks after **TARGET DOMAIN NAME 9** and **TARGET DOMAIN NAME 10** were registered. In or around September 2024, **TARGET DOMAIN NAME 11** contained numerous instances of Chinese characters appearing on the screen, suggesting the individuals responsible for the website used a Chinese language tool to build **TARGET DOMAIN NAME 11**.[18] Furthermore, the "Compensation" section of a TRUTHINFO job posting on both a job posting website and on **TARGET DOMAIN 11** was substantially similar to the "Compensation" section of a RIGHTINFO job posting, specifically including the grammatically incorrect phrase: "the company will sign contract with them and pay salary monthly."

12. TARGET DOMAIN NAME 12 (vandercons.com)

80. In approximately March and April 2025, through open source research, the FBI identified an entity titled Van Der Consulting or VanderCons (VANDERCONS) with website

[18] As of April 17, 2026, no Chinese characters appeared on the screen when visiting **TARGETING DOMAIN NAME 11**.

https://www.vandercons.com (**TARGET DOMAIN NAME 12**, last visited on April 6, 2026), which purported to be based in Australia. The entity made postings to various job recruitment platforms recruiting for positions including International Trade Policy Analyst, Political Risk Analyst, and Strategic Communications Advisor. The jobs posted to LinkedIn were made by a LinkedIn profile with the same name that listed **TARGET DOMAIN 12** on its profile. The job postings indicated a preference for U.S. based candidates. The job postings for the International Trade Policy Analyst job indicated candidates would investigate and report on U.S. trade policies and the position would require engaging with "government insiders to uncover exclusive stories and trends." The postings indicated a preference for "[g]overnment-affiliated professionals," and candidates who could build networks with policymakers and experts.

81. As of on or about April 2026, **TARGET DOMAIN NAME 12** contained generic descriptions of consulting services, included numerous stock photos, and did not list any information about employees or executives. **TARGET DOMAIN NAME 12** listed an office location in Australia, but the job recruitment platform indicated that one of the VANDERCONS jobs was posted by a user with a listed location of Thailand.

82. Google search warrant return records link **TARGET DOMAIN NAME 12** to [redacted] persona, discussed in more detail below, which is also linked to **TARGET DOMAIN NAMES 1, 2, 6, 9, 12, and 13**. These records show that, in or around May 2025, email account [redacted]@gmail.com contained two emails identifying [redacted] as an employee of "Vander Consulting."

13. TARGET DOMAIN NAME 13 (gulfpeace.org)

83. In approximately December 2025, the FBI identified an entity called the Gulf Peace Foundation (GULF PEACE) with website www.gulfpeace.org (**TARGET DOMAIN NAME 13**,

last visited on April 6, 2026). The website contained numerous stock photos and what appeared to be AI-generated images, as well as broken links to social media accounts.

84. As of at least early December 2025, a Facebook profile with the display name "[redacted]" listed current employment with the Gulf Peace Foundation and past employment with the Global Peace Foundation. The profile picture for [redacted] appeared to match another Facebook profile with the same display name that listed past employment with CENTRIK and RIGHTINFO (**TARGET DOMAIN NAMES 1** and **2**, respectively). The [redacted] persona and its association with CENTRIK are discussed in more detail below.

85. In or around February 2026, the FBI identified a Bluesky profile with display name "[redacted]" that listed employment with the Gulf Peace Foundation and included a link to **TARGET DOMAIN NAME 13**. The Bluesky handle for this profile was "[redacted]," which is similar to "[redacted]."

86. In or around January 2026, GULF PEACE made a job posting on LinkedIn for a remote position with the title "Senior Current Affairs Advisor"; the successful applicant would be responsible for analyzing global affairs, writing analytical papers, and providing "advice on complex and sensitive issues." The job posting specified a preference for candidates with experience in geopolitical affairs, diplomacy, or think tanks. As of April 2026, the GULF PEACE LinkedIn profile lists **TARGET DOMAIN NAME 13** in the About section of their profile.

E. The Conspirators Use of Foreign-Based Financial Accounts to Pay for U.S. Website Registrations

87. As noted above, the conspirators have paid for webhosting and domain services provided by U.S. companies through debit and credit cards issued by foreign banks and cryptocurrency. The FBI has obtained and reviewed available payment information for some of the **TARGET DOMAIN NAMES**. The results are detailed in the following paragraphs.

88. **TARGET DOMAIN NAME 6** was registered and renewed by two separate users, both with addresses in Pakistan. It was paid for using a credit card issued by Standard Chartered Pakistan, a bank headquartered in Pakistan. Payment was made to Namecheap, Inc., a company headquartered in Phoenix, AZ, via payments processing company Stripe, Inc., a company headquartered in San Francisco, CA.

89. **TARGET DOMAIN NAME 7** was registered by a user with an email address with thehorizzen in the moniker. The user's address was listed in India, and the domain was paid for using an Indian bank issued credit card. On the date of registration, the user logged in from an Indian IP address. Payment was made to Wix.com, a company based in New York, NY.

90. **TARGET DOMAIN NAME 8** was registered by "NYC Detal [sic] Hospital" with the true address of a dental business of the same name. The phone number given was the actual phone number of the same dental business and the email address was a ProtonMail email with a name seemingly unrelated to the dental business. Payments for the domain registration were made to Namecheap, Inc., a company headquartered in Phoenix, AZ, via cryptocurrency.

91. **TARGET DOMAIN NAME 10** was registered by three different names with the same company name, Future InfoBiz IT Solutions, and the same email address, which appears to be associated with the company name. The domain registrants used four different United Arab Emirates (UAE) bank-issued cards and two different Indian bank issued cards. Payment was made to Wix.com, a company based in New York, NY.

92. **TARGET DOMAIN NAME 12** was registered by an individual with an address in Thailand who registered multiple other domains unrelated to this investigation. Full payment information for **TARGET DOMAIN NAME 12** was not available, but the records indicated the payment, made to Spaceship.com, a company headquartered in Phoenix, AZ, originated from

Thailand. The user paid for all other domain registrations on the account by a Thai bank issued credit card.

93. **TARGET DOMAIN NAME 13** was registered to a user with address "123 Market Street" in Delaware. Searches for the address did not show it linked to any actual business or apparent residence. The U.S. phone number listed had a New York area code and ended in 555-0123. Of note, the email address associated with the registration was the same email address used to register **TARGET DOMAIN NAME 2**. During the FBI's review of search warrant returns for this email address, the FBI identified a document that appeared to be a script for an "HR Director" for **TARGET DOMAIN NAME 2** to read to a prospective recruit for a consulting business. The billing information for **TARGET DOMAIN NAME 13** showed the account was paid for by [redacted]" with a credit card issued by Shanghai Pudong Development Bank in China. Account change information showed the currency was changed to Hong Kong Dollars in November 2025. **TARGET DOMAIN NAME 13** was set up with the following email address for use: info@gulfpeace.org, career@gulfpeace.org, and richard@gulfpeace.org. Payment was made to GoDaddy.com LLC, a company based in Tempe, AZ.

F. <u>The Conspirators' Use of Stolen Identities Belonging to Actual U.S. Persons</u>

Use of Real U.S. Persons' Information to Register Websites and Accounts

94. As detailed above, Identity Theft Victim 1's name was used to register **TARGET DOMAIN NAMES 1** and **2**. The FBI interviewed Identity Theft Victim 1 in October 2025. Identity Theft Victim 1 stated she/he has never registered an internet domain and has never heard of MonsterMegs, Hosteons, RightInfo Consulting (affiliated with **TARGET DOMAIN NAME 2**), or Centrik Global Consulting (affiliated with **TARGET DOMAIN NAME 1**). Based on the IP address logins associated with [redacted]@gmail.com and travel records

showing Identity Theft Victim 1 was in the United States at the times [redacted]@gmail.com was accessed by foreign IP addresses, I believe Identity Theft Victim 1's information has been used by individuals other than Identity Theft Victim 1 to appear more legitimate and obfuscate the true identity of the people operating **TARGET DOMAIN NAMES 1** and **2**.

95. As also detailed above, Identity Theft Victim 2's identity has been used by CENTRIK (affiliated with **TARGET DOMAIN NAME 1**) and PWG (affiliated with **TARGET DOMAIN NAME 5**). As detailed below, Identity Theft Victim 2's identity has been used by CENTRIK in recruitment schemes. The FBI's investigation has identified Identity Theft Victim 2 as an actual U.S. Person who was [redacted]. Copies of the U.S. passports for Identity Theft Victim 2, along with other U.S. persons [redacted], were posted for sale on a cyber-criminal marketplace. The FBI interviewed Identity Theft Victim 2 in December 2025. Identity Theft Victim 2 told the FBI that his/her personal information was stolen [redacted] as part of a data breach. Identity Theft Victim 2 had never heard of CENTRIK nor held any human resources roles. Identity Theft Victim 2 did not recognize any of the profiles created in his/her name that were identified as part of this investigation.

