SEALED

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Holding a Criminal Term
Grand Jury Sworn in on July 9, 2018

		Case No. 1:19-cr-43
UNITED STATES OF AMERICA	:	Assigned To: Chief Judge Beryl A. Howell
	:	Date: 02/08/2019
	:	Description: INDICTMENT (B)
	:	
	:	18 U.S.C. § 794(c) (Conspiracy to Deliver
	:	National Defense Information to
v.	:	Representatives of a Foreign Government)
	:	(Count One)
	:	
	:	18 U.S.C. § 794(a) (Delivering National
	:	Defense Information to Representatives
MONICA ELFRIEDE WITT,	:	of a Foreign Government)
also known as "Fatemah Zahra,"	:	(Counts Two & Three)
also known as "Narges WITT,"	:	
	:	18 U.S.C. §§ 371, 1030 (Conspiracy to
MOJTABA MASOUMPOUR,	:	Commit Computer Intrusion)
	:	(Count Four)
BEHZAD MESRI,	:	
	:	18 U.S.C. § 1030 (Computer Intrusion)
HOSSEIN PARVAR, and	:	(Counts Five & Six)
	:	
MOHAMAD PARYAR,	:	18 U.S.C. § 1028A (Aggravated Identity
	:	Theft) (Count Seven)
	:	
Defendants.	:	18 U.S.C. § 2 (Aiding and Abetting)

INDICTMENT

The grand jury charges that:

GENERAL ALLEGATIONS

1. At all times relevant to this Indictment, the Islamic Republic of Iran ("Iran") was a hostile foreign power with which the United States had no formal diplomatic relations. The U.S. Secretary of State had designated the Government of Iran a state sponsor of terrorism each year

since 1984, based upon Iran's repeated and direct support for acts of international terrorism, including acts targeting U.S. and allied forces.

2. On March 15, 1995, the President issued Executive Order No. 12957, finding that "the actions and policies of the Government of Iran constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States" and declaring "a national emergency to deal with that threat." Executive Order No. 12957, as expanded and continued by Executive Orders Nos. 12959 and 13059, was in effect at all times relevant to this Indictment.

3. On September 23, 2001, the President issued Executive Order No. 13224, finding that "grave acts of terrorism and threats of terrorism committed by foreign terrorists . . . constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States," and declaring a "national emergency to deal with that threat."

4. On October 25, 2007, the U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), designated the Islamic Revolutionary Guard Corps (IRGC)–Qods Force (IRGC-QF) under the Global Terrorism Sanctions Regulations (GTSR). The IRGC is a branch of Iran's armed forces founded after the 1979 Revolution in April 1979 by order of the Ayatollah Khomeini.

5. The IRGC-QF was responsible for, among other things, conducting unconventional warfare and intelligence activities outside Iran, including assassinations and cyber-related attacks. The IRGC-QF was designated by OFAC because it had provided material support to the Taliban, Lebanese Hizballah, Hamas, Palestinian Islamic Jihad, and the Popular Front for the Liberation of Palestine-General Command. In its public designation, OFAC specifically found that the IRGC-QF was the Iranian regime's primary instrument for providing lethal support to the Taliban and

selecting Iraqi Shi'a militants to target and kill members of the U.S. military as well as innocent civilians in Iraq and Afghanistan.

6. On October 13, 2017, OFAC designated the IRGC for its activities in support of the IRGC-QF. The IRGC, which is the parent organization of IRGC-QF, undertakes to assist in, sponsor, and provide financial, material, and technological support for the IRGC-QF. The IRGC also provides support to a number of terrorist groups, including Hizballah and Hamas, as well as the Taliban.

7. The U.S. Air Force Office of Special Investigation (AFOSI) conducted counterintelligence investigations and operations both domestically and overseas in coordination with the larger U.S. intelligence community (USIC). AFOSI defined "counterintelligence" as information gathered, and activities conducted, to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.

8. Executive Order 13526 and its predecessor orders establish that information in any form that (1) is owned by, produced by or for, or under the control of the United States government, and (2) falls within any of the categories set forth in the order, to include intelligence sources or methods; cryptology; military plans; vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security; and foreign relations or foreign activities of the United States, including confidential sources, may be classified by an original classification authority whenever the unauthorized disclosure of the information could be expected to result in damage to the national security of the United States. Where such damage would be "serious," the

information may be classified as SECRET. Where such damage would be "exceptionally grave," the information may be classified as TOP SECRET.

9. Access to classified information at any level may be further restricted through compartmentation in SENSITIVE COMPARTMENTED INFORMATION (SCI) categories or through the implementation of a Special Access Program (SAP).

Definitions

10. A "defector" is a person who has abandoned his or her country or cause in favor of an opposing one.

11. A "spotter and assessor" works on behalf of a country's intelligence service, identifying persons who may have access to the intelligence and counterintelligence services of an opposing country and determining the potential value of such persons as sources.

12. "Bona fides," as used in the context of intelligence activity, are evidence of a potential spy's good faith or genuineness. The term may also refer to that individual's qualifications or achievements.

13. As defined by AFOSI, the term "target package" is a document, or set of documents, assembled to enable an intelligence or military unit to find, fix, track, and neutralize a threat. A human target package includes information collected about an individual, such as the official position of the individual, an analysis of personal vulnerabilities or other opportunities to exploit the individual, and confirmation of the identity and location of the individual. Finally, a target package recommends a neutralization plan, which may include apprehension, recruitment, cyber exploitation, or capture/kill operations.

14. "Human intelligence" (HUMINT) is defined as intelligence information gathered from human sources. Intelligence assets and counterintelligence officers have lost their lives collecting HUMINT.

15. "Malware" is malicious computer software intended to cause the victim computer to behave in a manner inconsistent with the intention of the owner or user of the victim computer, usually unbeknownst to that person, including capturing a target's keystrokes, accessing a computer's web camera, and monitoring other computer activity.

16. "Spearphishing" messages are typically designed to resemble emails from trustworthy senders, and to encourage the recipient to open attached files or click on hyperlinks in the messages. Some spearphishing emails attach or link to files that, once opened or downloaded, install "malware"—malicious code or programs—that provide unauthorized access to the recipient's computer. Other spearphishing emails lure the recipient into providing valid login credentials to his or her account(s), thereby allowing the senders to bypass normal authentication procedures.

The Defendants and Other Key Individuals

Monica Witt

17. At all times relevant to this Indictment, Defendant **MONICA ELFRIEDE WITT**, also known as Fatemah Zahra, also known as Narges Witt (hereinafter referred to as **WITT**), a United States citizen, was a former active duty U.S. Air Force Intelligence Specialist and Special Agent of the AFOSI, who entered on duty in or around August 1997 and served continuously until in or around March 2008.

18. On entering active duty and again upon assuming the role of Special Agent, **WITT** swore the following oath: "I will support and defend the constitution of the United States against

all enemies foreign and domestic; that I will bear true faith and allegiance to the same; that I take this oath freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter, So help me God."

19. **WITT** was granted access to SECRET and TOP SECRET national defense information relating to the foreign intelligence and counterintelligence of the United States, including HUMINT containing the true names of intelligence sources and clandestine agents of the USIC.

20. From in or around February 1998 to in or around April 1999, **WITT** was assigned to the U.S. Defense Language Institute in Monterey, California, where she undertook training in Persian Farsi.

21. From in or around May 1999 to in or around November 2003, **WITT** deployed to several overseas locations in order to conduct classified missions collecting signals intelligence, or SIGINT, involving adversaries of the United States.

22. From in or around November 2003 to in or around March 2008, **WITT** was assigned as an AFOSI Special Agent criminal investigator and counterintelligence officer.

23. As an AFOSI counterintelligence officer, **WITT** was deployed to locations in the Middle East to conduct classified operations.

24. As an AFOSI Special Agent, **WITT** was granted access to a SAP that housed classified information, including details of ongoing counterintelligence operations, true names of sources, and the identities of U.S. agents involved in the recruitment of those sources.