Use of Identity Theft Victim 2's Identity Linked to Hong Kong, China, and Macau.

96. Records obtained from Google and open-source research revealed that [Identity Theft Victim 2]@gmail.com was registered on or about May 21, 2024, from an IP address that resolved to the Internet Service Provider China Unicom (Hong Kong) Operations Limited in Hong Kong. Records obtained from Meta and open-source research show that [Identity Theft Victim 2]@gmail.com is associated with a Facebook account with the name "[redacted]" that was created on or about June 20, 2024, from an IP address that also resolved to the Internet Service

Provider China Unicom (Hong Kong) Operations Limited in Hong Kong. That second IP Address, 203.160.71.136, was used to access [Identity Theft Victim 2]@gmail.com on the same date. Specifically, [Identity Theft Victim 2]@gmail.com was logged into by IP address 203.160.71.136 approximately 13 times on or about June 20, 2024, the same day it was used to register a Facebook account for "[redacted]." Similarly, on or about July 19, 2024, the Google account for [Identity Theft Victim 2]@gmail.com and the Facebook account associated with [Identity Theft Victim 2]@gmail.com and the name "[redacted]" were logged into by the same IP address, 203.160.71.176. This IP address resolves to the internet service provider China Unicom (Hong Kong) Operations Limited in Hong Kong.

97. According to Google records, [Identity Theft Victim 2]@gmail.com has an associated Android device with a listed user of [Identity Theft Victim 2]@gmail.com. The time zone for the Android device is Asia/Shanghai, and the associated locale is zh_CN_#Hans (believed to refer to China). According to MCC-MNC research, the Android's SIM operator resolves to Macau (China), and the Android's cell operator resolves to China.

98. According to records provided by Google, on or about January 9, 2025, [Identity Theft Victim 2]@gmail.com received an email from [redacted]@centrikglobalconsulting.com [**TARGET DOMAIN NAME 1**]. According to records provided by LinkedIn and Meta and information outlined later in this affidavit, [redacted] is another online persona affiliated with CENTRIK and **TARGET DOMAIN NAME 1**. Records from Meta revealed a Meta account affiliated with [redacted] that was registered on or about April 17, 2024, with IP address 103.143.92.160, and with currency set to CNY. Open-source searches show this IP address resolves to China Telecom(macau) Company Limited in Macao.

99. According to records provided by Hosteons in January 2025, CENTRIK has

multiple different email addresses affiliated with **TARGET DOMAIN NAME 1**, including one impersonating Identity Theft Victim 2, one using the [redacted]" persona, and some with obvious fake names, such as:

a. Identity Theft Victim 2, [Identity Theft Victim 2]@centrikglobalconsulting.com;

b. Bat Wayne bat-wayne@centrikglobalconsulting.com;

c. Bruce Wayne, bruce-wayne@centrikglobalconsulting.com;

d. [redacted]@centrikglobalconsulting.com;

e. [redacted]@centrikglobalconsulting.com;

f. [redacted]@centrikglobalconsulting.com;

G. Evidence of Chinese State-Sponsored Activity and the Use of Fictitious Personas

100. In approximately March 2024 and May 2024, the FBI received a tip that LinkedIn accounts affiliated with CENTRIK and RIGHTINFO (**TARGET DOMAIN NAMES 1** and **2**, respectively) may be engaging in Chinese state-sponsored activity. The tip included a LinkedIn account affiliated with [redacted]@gmail.com, LinkedIn display name: [redacted] and an account purportedly affiliated with Identity Theft Victim 2,[19] email address: [Identity Theft Victim 2]@centrikglobalconsulting.com [**TARGET DOMAIN NAME 1**]. As noted above, someone using the name of Identity Theft Victim 2 created a LinkedIn account on or about December 4, 2023, from an IP address resolving to China. According to Google records for [redacted]@gmail.com, the country for the account's Terms of Service changed from Bangladesh to Hong Kong on or about March 4, 2024.

101. Other evidence links [redacted]@gmail.com to China. On or

[19] As discussed in more detail below, Identity Theft Victim 2 is a U.S. Person whose United States passport was posted for sale on a cyber-criminal marketplace.

about April 26, 2024, [redacted]@gmail.com received an email in Chinese from online@6park.com with a subject written in Chinese characters that translates to "Liuyuan account activation email;" the body of the email included an account activation link for an email account at the 6park.com domain, a Chinese internet forum. On or about May 30, 2024, [redacted]@gmail.com sent an email titled "baoxiao" with two excel spreadsheets attached with titles in Chinese characters. A rough translation of "Baoxiao" in English is "to reimburse;" rough translations of the titles of the spreadsheet files are "February reimbursement" and "Screenshot of reimbursement summary for March and April." The excel spreadsheets appear to contain screenshots of payments made in cryptocurrency.[20]

February to August 2024: CENTRIK's Use of Identity Theft Victim 2's Identity to Recruit SUBJECT A

102. Based on Google records, on or about February 6, 2024, SUBJECT A received an email from careers@centrikglobalconsulting.jobsoid.com. From approximately February 7, 2024, to August 6, 2024, SUBJECT A exchanged approximately 31 emails with emails affiliated with centrikglobalconsulting.jobsoid.com.

103. According to Hosteons records, on or about May 16, 2024, SUBJECT A emailed info@centrikglobalconsulting.com [**TARGET DOMAIN NAME 1**], with the Subject: "Telegram communication with [redacted]" with the following:

> Good day,
> I am one of the consultants working with [redacted]. For some odd reason, my Telegram account was deleted today. I am no longer able to access my account. I have asked Telegram support for assistance, but would you please relay the message to [redacted]
> Is there another way I can communicate with [redacted]
> Kind regards

[20] [redacted]@gmail.com is linked to nine other Google accounts by IP address 37.111.199.80 used to sign the Terms of Service with Google within a matter of three days. An open-source search of this IP address reveals it resolves to Dhaka, Bangladesh.

[SUBJECT A]

104. According to Hosteons records, on or about May 16, 2024, CENTRIK GLOBAL CONSULTING LIMITED, using careers@centrikglobalconsulting.jobsoid.com, wrote the following message to SUBJECT A:

> Hi [SUBJECT A]. I received it and will relay all of the info to him. Our leadership said in the meeting that you are the best cooperator, and it is pretty nice to work with you. We all see your effort in the report. So don't worry, we highly value our partnership. [redacted] is in the meeting now, I promise he will get back to you when he is available. If you need any other assistance, please feel free to let me know.
> Kind regard,
> [Identity Theft Victim 2's First Name]

105. On or about July 23, 2024, and July 24, 2024, SUBJECT A sent a series of additional emails to other CENTRIK-related email addresses inquiring about [redacted] well-being and wondering if the company was satisfied with SUBJECT A's work.

May to July 2024: TARGET DOMAIN NAME 2's Use of "[redacted]" Persona to Recruit a U.S. Person

106. As part of its investigation, the FBI has reviewed records, including communications, for **TARGET DOMAIN NAME 2**. These records indicate that **TARGET DOMAIN NAME 2** has been used in the same way as **TARGET DOMAIN NAME 1**, that is, to target current and former U.S. government employees. Communications from approximately May 2024 to July 2024 between email account [redacted]@rightinfoconsult.com [**TARGET DOMAIN NAME 2**] ([redacted] believed to be a fictitious persona) and Recruit B show that [redacted] solicited Recruit B to write at least one report and that Recruit B shared payment information. The FBI has confirmed that Recruit B is a U.S. person who has held an active Top Secret clearance with the U.S. military since at least [redacted]

107. The **TARGET DOMAIN NAME 2** communications show that Recruit B provided Recruit B's resume to [redacted] this resume indicated that Recruit B maintained a Top

Secret/Sensitive Compartmented Information (SCI) clearance and was an active-duty member of the U.S. military from [redacted]. Recruit B provided his/her PayPal account information and Telegram account to [redacted] Within the **TARGET DOMAIN NAME 2** emails, in or around [redacted], Recruit B provided one report titled, "United States Strategic Interest in the [redacted]: Objectives and Talking Points." It is unclear if she/he was paid for this report.

108. The **TARGET DOMAIN NAME 2** communications, specifically the resume, payment information, and report sent by Recruit B to [redacted] further supports that **TARGET DOMAIN NAME 2** has been used to recruit U.S. government employees such as military servicemembers with active security clearances to obtain sensitive and potentially classified information.