25. This SAP was known within the USIC by a code name. The code name allowed agents to communicate in the open without disclosing the true nature of their operations. At all

times relevant to this Indictment, the SAP was known by two successive code names, which are referred to in this Indictment as "PROJECT A" and "PROJECT B."

26. From in or around March 2008 until in or around August 2010, **WITT** was employed as a U.S. government contractor, during which she acted as the AFOSI Desk Officer for PROJECT A/PROJECT B.

27. **WITT** held a TOP SECRET/SCI security clearance continuously from the time she joined the U.S Air Force in 1997 until she terminated her employment as a contractor with the USIC in or around August 2010. **WITT** passed all appropriate security evaluations, including background investigations at regular intervals and other protocols designed to detect whether she posed a risk to the national security. As a result, **WITT** was granted access to a variety of programs classified at the SECRET and TOP SECRET levels. Specifically:

a. On or about November 29, 1999, **WITT** signed a "Classified Information Nondisclosure Agreement" in which she acknowledged that:

> Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. . . . I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.
>
> I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation.
>
> I have been advised than any unauthorized disclosure of classified information by me may constitute a violation, or violations of United States criminal laws, including the provisions of Section 794[,] Title 18, United States Code, and provisions of the Intelligence Identities Protection Act of 1982.

b. On at least twelve other occasions during her work on behalf of the United States, **WITT** signed various iterations of classified information nondisclosure agreements. In these agreements, she acknowledged that she had received security briefings and understood that disclosure of the classified information she acquired could place human life in jeopardy. She also pledged that she would "never divulge such information, in any form or any manner, to anyone who is not authorized to receive it, without prior written authorization from an appropriate official of the United States Government."

c. In or around October 2004, **WITT** signed and attested to a "Sensitive Compartmented Information Nondisclosure Agreement" for a compartment designated "HCS." HCS stands for HUMINT control system, and denotes, among other things, classified information that included the identities and locations of human beings who are clandestinely assisting the United States and its allies against a hostile foreign threat.

d. In or around November 2008, **WITT** again pledged secrecy to the United States by signing a "Special Access Program Indoctrination Agreement," which allowed **WITT** to be granted access to the TOP SECRET, or highest, level of the PROJECT A/PROJECT B SAP. Information protected under the SAP may be classified at the SECRET or TOP SECRET level depending on the severity of damage to the United States that could be expected to accrue if the information is divulged.

Individual A

28. At all times relevant to this Indictment, Individual A, a dual United States-Iranian citizen, whose identity is known to the grand jury, resided primarily in Iran. As described below,

Individual A engaged in acts consistent with serving as a spotter and assessor on behalf of the Iranian intelligence services.

Iranian Cyber Conspirators

29. At all times relevant to this Indictment, Defendants **MOJTABA MASOUMPOUR, BEHZAD MESRI, HOSSEIN PARVAR,** and **MOHAMAD PARYAR,** and other individuals whose identities are known and unknown to the grand jury (hereinafter referred to collectively as the "Cyber Conspirators"), were nationals of Iran, lived and worked in Iran, and were leaders, employees, and contactors of, or otherwise associated with, a corporate entity in Tehran, Iran (hereinafter referred to as the "Iranian entity"), the identity of which is known to the United States and which conducted malicious computer intrusions on behalf of the IRGC.

U.S. Government Agents 1 through 8

30. U.S. government employees (hereinafter referred to as "USG Agents") 1 through 8 are current or former Special Agents, counterintelligence analysts and other USIC employees who were co-workers or colleagues of **WITT**, as described herein.

31. USG Agents 1 and 2 worked with **WITT** in **WITT**'s position relating to PROJECT A/PROJECT B.

32. USG Agents 3 and 5 worked with **WITT** during **WITT**'s tenure with the U.S. government in the United States.

33. USG Agents 4 and 6 worked with **WITT** during **WITT**'s deployment in the Middle East.

34. USG Agent 7 served in a leadership role during **WITT**'s tenure with the U.S. government.

35. USG Agent 8 attended training with **WITT** and interacted with **WITT**.

Jurisdiction and Venue

36. Acts referred to in each count of the Indictment were begun and committed in Iran and elsewhere outside the jurisdiction of any particular State or district but within the extraterritorial jurisdiction of the United States. Pursuant to Title 18, United States Code, Section 3239, Counts One through Three are within the venue of the United States District Court for the District of Columbia and, pursuant to Title 18, United States Code, Section 3238, Counts Four through Seven are within the venue of the United States District Court for the District of Columbia.

COUNT ONE
(Conspiracy to Deliver National Defense Information to Representatives of a Foreign Government)

37. The grand jury realleges and incorporates by reference the General Allegations set forth in this Indictment.

38. From in or around January 2012 to in or around May 2015, in Iran, and elsewhere outside the jurisdiction of any particular State or district, defendant **MONICA ELFRIEDE WITT** did knowingly and unlawfully combine, confederate, and agree with other persons, both known and unknown to the grand jury, including officers of the IRGC, to knowingly and unlawfully communicate, deliver, and transmit to a foreign government, specifically Iran, and to that foreign government's representatives, officers, and agents, directly and indirectly, documents and information relating to the national defense of the United States, with the intent and reason to believe that the same would be used to the injury of the United States and to the advantage of Iran, in violation of Title 18, United States Code, Section 794(a).

Ways, Manner, and Means of the Espionage Conspiracy

39. It was a part of the conspiracy that **WITT** did through her position as a Special Agent with the AFOSI gain access to classified information relating to the national defense.

40. It was further part of the conspiracy that **WITT** did travel to Iran, where she publicly identified herself as a U.S. military veteran.

41. It was further part of the conspiracy that **WITT** did travel to Iran, where she met with representatives of the IRGC and identified herself as a veteran of the U.S. military who desired to defect to Iran.

42. It was further part of the conspiracy that **WITT** did make efforts to provide her bona fides to representatives of the IRGC in order to establish her ability and willingness to disclose U.S. national defense information to the Government of Iran.

43. It was further part of the conspiracy that **WITT** did conduct research for the purpose of creating target packages against U.S. counterintelligence agents, and did create such packages in order to enable the Government of Iran to target U.S. counterintelligence agents.

44. It was further part of the conspiracy that **WITT** did disclose information relating to the national defense of the United States to Iranian government officials.

Overt Acts

45. In furtherance of the conspiracy and to effect the object thereof, **WITT** and other unindicted co-conspirators, whose identities are known and unknown to the grand jury, did commit the following overt acts:

a. In or around February 2012, **WITT** traveled to Iran for the purpose of attending the New Horizon Organization's "Hollywoodism" conference, an IRGC-sponsored event aimed at condemning American moral standards and promoting anti-U.S. propaganda.

b. In or around February 2012, **WITT** appeared in one or more videos in which she was identified as a U.S. veteran and made statements that were critical of the U.S. government, knowing these videos would be broadcast by Iranian media outlets.

c. In or around February 2012, co-conspirators did cause to be broadcast on Iranian television a ceremony during which **WITT** converted to Islam.

d. On or about May 25, 2012, **WITT** was warned by Federal Bureau of Investigation (FBI) Special Agents that she was a target for recruitment by Iranian

intelligence services. In response, **WITT** stated that if she ever returned to Iran she would refuse to provide any information pertaining to her work with AFOSI.

e. In or around June 2012, Individual A traveled to the United States and hired **WITT** to work as her assistant in connection with the filming of an anti-American propaganda film that was later aired in Iran.

f. In or around February 2013, **WITT** again traveled to Iran to attend another "Hollywoodism" conference.

g. In or around February 2013, **WITT** met with members of the IRGC and identified herself as a U.S. veteran who was critical of the U.S. military and who desired to emigrate to Iran.

h. In or around February 2013, while in Iran, **WITT** appeared in one or more videos in which she was identified as a U.S. veteran and made statements that were critical of the U.S. government, knowing these videos would be broadcast by Iranian media outlets.