July 2024: CENTRIK's Use of Identity Theft Victim 2's Identity and "[redacted]" Persona for Recruitment

109. As discussed above, the FBI received a tip [redacted] that a LinkedIn account purportedly affiliated with Identity Theft Victim 2 may be engaging in Chinese state-sponsored activity. As noted above, a LinkedIn account in the name of Identity Theft Victim 2 was registered on or about December 4, 2023, from IP address that resolved to China. This LinkedIn account is associated with email addresses [Identity Theft Victim 2]@centrikglobalconsulting.com [**TARGET DOMAIN NAME 1**] and a second email account. The Identity Theft Victim 2 LinkedIn account advertised the user as "a Policy Analyst at a renowned CENTRIK, dedicated to providing reliable insights and recommendations to policymakers through in-depth research and analysis." In or around December 2023, a person using Identity Theft Victim 2's LinkedIn account messaged multiple people on behalf of CENTRIK, asking them to join a part time project that focuses on "global military and geopolitical hotspots." When asked for clarification on what this meant, a person using Identity Theft Victim 2's LinkedIn account provided feedback that the topics

are dynamic but include the "Russia-Ukraine conflict, The Israeli-Palestinian conflict, 2024 US Presidential Election, cyber-attacks, [and] Indo-Pacific strategy." The person using Identity Theft Victim 2's LinkedIn account offered to pay people via PayPal, Wise, and cryptocurrency.

110. On or about July 18, 2024, [Identity Theft Victim 2]@centrikglobalconsulting.com **[TARGET DOMAIN NAME 1]** sent the following email to an applicant that applied for an International Affairs Consultant position with Centrik and signed the email "Best regards, [redacted] HR Director Rightinfo Consulting Corporation:"[21]

> Subject: Re: Application for International Affairs Consultant
>
> Hi,[Redacted].
>
> Thanks for your application. After carefully reviewing your resume and cover letter, we are keen to have a further discussion with you about our potential cooperation. I am delighted to provide you with more detailed information about the role and discuss the next steps in the hiring process. The position we are offering is fully remote and requires the analyst to conduct extensive research on specific regions to identify important issues such as potential political changes, military conflicts, and security policy changes in the region. Analysts should be proficient in sourcing authentic information from various sources and analyzing international geopolitical and regional security policies from different perspectives simultaneously like
> Therefore, during the recruitment process, qualified candidates will be invited to participate in a paid assessment test to better identify their potential capabilities and alignment with the job. This test will be customized base on their background and our concerns, and entail the completion of a research report on a specific topic. Successful completion of the assessment will result in a remuneration of $500. If you are willing to take our test, please share your expertise brief. It will helps us to customize the topic that best suits you.
> Looking forward to your early reply.
>
> Best regards,
> [redacted]
> HR Director
> Rightinfo Consulting Corporation

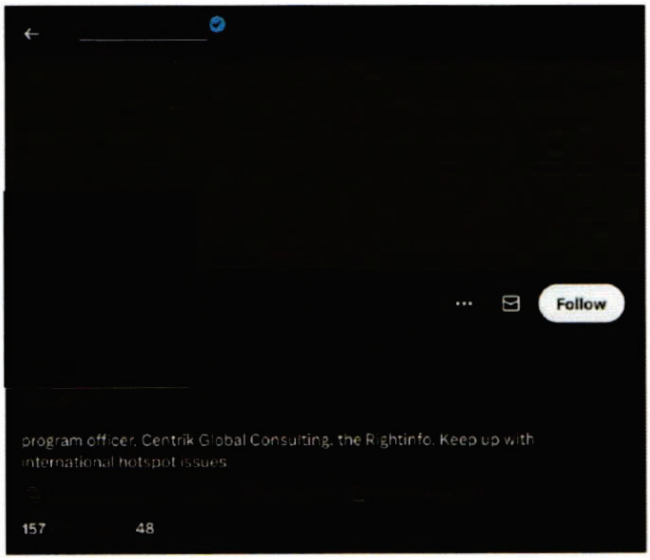
111. Based on my training and experience, the information above indicates that

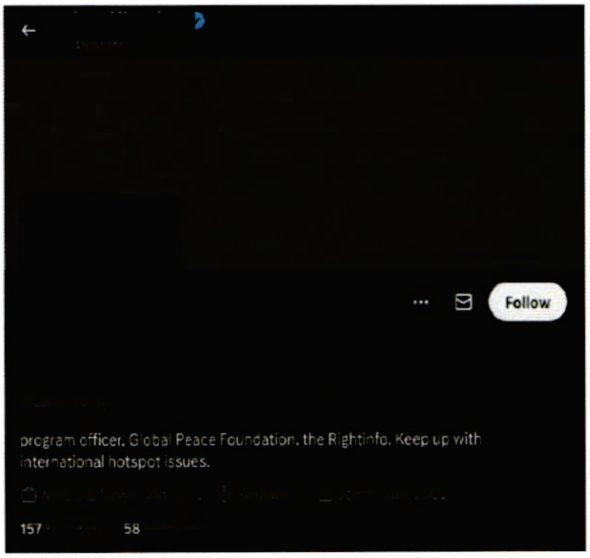
[21] Errors in this quotation and those below are in the original.

CENTRIK and RIGHTINFO are likely front companies used by the PRCIS to spot, assess, and recruit individuals to obtain sensitive and nonpublic U.S. government information, among other things.

July 2024: TARGET DOMAIN NAME 2's Use of "[redacted] Persona to Recruit a U.S. Person

112. The March 2024 tip about LinkedIn accounts that may be engaging in Chinese-state sponsored activity (described above at para. 100) included a LinkedIn account for [redacted]" [redacted]@rightinfoconsult.com [**TARGET DOMAIN 2**]. In September 2024, the FBI interviewed Recruit C, a U.S. person residing in the United States, regarding a suspicious message (detailed below) she/he had received in July 2024, while Recruit C was in the United States, from "[redacted]" on Twitter/X and that Recruit C had described as potentially "some sort of either Russian or Chinese agitprop." Open-source checks have revealed that, as of on or about September 13, 2024, [redacted], @[redacted] listed his employment as a program officer with CENTRIK and listed an affiliation with RIGHTINFO. Open-source searches conducted on or about September 27, 2024, and March 4, 2025, revealed that [redacted] no longer listed employment as a program officer with CENTRIK. Instead, the profile listed the following: "program officer, [redacted]. the Rightinfo. Keep up with international hotspot issues." [redacted] is a well-known, legitimate non-profit organization, as discussed above, and is similar in name to GPFI, affiliated with **TARGET DOMAIN NAME 12**. The "[redacted]" profile posts are shown below:





113. Recruit C is a career national political reporter [redacted].

114. On or about July 23, 2024, Recruit C received a message on X from [redacted], @[redacted] wrote to Recruit C:

> Hello [Recruit C],
> I am [redacted] BD manager from the Rightinfo Consulting Singapore, website: rightinfoconsult.com.[22] We are looking for experts in US politics and foreign policy. Considering your experience and knowledge, would you like to be our Senior Analyst? This is a part-time position and will not affect your current job. If you're interested, I'd like to discuss the role's responsibilities and compensation with you further.
> Best wishes,
> [redacted]

115. On or about July 25, 2024, [redacted] emailed Recruit C from [redacted]@rightinfoconsult.com **[TARGET DOMAIN NAME 2]** the following with the Subject line: "Continue the role discussion on X:"

[22] **TARGET DOMAIN NAME 2.**

Hi [Recruit C],
You gave me your email address on X.
We appreciate your knowledge and experience and would like you to advise us on American politics and other issues. Usually in written form. 1 to 2 pieces per month. The topic is determined by us. The compensation is 1.5k$-2.5k$ per piece at the beginning. I'd be happy to answer any questions you may have.
Thank you,
[redacted]

Recruit C told the FBI that, after receiving the communication from [redacted] Recruit C did his/her own research. Recruit C looked at the website [redacted] provided and after viewing **TARGET DOMAIN NAME 2**'s stock photos, Recruit C saw news stories about bombings and feminist Nazis on **TARGET DOMAIN NAME 2** indicating to Recruit C that the company may not be legitimate. [redacted] offer of $1,500 to $2,000 per piece was the most glaring indicator this likely was not a legitimate freelance request. This was a lot of money compared to other offers for reporters to do freelance work.

Fall of 2024: CENTRIK's Use of "[redacted] Persona to Recruit a U.S. Government Contractor

116. In November 2024 and February 2025, the FBI interviewed Recruit D, a U.S. person working for a U.S. government contractor. Around September 2024, Recruit D applied to a Political Dynamics Consultant (Remote) job with CENTRIK via LinkedIn. To apply, Recruit D sent their resume—which included mention of their holding a Secret level security clearance from [redacted] and personal email—on LinkedIn.