i. Between in or around July 2012 and in or around August 2013, **WITT** communicated regularly with Individual A.

j. On or about October 17, 2012, Individual A wrote to **WITT**, "should i thank the sec of defense . . u were well trained." In response, **WITT** wrote, "LOL thank the sec of defense? For me? Well, I loved the work, and I am endeavoring to put the training I received to good use instead of evil. ☺ Thanks for giving me the opportunity."

k. On or about June 23, 2013, **WITT** wrote to Individual A, stating, "If all else fails, I just may go public with a program and do like Snowden :)"

l. On or about June 30, 2013, **WITT** wrote to Individual A that she had gone to the Iranian embassy in Kabul, Afghanistan, and "told all." **WITT** continued, "They are

going to get back to me on if they can help me very soon before I leave. I told them I am down to little choices and will be traveling to other areas to request assistance."

m. On or about July 1, 2013, Individual A wrote to **WITT**, "I was talking to people until about 2 in the morning about your case. I have several different channels working on it, but to be honest with one of them, he said they got suspicious that on one hand, you said u had no money and on the other hand u r going from country to country." That same day, **WITT** replied, ":(Grrr.....No matter what, they are just going to be suspicious, right? . . . I just hope I have better luck with Russia at this point. I am starting to get frustrated at the level of Iranian suspicion."

n. On or about July 3, 2013, **WITT** wrote Individual A, "I think I can slip into Russia quietly if they help me and then I can contact wikileaks from there without disclosing my location."

o. On or about July 30, 2013, Individual A wrote, "MONICA ARE YOU THERE????. . .The name of the [Iranian] ambassador is Mr. Shehr Doost. His mobile is 009929 196[xxxxx]. Right now he is not in Dushanbe, but you are to call him at 7pm and then go and see him. When you call him on the phone just say that you are the one who is suppose (sic) to see him today for a visa and that's it." In response, on or about July 31, 2013, **WITT** wrote to Individual A, "Okay. Quick update. They are giving me money to head to Dubai. I will wait to get the approval there and get it from the embassy in Dubai. They are so kind...even taking me to the airport."

p. On or about August 12, 2013, Individual A wrote to **WITT**, "Well I am looking into the Turkey situation . . . . This has been a difficult situation, one because of the timing, a change in governments here, and two because of your personal situation

(history)." **WITT** responded, "I am a little nervous, though, when it comes to Turkey as it is an extradition country. . . . If it weren't for my "history" I suppose I wouldn't require asylum[.]"

q. On or about August 25, 2013, **WITT** sent an email to Individual A containing **WITT**'s bona fides, entitled, "My Bio and Job History." Attached to the email was a typewritten narrative of **WITT**'s bona fides and "conversion narrative," as well as a chronological listing of her work history and a copy of her "Certificate of Release or Discharge From Active Duty," Form DD 214. Approximately nine minutes later, on August 25, 2013, Individual A forwarded the above-described email and its attachments, without comment, to an email address associated with Iran.

r. Between in or around July 2013 and on or about August 28, 2013, **WITT** conducted multiple searches on Facebook for the names of her former fellow counterintelligence agents, including USG Agent 1, and the spouse of USG Agent 3.

s. On or about August 28, 2013, **WITT** wrote to Individual A that she was about to board her flight from Dubai to Tehran, stating, "I'm signing off and heading out! Coming home ☺."

t. On or about August 28, 2013, **WITT** defected to Iran.

u. Beginning on or about August 28, 2013, Iranian government officials provided **WITT** with goods and services, including housing and computer equipment, in order to facilitate her work on behalf of the Government of Iran.

v. Beginning on or about August 28, 2013, **WITT** disclosed to Iranian government officials the code name and mission of a U.S. Department of Defense SAP, to

wit: the fact that PROJECT A/PROJECT B involved U.S. intelligence operations against a specific target, which information was classified SECRET.

w. Between in or around January 2014 and in or around May 2015, **WITT** conducted multiple Facebook searches for USG Agents using Facebook accounts registered to various fictitious individuals.

x. Between in or around January 2014 and in or around May 2015, **WITT** created target packages for use by Iran against USG Agents, including USIC counterintelligence officers.

y. Between in or around January 2014 and in or around May 2015, **WITT** disclosed the true name of USG Agent 1, and the fact that USG Agent 1 conducted counterintelligence activities against a specific target, which information was classified SECRET.

(**Conspiracy to Transmit National Defense Information to a Representative of a Foreign Government**, in violation of Title 18 United States Code Section 794(c))

COUNT TWO
(Delivering National Defense Information to Representatives of a Foreign Government)

46. The grand jury realleges and incorporates by reference the General Allegations set forth in this Indictment and paragraphs 38-45 of Count One.

47. Between in or around August 2013 and in or around December 2013, in Iran and elsewhere out of the jurisdiction of any particular State or district, defendant **MONICA ELFRIEDE WITT**, with the intent and reason to believe that it was to be used to the injury of the United States and to the advantage of a foreign government, specifically Iran, did knowingly and unlawfully communicate, deliver, and transmit, and attempt to communicate, deliver, and transmit to a foreign government, specifically Iran, and to representatives, officers, agents, and employees thereof, directly and indirectly, information relating to the national defense of the United States, specifically the codename and mission of a U.S. Department of Defense SAP, to wit: the fact that PROJECT A/PROJECT B involved U.S. intelligence operations against a specific target, which information was classified SECRET.

(**Communication or Transmission to Representatives, Officers and Employees of a Foreign Government, With Intent That it Be Used to the Injury of the United States or to the Advantage of a Foreign Nation, Information Relating to the National Defense**, in violation of Title 18, United States Code, Section 794(a))

COUNT THREE
(Delivering National Defense Information to Representatives of a Foreign Government)

48. The grand jury realleges and incorporates by reference the General Allegations set forth in this Indictment and paragraphs 38-45 of Count One.

49. Between in or around August 2013 and in or around May 2015, in Iran and elsewhere out of the jurisdiction of any State or district, defendant **MONICA ELFRIEDE WITT**, with the intent and reason to believe that it was to be used to the injury of the United States and to the advantage of a foreign government, specifically Iran, did knowingly and unlawfully communicate, deliver, and transmit, and attempt to communicate, deliver, and transmit to a foreign government, specifically Iran, and to representatives, officers, agents, and employees thereof, directly and indirectly, information relating to the national defense of the United States, specifically the true name of USG Agent 1, and the fact that USG Agent 1 conducted counterintelligence activities against a specific target, which information was classified SECRET.

(Communication or Transmission to Representatives, Officers and Employees of a Foreign Government, With Intent That it Be Used to the Injury of the United States or to the Advantage of a Foreign Nation, Information Relating to the National Defense, in violation of Title 18, United States Code, Section 794(a))

COUNT FOUR
(Conspiracy to Commit Computer Intrusions)

50. The grand jury realleges and incorporates by reference the General Allegations set forth in this Indictment.

51. Beginning in or around December 2014, and continuing until at least in or around May 2015, the Cyber Conspirators, that is, **MOJTABA MASOUMPOUR, BEHZAD MESRI, HOSSEIN PARVAR,** and **MOHAMAD PARYAR**, and other individuals whose identities are known and unknown to the grand jury, knowingly and intentionally conspired to commit computer intrusions targeting current and former USG Agents.

Ways, Manner, and Means of the Cyber Conspiracy

52. It was a part of the conspiracy that the Cyber Conspirators did obtain computer and online infrastructure, including virtual private servers, email accounts, and social media accounts, and used this infrastructure to communicate with each other, to contact targets, and to transmit spearphishing emails and malware.

53. It was further part of the conspiracy that the Cyber Conspirators did develop and obtain malware designed to capture a target's keystrokes, access a computer's web camera, and monitor other computer activity.

54. It was further part of the conspiracy that the Cyber Conspirators did use fictitious and imposter personas to deceive their targets in their communications, and the Cyber Conspirators did knowingly use, without lawful authority, the names of other true persons, including USG Agents and persons affiliated with them, to entice targets to engage with the Cyber Conspirators online.