117. Open-source searches conducted on or about August 28, 2024, identified multiple jobs posted on LinkedIn for "Political Dynamics Consultant(Remote)" by CENTRIK that required the following qualifications: Bachelor's or Master's Degree in Public Policy, International Development or related fields with work experience in the public sector. The position responsibilities included conducting assessments of "geopolitical risks affecting client interest,

including regional conflicts, economic sanctions, and security threats"; analyzing legislative and regularly developments at local, national, and international levels; and assessing the potential impact of policy changes on client operations, investments, and strategic objectives; among other things.

118. On or about September 25, 2024, Recruit D received an email from [Identity Theft Victim 2]@gmail.com, using Identity Theft Victim 2's name and the title, "HR Director" for "Centrik Global Consulting," thanking Recruit D for their application and inviting Recruit D to complete "a paid assessment test" by preparing a report on a topic relevant to their expertise. The user of [Identity Theft Victim 2]@gmail.com said that Recruit D would be paid $500 upon successful completion of the assessment and thanked Recruit D for their interest in CENTRIK.

119. Based on the interviews with Recruit D, documents Recruit D provided Recruit D's employer that were provided to the FBI, records obtained from Google and Meta, and open-source research, CENTRIK has used Identity Theft Victim 2's name and identity as an online persona.

120. On or about September 28, 2024, a user of [Identity Theft Victim 2]@gmail.com sent Recruit D the topic to write about, specifically Israel's assassination of Hassan Nasrallah and its potential to bring Iran and the United States into a wider conflict, and included the following questions for Recruit D to write about: "What is Iran's internal assessment of this situation?" "Has Iran had any private communication with Hezbollah in Lebanon?" and "What is Iran planning to do next?" The user of [Identity Theft Victim 2]@gmail.com requested that Recruit D send the report within three days and that information from "well-informed sources will be welcomed." On or about October 2, 2024, Recruit D sent the completed report to [Identity Theft Victim 2]@gmail.com.

121. On or about October 9, 2024, a user of [Identity Theft Victim 2]@gmail.com asked Recruit D to create a Telegram and PayPal account to continue communication and receive payment.

122. On or about October 10, 2024, a person using @[Identity Theft Victim 2] contacted Recruit D on Telegram.[23] The person using @[Identity Theft Victim 2] sent the following message to Recruit D:

> Hi, [Recruit D], here is [Identity Theft Victim 2's first name]. It is glad to connect to you in this platform. I have contacted my colleague [redacted] from the analysis department to share their feedback on your report, and he will also directly discuss the details of the follow-up cooperation. He will reach out to you soon.

123. On or about October 13, 2024, or October 14, 2024, a Telegram account "[redacted] username @[redacted], sent Recruit D the following message via Telegram:

> Hi, [Recruit D], Nice to have your reply.
> I have just reviewed your report about Middle East. First of all, I really appreciate your efforts to the report. Here are some suggestions to you.
> As we told you before, we hope exclusive information rather than simple analysis. However, the report is full of public information and well known facts, which is very superficial and not very useful. As we have OSINT branch in the company, we hope you to submit reports with insider and exclusive insights rather than just listing the public media information.
> After consideration, cuz it's the firtst time of cooperation, as to show our sincerity and credibility, the company will still pay you 500USD, which will be given to you soon.
> As to push forward our cooperation, we also want to hear about your opinion about how to improve the quality of report in the future, especially to gain exclusive and insightful information.

124. The following messages between Recruit D and [redacted] took place between approximately October 13, 2024, and October 19, 2024.

---

[23] Open-source searches revealed a telegram account, @[Identity Theft Victim 2], that is purportedly affiliated with "Identity Theft Victim 2" and which states the following in its bio: "HR Director, Centrik Global Consulting." As noted above, CENTRIK has used Identity Theft Victim 2's name for a **TARGET DOMAIN NAME 1** email address: Identity Theft Victim 2, [Identity Theft Victim 2]@centrikglobalconsulting.com.

125. After Recruit D responded to [redacted] seeking guidance and feedback and asserting that Recruit D did not have access to classified information, [redacted] responded to Recruit D with the following message:

> Thanks for reply. After reviewing your CV, you have worked in [redacted], and you write down the clearance in the CV, so I thought maybe you have some exclusive inside information. But it's OK, so now you have already left the [redacted]?

126. Recruit D explained to [redacted] that Recruit D "would never be able to reveal secretive government information to you or your company. That is illegal." [redacted] responded to Recruit C: "I don't ask you to break the laws. We think we can find out a way suitable to both of us to gain exclusive information. I will make the payment done first."

127. Recruit D reminded [redacted] that Recruit D did not work for the U.S. government and did not have access to any of that information. [redacted] responded to Recruit D: "I think if you can reach to some well-informed sources to make interview, then we can get such info. I mean exclusive, no classified." Recruit D responded to [redacted] that Recruit D did not have access to "exclusive information," asked [redacted] not to send Recruit D any money, and reaffirmed that Recruit D "would not like to be associated with anything illegal."

128. [redacted] then sent Recruit D the following messages:

> Friend, what we do is definitely legal consultancy job. We have plenty of consultants all over the world. As a consultancy company, our priority is to make insightful and qualified report for our clients, so we need to ensure the report full of insights.
>
> Friend, let's just try some times cooperation, you will know our professionalism and sincerity.
>
> I understand your concern, I hope you can also understand our requirements to submit enough qualified reports to clients
>
> i don't meant to offend you, just hope to build good partnership

Recruit D then told [redacted] not to contact Recruit D again because Recruit D was not interested.

129. On or about October 19, 2024, [redacted] messaged Recruit D: "Friend, the financial department has already transferred the 500usd to your PayPal. Please check it. I still hope to keep partnership with you, really hope you to reconsider our cooperation." On or about October 21, 2024, Recruit D received a $500 payment via PayPal from "[redacted]" with associated email address [redacted]@outlook.com. A review of this PayPal account indicated it was registered to a [redacted] with an address in Great Britain. The linked payment accounts were five different China-issued credit or debit cards in the name [redacted] with the following banks: Ping An Bank Co Ltd., Bank of China Limited, Agricultural Bank of China, Shanghai Pudong Development Bank, and Bank of Communications.

Fall of 2024: SUBJECT A's Creation of the "[redacted]" Persona for CENTRIK Recruitment

130. According to LinkedIn records, on or about November 6, 2024, a LinkedIn account was registered for "[redacted]" "Deputy Director, Personnel at Centrik Global Consulting," geo location: United Kingdom, email address: [redacted]@centrikglobalconsulting.com [**TARGET DOMAIN NAME 1**], from IP address 41.193.163.237. According to LinkedIn records, this account is linked to SUBJECT A's account via cookies. On the same day that IP address 41.193.163.237 was used to create the LinkedIn account for "[redacted]," SUBJECT A logged into his/her LinkedIn account in his/her true name from that same IP address. SUBJECT A used that IP address, 41.193.163.237, to log into or access the LinkedIn account in his/her true name on multiple occasions, including on September 16, 2024; October 14, 2024; October 18, 2024; November 11, 2024; and November 12, 2024. Based on open source searches this IP address, 41.193.163.237, resolves to South Africa, where SUBJECT A lived at the time.

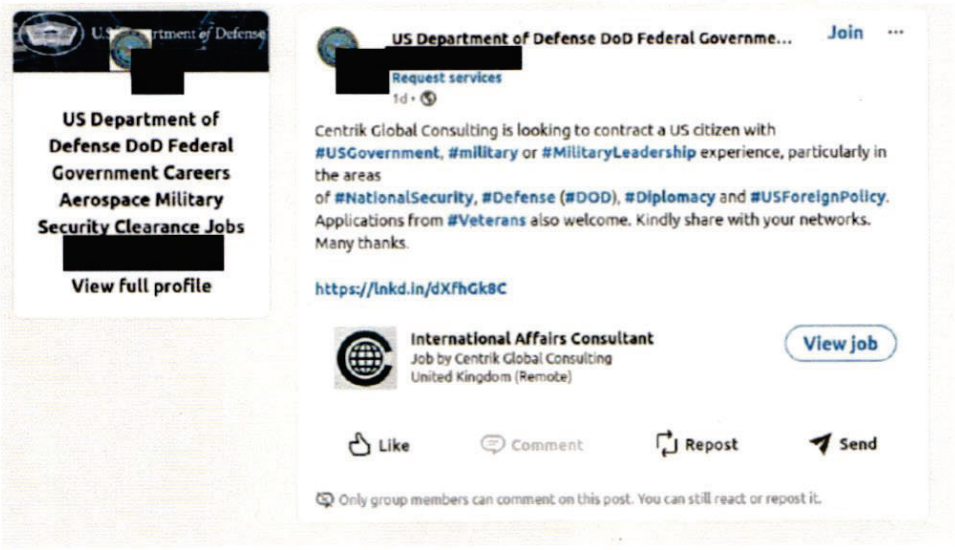
131. Based on the information above, along with other information developed in this investigation, I believe SUBJECT A created a LinkedIn in the fake name "[redacted] to continue to recruit current and former U.S government employees to work for CENTRIK. SUBJECT A used this fake name along with accounts in his/her true name to target and recruit current and former U.S. government officials on behalf of CENTRIK.

H. SUBJECT A's Targeting of Current and Former U.S. Government Officials Through CENTRIK From August to November 2024

132. As discussed below, based on records obtained from LinkedIn, PayPal, Google, Meta, and X; and open-source research, SUBJECT A appears to have worked for and/or operated CENTRIK from at least May 2024 through November 2024. As detailed below, CENTRIK (affiliated with **TARGET DOMAIN NAME 1**) has posted jobs on LinkedIn and elsewhere specifically requesting current or former U.S. government experience.

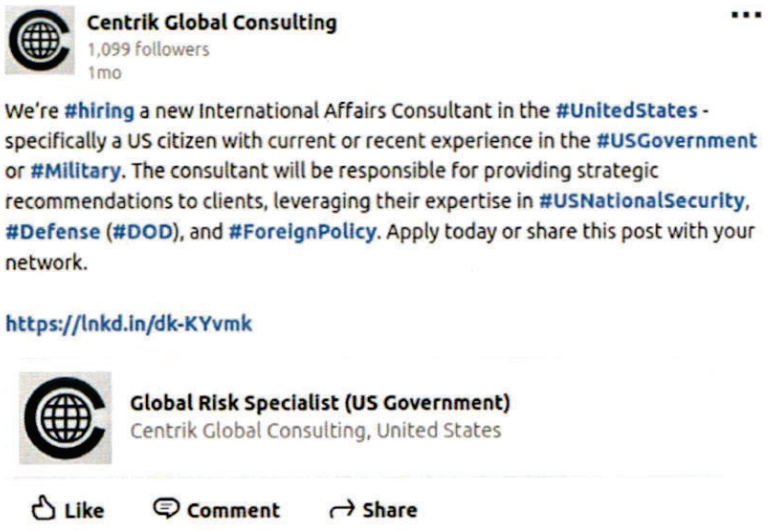
CENTRIK's Job Postings Directed at Current and Former U.S. Government Employees

133. On or about August 22, 2024, approximately seven days after SUBJECT A set up CENTRIK's LinkedIn page, SUBJECT A posted the following job listing in a LinkedIn group with the name "US Department of Defense DoD Federal Government Careers Aerospace Military Security Clearance Jobs":



134. Open-source research conducted on August 26, 2024, identified a LinkedIn job posting for CENTRIK for an "International Affairs Consultant," described as follows: "This is a contract remote role for a US-based Consultant at Centrik Consulting, ideal for US citizens with current or recent experience in the US Government or Military. The consultant will be responsible for providing strategic recommendations to clients, leveraging their expertise in US National Security, Defense (DOD), and Foreign Policy" with the following qualifications: "strong understanding of US Government operations, DOD strategies, and American diplomatic efforts" and "current or recent experience in US Government or Military institutions, including leadership roles in national security or defense", among others.

135. In or around September 2024, CENTRIK's public LinkedIn page posted the following job listing for a "Global Risk Specialist (US Government)":



136. On or about September 19, 2024, open-source searches identified a job posting by CENTRIK on LinkedIn with the title "Global Risk Specialist (US Government)." The role is described as follows: "This is a contract remote role for a US-based Consultant at Centrik Global Consulting, ideal for US citizens with current or recent experience in the US Government or Military. We are particularly interested in candidates who have served in the Central Intelligence Agency (CIA) and Congress." The job posting qualifications are "current or recent experience in the CIA" and "current or recent experience as a US Congressional Aide or Legislative Assistant, especially from a minority ethnic group, with a deep understanding of US Government operations, DOD strategies, American diplomatic efforts, and religious affairs."

137. According to LinkedIn records, starting in approximately August 2024, SUBJECT A messaged multiple individuals as a representative of CENTRIK looking to hire individuals who could obtain "exclusive inside information on key government/military issues." As explained below, SUBJECT A sent individual consulting contracts, confidentiality agreements, and coordinated PayPal payments on behalf of CENTRIK. From approximately September 2024 to November 2024, SUBJECT A recruited at least seven current and former U.S. government

employees to obtain sensitive or nonpublic U.S. government information for CENTRIK.

SUBJECT A Recruits Former [redacted] Employee to Work for CENTRIK

138. According to LinkedIn records, SUBJECT A was in communication with Recruit E. According to Recruit E's LinkedIn, Recruit E was an [redacted] from [redacted]. According to Recruit E's LinkedIn, from [redacted], Recruit E worked [redacted] with the [redacted] According to government records, Recruit E previously held a Top-Secret SCI clearance through his/her employment with [redacted] Recruit E was debriefed [redacted] and no longer holds an active security clearance.

139. A selection of messages exchanged between SUBJECT A and Recruit E via LinkedIn is below at paras. 140-145. All typographical errors were in original messages.

140. On or about August 26, 2024, SUBJECT A messaged Recruit E as follows:

> Hi [Recruit E], Thank you for your application. I am contacting you in my capacity as a representative of Centrik Global Consulting, a UK headquartered risk management consultancy. We're looking to hire a US citizen who is able to obtain exclusive insights on key government/military issues from their contact network. We are not looking for secret information, only insight that our internal team cannot obtain. A recent question from a client was related to NATO's assessment of Ukraine's attack on the Russian mainland. The deliverable is typically a report of between 1500-3000 words, and payment for a standard report starts at $1,000 and increases based on the quality of the insight (as determined by our client). Would this opportunity be of interest to you? Regards, [SUBJECT A's first name]

141. That same day, Recruit E responded to SUBJECT A indicating Recruit E's interest in moving forward with the application process. On or about August 27, 2024, the next day, SUBJECT A asked Recruit E, if Recruit E had "a particular area of expertise in the geopolitical realm." After Recruit E responded with his/her areas of expertise, SUBJECT A wrote:

> The topic is the following: Internal views of the US government on the current situation in Russia and Ukraine and next considerations. The topic is sufficiently broad to be able to choose an angle that suits you best,Â For the time frame, let's look at the next few weeks

to months (tactical considerations). The USG's likely plans are most important. Feel free to address political stability, security, arms sales factors, and any other important factors you deem worthy of mentioning, but the key is very specific information that is of a granular nature. You will be remunerated for the report. Can you share any details about the sources you will be consulting?

142. On or about August 28, 2024, Recruit E attached a paper on the [redacted] conflict and the United States. The following messages were all exchanged on or about August 29, 2024, the next day:

SUBJECT A	Are you perhaps able to include any inside information specific to a particular incident?
Recruit E	Hi, yes. I can describe some instances on the efforts to prevent more citizens being taken and on the military industry topics. I will have to be careful about how much details so as to not disclose anything my contacts wish to ensure prevents spillage.
SUBJECT A	Yes please go ahead and add more at your discretion.
SUBJECT A	Would you like to move over to Telegram messaging app to continue discussing? Can you send me your username?
SUBJECT A	the company will maintain the utmost confidentiality for you andÂ your work.
SUBJECT A	Maximize the granularity of information as much as possible, and the company will pay a higher amount for the report.

143. On or about September 2, 2024, SUBJECT A messaged Recruit E, asking about an updated report. On or about September 5, 2024, Recruit E told SUBJECT A to "check your email."

144. On or about September 9, 2024, SUBJECT A told Recruit E: "We've reviewed your report and are happy to announce we would like to move forward. Typical next steps include moving the conversation onto the Telegram messaging app, where we discuss next steps. This will include a contract, discussion of remuneration for the trial report."

145. SUBJECT A told Recruit E on or about September 11, 2024, that CENTRIK would pay Recruit E for the report via PayPal. According to PayPal records, from approximately September 13 to 19, 2024, Recruit E received three payments totaling $[redacted] from three seemingly

unrelated persons using three seemingly unrelated email addresses: [redacted]@gmail.com, [redacted]@gmail.com, and [redacted]@gmail.com. According to Recruit E's PayPal records, on or about September 20, 2024, these PayPal payments were reversed. On that same day, September 20, 2024, Recruit E emailed [redacted]@centrikglobalconsulting.com [**TARGET DOMAIN NAME 1**] the following about a "hiccup" with his/her PayPal account and PayPal had to return the money she/he was already paid. A review of these three PayPal accounts indicated one was registered to a [redacted], email address [redacted]@gmail.com, with addresses in Florida and California. The account had no linked payment accounts. Another account was registered to a [redacted], email address [redacted]@gmail.com, with addresses in Georgia and Florida. The account had no linked payment accounts. The third account was registered to a [redacted], email address [redacted]@gmail.com, with an address in Florida. The account was linked to five different China issued debit or credit cards in the name [redacted]. These were the same cards as were linked to the PayPal account used to pay Recruit D, as detailed above.

146. Recruit E sent a report to "[redacted]" on or about September 20, 2024. On that date, Recruit E emailed [redacted]@centrikglobalconsulting.com [**TARGET DOMAIN NAME 1**] including a message that "[a]ttached is the final document on the 3rd assignment." In this September 20, 2024 email, Recruit E attached a pdf document labeled "Centrik doc3.pdf". The content of the document is a report on the implications of assassination attempts involving both foreign and domestic actors targeting former [redacted]. The paper discusses the [redacted].

147. According to PayPal records, on or about October 3, 2024, Recruit E received approximately two one-cent payments from two more seemingly unrelated accounts, one from

[redacted]@hotmail.com and another with the Title [redacted]" into his/her personal PayPal account. A review of these PayPal accounts indicated one was registered to a "[redacted]" with an address in California. The account was linked to two cards in the name [redacted], a debit card issued in the United States by the Bancorp Bank National Association and a credit card issued in Hong Kong by Citibank N.A. The other account was registered to an "[redacted]" with an address in Ireland. The account was registered with a debit card issued by a U.S. bank and a Single Euro Payments Area (SEPA) virtual IBAN, a digital identifier linked to a physical bank account, often used for the purpose of sending and receiving international payments. On or about that same day, Recruit E received approximately [redacted] in six separate payments from yet another seemingly unrelated account in the name of "[redacted]"; the account was linked to one financial account with the country of issuance as Ireland. On or about October 4, 2024, Recruit E received $[redacted] into his/her personal PayPal account from this same account with the Item Title "[redacted]." Given the facts described above, including the discussion about the "hiccup" with his/her PayPal payments, I believe these payments on October 3 and 4, 2024, were all related to Recruit D's work for CENTRIK.

SUBJECT A Recruits Former [redacted] with [redacted] and Receives Document with "Insider Information"

148. According to LinkedIn records, SUBJECT A was also in communication with Recruit F. According to Recruit F's LinkedIn profile, Recruit F was an [redacted] with the [redacted] from [redacted]. According to Recruit F's LinkedIn profile, Recruit F was self-employed as a "[redacted] from [redacted].

149. On or about September 3, 2024, SUBJECT A messaged Recruit F via LinkedIn that she/he was contacting him/her on behalf of CENTRIK and that CENTRIK was looking to hire a U.S. citizen who could obtain insights on key government/military issues from their contact

network. SUBJECT A noted that they were "not looking for secret information, only insight that our internal team cannot obtain."

150. On or about September 3, 2024, Recruit F asked SUBJECT A about signing a contract and where Recruit F should send a sample piece. The same day, SUBJECT A responded that there would be a contract and that Recruit F should email the paper to [SUBJECT A]@gmail.com. SUBJECT A then asked Recruit F about his/her geographic area of expertise.

151. On or about September 3, 2024, SUBJECT A asked Recruit F to write about "US government considerations in the Israel-Palestine conflict and the likely next steps." SUBJECT A asked Recruit F to focus the time frame on "the next few weeks to months (tactical considerations)" and noted that the "USG's likely plans are most important. Feel free to address political stability, security, arms sales factors, and any other important factors you deem worthy of mentioning, but the key is very specific information that is of a granular nature."

152. On or about September 6, 2024, Recruit F messaged SUBJECT A that she/he had sent SUBJECT A the sample report. According to Google records, on or about September 6, 2024, Recruit F sent [SUBJECT A]@gmail.com an email. On or about September 6, 2024, using LinkedIn, SUBJECT A told Recruit F the report did not meet the length requirements.

153. On or about September 10, 2024, Recruit F told SUBJECT A that she/he had sent SUBJECT A an updated writing sample. On or about September 12, 2024, SUBJECT A told Recruit F she/he was working on getting an answer for Recruit F from his/her "team." SUBJECT A asked Recruit F for his/her PayPal information to compensate Recruit F for the report and the "company has decided on $500." Recruit F provided an email address and phone number.

154. On or about September 17, 2024, SUBJECT A messaged Recruit F that she/he should have received payment. Recruit F told SUBJECT A she/he hadn't received payment. Later

that same day, after Recruit F asked SUBJECT A for the next report topic, SUBJECT A told Recruit F that the "lead analyst has asked if [Recruit F] wouldn't mind creating a Telegram account where all the analytic topics are shared." SUBJECT A told Recruit F the lead analyst would "discuss the next report topic" on Telegram. Recruit F then messaged SUBJECT A with what appears to be Recruit F's Telegram account username. Also on or about September 17, 2024, Recruit F asked SUBJECT A for the analyst's name and SUBJECT A told Recruit F the analyst's name was "[redacted] (likely referring to [redacted], discussed above).

155. On or about September 18, 2024, SUBJECT A sent Recruit F a document titled "Consultancy Contract" for an International Affairs Consultant position effective June 1, 2024. The contract included a payment rate of $1,000 per report and included a referral fee of $700 per individual Recruit F would refer to CENTRIK. The contract included a confidentiality agreement and a governing law section that stated the contract will be "governed by the employment laws of Singapore."

156. On or about September 30, 2024, Recruit F sent SUBJECT A the following message: "[SUBJECT A's first name], attached is the signed contract." The document Recruit F sent is a signed CENTRIK contract for the International Affairs Consultant position effective October 1, 2024, and signed by Recruit F with what appears to be a signature on the last page with "September 30, 2024" written on it. (The signed contract does not appear to include all the sections of the original contract SUBJECT A had emailed Recruit F.)

157. According to PayPal records, as of October 5, 2024, a PayPal account registered to Recruit F received $[redacted] on October 5, 2024, from [redacted], [redacted]@outlook.com and withdrew the payment to a [redacted] account tied to his/her PayPal account. Based on the discussion between SUBJECT A and Recruit F

discussed above, I believe this payment was for Recruit F's work on behalf of CENTRIK. As noted above, this PayPal account also paid Recruit D. A review of this PayPal account showed an address in Great Britain. It was linked to five different China-issued debit or credit cards in the name [redacted], the same cards that were linked to a PayPal account in the name [redacted] used to pay Recruit E.

158. On or about October 9, 2024, using LinkedIn, Recruit F asked SUBJECT A to set up a meeting between "[redacted] and myself." SUBJECT A did not respond. On or about October 19, 2024, Recruit F sent SUBJECT A the following message: "Hey [SUBJECT A's first name], here is the report I spoke to [redacted] about writing." Recruit F sent SUBJECT A a Microsoft word document regarding [redacted] involvement in the [redacted] conflict and the potential impact of a [redacted] on the war in [redacted] Based on information disclosed from an interview of Recruit C (discussed above), I believe Recruit F was referring to someone using the name "[redacted]."

159. On or about October 22, 2024, Recruit F asked SUBJECT A to set up a meeting between him/her, SUBJECT A, and "[redacted] Recruit F then sent SUBJECT A a new version of the report.

160. The new version of the report is the same report Recruit F sent SUBJECT A on October 19, 2024, regarding [redacted] involvement in the [redacted] conflict and the potential impact of [redacted] on the war in [redacted] However, this time the document included comments from an identified person that stated "Yellow=Open Source" and "Green= Insider Information." The document includes eight words highlighted in green and six words highlighted in yellow. This marking suggests that the text following the highlighted words is either open source or "insider information."

161. According to PayPal records, Recruit F received the following additional payments: [redacted] on October 29, 2024, from [redacted]@outlook.com, and $[redacted] on December 24, 2024, from an "[redacted]" using a United Kingdom email address. On the same day Recruit F received these payments, Recruit F withdrew each payment to a [redacted] account tied to his/her PayPal account. A review of PayPal account information indicated the account registered to [redacted] used email address [redacted]@koonka.uk and listed an address in Great Britain. It was linked to eight different China-issued debit or credit cards with seven Chinese banks.

162. Based on the information above and outlined elsewhere in this affidavit and based on my training and experience, I believe Recruit F was paid [redacted] for a report she/he sent SUBJECT A via email and [redacted] and $[redacted] for reports she/he sent "[redacted] via Telegram. As discussed above, I believe Recruit F was referring to someone using the name "[redacted]."

SUBJECT A Recruits Clearance Holders and Hands off Communications to "[redacted]" of CENTRIK

163. In or around September 2024, SUBJECT A recruited Recruit F, a former U.S. government employee and current clearance holder, through LinkedIn. According to U.S. government records, Recruit F has a Secret clearance. According to his/her LinkedIn profile, as of [redacted], Recruit F works as a [redacted] with a Defense Contractor, where she/he has worked since [redacted]. According to [redacted] records, Recruit F was [redacted].

164. In or around September 2024, SUBJECT A recruited a purported former U.S. government employee and current clearance holder, Recruit G, through LinkedIn. According to U.S. government records, Recruit G has a Top Secret with SCI clearance. According to his/her LinkedIn profile, as of in or around [redacted] since [redacted] Recruit G has been the [redacted]

[redacted] at an identified U.S. Defense Contractor. According to a LinkedIn profile, prior to joining the Defense Contractor, Recruit G was a [redacted] with [redacted] from [redacted].

165. The messages below were exchanged between SUBJECT A and Recruit G via LinkedIn.

166. On or about September 12, 2024, SUBJECT A messaged Recruit G thanking him/her for his/her application to CENTRIK. That same day, SUBJECT A asked Recruit G for his/her area of expertise in the geopolitical realm to move forward with a trial report. SUBJECT A also told Recruit G that CENTRIK does not provide any documentation for the revenue service. On or about September 13, 2024, Recruit G told SUBJECT A his/her area of expertise is in [redacted], and that she/he has experience with [redacted]."

167. On or about September 17, 2024, SUBJECT A messaged Recruit G that she/he would be handing Recruit G off to CENTRIK's "Lead Analyst, [redacted]." SUBJECT A requested Recruit G send SUBJECT A his/her Telegram handle and then [redacted] would contact him/her. That same day, Recruit G provided what appears to be his/her Telegram username to SUBJECT A.

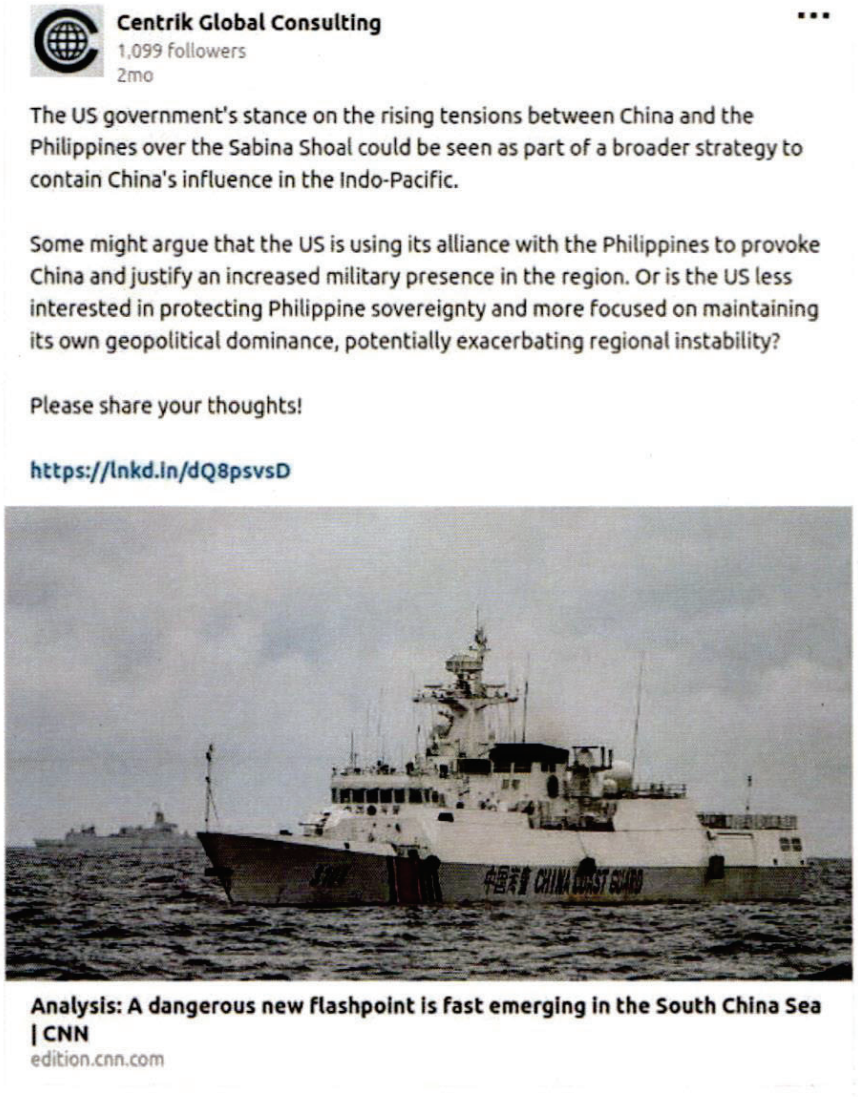
I. <u>Evidence That the TARGET DOMAIN NAMES Conduct Targeting on behalf of the PRC</u>

168. Based on the facts discussed above, the FBI believes that the conspirators have used the **TARGET DOMAIN NAMES** to identify and target persons with access to classified and/or sensitive U.S. government information who can be persuaded to gather and/or provide that information to the conspirators through their front companies. Despite SUBJECT A's claim to individuals on LinkedIn that CENTRIK works with large corporations and does not work with

foreign governments, I believe that a foreign government or foreign government official may well be directing the **TARGET DOMAIN NAMES**, as shown below.

169. According to open-source research conducted in approximately October, 2024, CENTRIK's LinkedIn page contained multiple posts on current foreign policy issues, including posts on matters related to the ongoing Russia-Ukraine conflict, the Israel-Palestine war, and matters related to the United States and China.[24] As of October 2024, the majority of CENTRIK's job postings were on issues concerning the United States and China, such as in or around August 2024, CENTRIK posted a link to a CNN article titled "Analysis: A dangerous new flashpoint is fast emerging in the South China Sea" with the following comment in the post:

[24] As of March 2025, CENTRIK's LinkedIn page appeared to be no longer active on LinkedIn.



170. In or around September 2024, CENTRIK posted a CNN article with "China kicks off major African summit as it seeks to woo leaders amid pressure from the West" with the following comment:

Centrik Global Consulting
1,099 followers
1mo

China's expanding engagement with African countries, highlighted at the recent China-Africa Summit in Beijing, is increasingly shaping the geopolitical landscape. By positioning itself as Africa's key partner through substantial investments and infrastructure projects, China is offering immediate economic benefits that appeal to many African nations. However, this growing relationship also underscores a subtle friction between African states and the United States.

Many African leaders are navigating a complex diplomatic environment, balancing the immediate gains from Chinese partnerships with concerns over long-term dependency and the impact on sovereignty. Meanwhile, some African nations have expressed frustration with U.S. policies, which they view as more focused on governance and human rights than on immediate economic needs. As Africa becomes a battleground for influence between major global powers, the choices made today will have lasting implications for the continent's development and international alliances.

#ChinaAfrica #USAfricaRelations #Geopolitics #EconomicDevelopment #Diplomacy #GlobalInfluence

https://lnkd.in/dDieiu5u

China kicks off major African summit as it seeks to woo leaders amid pressure from the West | CNN
edition.cnn.com

171. SUBJECT A frequently has asked recruits and potential recruits to report on issues of particular interest to the PRC. For example, on or about August 28, 2024, SUBJECT A messaged an individual (Recruit H) write a test report on the "U.S. internal views" and what the U.S. will do next regarding the UN OHCHR's urging China to review Xinjiang policies related to human rights violations. According to ohchr.org/en/about-us, UNOHCHR stands for the United Nations Office of the High Commissioner for Human Rights. According to this website, on or about August 27, 2024, the Office of the High Commissioner for Human Rights issued a public statement titled "China: Update on the work of the UN Human Rights Office." The statement included mention of a June 2024 UN Human Rights team visit to China, which included dialogue on Xinjiang. The statement said that "problematic laws and policies remain in place" and the UN had called upon authorities for a full review, including into torture and other allegations of human rights violations. Multiple news outlets have covered the Chinese government's treatment of Uyghurs, "a predominately Muslim Turkic-speaking ethnic group,"[25] in Xinjiang, including details of surveillance, reeducation camps, detainment, forced labor, and forced sterilization. China's treatment of groups in the Xinjiang Uyghur Autonomous Region has been a sticking point in United States and China relations. Enacted in December 2021 and effective beginning in June 2022, the U.S. Congress passed a bill, the "Uyghur Forced Labor Prevention Act," which prevents goods made with forced labor in Xinjiang from entering the United States.[26] Additional examples are described in the two paragraphs below.

---

[25] https://www.cfr.org/backgrounder/china-xinjiang-uyghurs-muslims-repression-genocide-human-rights (last accessed on April 9, 2026)

[26] https://www.state.gov/office-to-monitor-and-combat-trafficking-in-persons/releases/2025/01/uyghur-forced-labor-prevention-act-uflpa-fact-sheet (last accessed on April 9, 2026)

172. On or about October 5, 2024, SUBJECT A asked an individual (Recruit I), who in the past held a security clearance with the [redacted] according to government records, to write about "the South China Sea issue" and the U.S. government's views and likely next steps. According to Britannica.com/place/South-China-Sea, the "South China Sea" is a part of the Pacific Ocean that is bordered on the east by Taiwan and the Philippines, "on the southeast and south by Borneo, the southern limit of the Gulf of Thailand, and the east coast of the Malay Peninsula." "The South China Sea and the East China Sea together form the China Sea." According to multiple open-source news articles and publications, the South China Sea is the major focus of ongoing territorial disputes involving China for many years.

173. On or about October 28, 2024, SUBJECT A messaged an individual (Recruit J), who had past employment at [redacted] listed on their LinkedIn profile, on behalf of CENTRIK requesting the individual write the following trial report:

> For the trial report we would like you to focus on the following report:Â https://www.rfa.org/english/uyghur/2024/10/26/uyghur-wuc-election-10262024/ Please investigate the election and the next steps for the group. Please limit your use of open source information and consult sources in your network for exclusive insights.

174. On or about November 14, 2024, SUBJECT A asked another individual (Recruit K) to "list the next steps in the Trump Administration China policy considerations."

175. Similarly, job posts made by the other **TARGET DOMAIN NAMES** targeted information centered around topics related to geopolitics that would be of interest to the Chinese government. A **TARGET DOMAIN NAME 2** job post viewed by the FBI in September 2023 advertised for an advisor who would research the Indo-Pacific region, including Singapore, China, Japan, Taiwan, and Vietnam, to "understand hot issues such as possible political changes, military conflicts, and trade policy changes in the region."

176. A **TARGET DOMAIN NAME 3** job post viewed by the FBI in October 2025 for job title "International Affairs Analyst (Latin America)" called for the tracking and analysis of "political developments, economic trends, and social issues across Latin America, including the impact of US-Latin America relations, China's growing influence, and region integration efforts."

177. A **TARGET DOMAIN NAME 6** job post viewed by the FBI in July 2024 indicated the job responsibilities would include "research on global development, focusing on the trends and dynamics in the international affairs, especially the event in Indo-Pacific region."

178. A **TARGET DOMAIN NAME 8** job post viewed by the FBI in May 2025 advertised an image of a U.S. Army officer and mentioned researching defense topics and military budgets. A screenshot is below.

179. A **TARGET DOMAIN NAME 10** job post viewed by the FBI in May 2025 for an "Economic Security Analyst," listed in its job responsibilities to "[m]onitor and interpret financial,

economic, and trade policies from key jurisdictions (e.g., U.S., EU, China, emerging markets)" and "[e]valuate how geopolitical shifts, tariffs, sanctions, or fiscal reforms impact client operations, supply chains, and market access." This job stated priority would be given to "candidates with experience in government agencies (e.g. The Treasury, FED, USTR and counterparts in other countries) or roles directly interfacing with policymakers." Of note, in early April 2025, the U.S. government raised tariffs on China.[27]

180. Similarly, a **TARGET DOMAIN NAME 12** job post from approximately April 11, 2025, contained in the list of responsibilities to "[i]nvestigate and report on evolving U.S. trade policies, including historical impacts of the Trump-era strategies and current developments" and to "[a]nalyze geopoligical and economic factors influencing international trade negotiations, sanctions, and bilateral agreements." Again, this job was posted in the midst of trade negotiations between the United States and China after the U.S. government raised tariffs on China in April 2025.[28]

181. Based on the information in this affidavit, the conspirators operating the **TARGET DOMAIN NAMES** have taken steps to obfuscate the true nature of their companies and the true operators of its accounts, including using accounts or operating accounts in the names of actual U.S. persons and using vague or coded language when referring to nonpublic or classified information. As detailed above, there are numerous instances of IP hits resolving to China and/or Macau, which, based on my training and experience, is consistent with PRC tradecraft by which PRC officials tend to mask their identities by using purported western company names/identities

---

[27] https://www.congress.gov/crs-product/R48549 (last accessed on April 12, 2026)

[28] https://www.whitehouse.gov/presidential-actions/2025/11/modifying-reciprocal-tariff-rates-consistent-with-the-economic-and-trade-arrangement-between-the-united-states-and-the-peoples-republic-of-china/ (last accessed on April 12, 2026)

while the IP hits show the true location.

TARGET DOMAIN NAMES' Involvement in Money Laundering

182. As shown above, the **TARGET DOMAIN NAMES** are fake consulting websites set up to attract and support recruits and served as key facilitating property for the bribery, theft of government property, identity theft, and money laundering conspiracies: Conspirators believed to be located overseas, including in China, Hong Kong, Macau, South Africa, and the United Kingdom, paid for many of these domain names through international money payments and used the domains to induce and attempt to induce U.S. persons, including current and former U.S. government officials with access to classified and/or sensitive U.S. government information, to send such information, in exchange for payments from accounts located overseas, to promote bribery, theft of government property, identity theft, and money laundering conspiracy schemes. In other words, the **TARGET DOMAIN NAMES** facilitated the transfer of funds from a place in the United States to a place outside the United States with the intent to promote a specified unlawful activity, in violation of 18 U.S.C. §§ 1956(a)(2)(A), (h).

SEIZURE PROCEDURE

183. The top-level domain for the **TARGET DOMAIN NAMES 1-8 and 10-12** is ".com." VeriSign, Inc. (Verisign), headquartered at 12061 Bluemont Way, Reston, Virginia, manages all ".com" domains.

184. The top-level domain for the **TARGET DOMAIN NAMES 9 and 13** is ".org." Public Interest Registry (PIR), headquartered at 1191 Freedom Drive, Reston, Virginia, manages all ".org" domains.

185. As detailed in Attachment A-1 and A-2, upon execution of the seizure warrant, the registry for the ".com" top-level domain, Verisign, and the registry for the ".org" top-level domain,

PIR, shall be directed to restrain and lock the **TARGET DOMAIN NAMES** pending transfer of all right, title, and interest in the **TARGET DOMAIN NAMES** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **TARGET DOMAIN NAMES** cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or the Department of Justice.

186. In addition, upon seizure of the **TARGET DOMAIN NAMES** by the FBI, Verisign and PIR will be directed to associate the **TARGET DOMAIN NAMES** to a new authoritative name server(s) to be designated by a law enforcement agent. The government will display a notice on the website to which the **TARGET DOMAIN NAMES** will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

CONCLUSION

187. The **TARGET DOMAIN NAMES**, centrikglobalconsulting.com, rightinfoconsult.com, finnaclevesperconsulting.com, cydfconsulting.com, pulsewaveglobal.com, catalystglobalsolutions.com, thehorizzen.com, geoindopacific.com, gpf-ina.org, safesec-group.com, thetruthinfo.com, vandercons.com, and gulfpeace.org each was used by subjects believed to be located outside the United States as a facility in a conspiracy in which the conspirators used stolen identities to recruit current and former U.S. officials for fake consulting jobs on behalf of the Chinese government with the promise of money in exchange for violating their lawful duties. Each of the **TARGET DOMAIN NAMES** also was involved in a conspiracy to commit international promotional money laundering. Accordingly, there is probable cause to believe that violations of 18 U.S.C. §§ 201 (Bribery of public officials and witnesses), 641 (Public money, property or records), 1028 (Fraud and related activity in connection with identification documents, authentication features, and information), and 1956 (Laundering of monetary

instruments) have been committed by known and unknown individuals. There is also probable cause to seize the **TARGET DOMAIN NAMES** described in Attachments A-1 and A-2 as property subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A), 982(a)(1), and 21 U.S.C. § 853.

188. Based on the foregoing, I submit that the **TARGET DOMAIN NAMES** are subject to seizure and forfeiture, pursuant to the above referenced statutes, and I request that the Court issue the proposed seizure warrant.

189. Because the warrant will be served on the registry that controls the **TARGET DOMAIN NAMES**, and the registry at a time convenient to them, will transfer control of the **TARGET DOMAIN NAMES** to the government, there exists reasonable cause to permit the execution of the requested warrant at any time of day or night.

Respectfully submitted,

[redacted]
Special Agent
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on June 5, 2026

G. MICHAEL HARVEY
UNITED STATES MAGISTRATE JUDGE