55. It was further part of the conspiracy that, after engaging online with a target, the Cyber Conspirators would and did send links and attachments that, when accessed by current and

former U.S. counterintelligence agents, were designed to deploy malware and establish covert, persistent access to the recipient's computer and associated network.

Overt Acts

56. In furtherance of the conspiracy and to effect the object thereof, the Cyber Conspirators did commit the following overt acts:

a. On or about December 23, 2014, **MESRI** registered an Iranian entity, the identity of which is known to the United States and which, on behalf of the IRGC, conducted computer intrusions against targets inside and outside of the United States. **MESRI** was the chief executive officer of the Iranian entity, which operated in many ways like a typical business or organization, in that it disbursed regular salaries, established work hours, issued assignments, and employed supervisors and managers whose identities are known to the United States.

b. Beginning in or around December 2014, **MESRI** obtained computer infrastructure, including virtual private servers, for use in the conspiracy. **MESRI** obtained the infrastructure from an Iranian individual whose identity is known to the United States and who had previously provided computer infrastructure to the IRGC. The Cyber Conspirators used the infrastructure to test the conspiracy's malware and gather information from target computers or networks.

c. In or around December 2014, **PARYAR** entered into a contract with **PARVAR** and **MASOUMPOUR** for **PARYAR** to procure and provide technical support for malware used in the conspiracy.

The "Bella Wood" Persona

d. On or about January 5, 2015, the Cyber Conspirators created an email account, bella.wood87@yahoo.com, and an associated Facebook account in the name of "Bella Wood."

e. On or about January 5, 2015, the Cyber Conspirators, using the "Bella Wood" Facebook account, sent a Facebook friend request to USG Agent 2, who accepted the request. At the time, USG Agent 2 was deployed to Kabul, Afghanistan, as part of a U.S. Central Command (CENTCOM) Joint Intelligence Unit. While in Afghanistan, USG Agent 2 accessed Facebook through a U.S. Department of Defense server while using a U.S. government computer issued by CENTCOM. USG Agent 2 also accessed Facebook using personal devices that connected to the Internet via wireless networks controlled and hosted by the U.S. Department of Defense.

f. On or about January 9, 2015, the Cyber Conspirators, using the bella.wood87@yahoo.com account, sent an email to USG Agent 2 that stated: "Hello my dear . . . invitation card sent to you by email I got this pretty card accept me as a kind friend." This email contained a spoofed link that, on its face, purported to take a recipient to a "pretty card." Had USG Agent 2 clicked the "pretty card" link, USG Agent 2's computer would have been directed not to a greeting card, but to a server controlled by the Cyber Conspirators. The Cyber Conspirators sent the "pretty card" email to USG Agent 2 utilizing covert tracking software, so that when USG Agent 2 opened the email, the tracking software allowed the Cyber Conspirators to confirm that USG Agent 2 had opened the email via a U.S. Department of Defense computer network located in Kabul, Afghanistan.

g. On or about January 9, 2015, the Cyber Conspirators, using the bella.wood87@yahoo.com account, sent another email to USG Agent 2 intended to induce USG Agent 2 to click on certain links. The body of the email stated:

> I'll send you a file including my photos but u should deactivate your anti virus to open it because i designed my photos with a photo album software, I hope you enjoy the photos i designed for the new year, they should be opened in your computer honey.

Although not apparent to the recipient, clicking one of the links in this email would cause the recipient's computer to connect to a server controlled by the Cyber Conspirators.

The USG Agent 3 Imposter Account

h. On or about March 8, 2015, the Cyber Conspirators created an imposter Facebook account under the true name of USG Agent 3 (hereinafter referred to as the "Imposter Account"). The Cyber Conspirators designed the Imposter Account using information and photos taken from a legitimate Facebook account maintained by USG Agent 3.

i. On or about March 15, 2015, the Cyber Conspirators, using the Imposter Account, sent a Facebook friend request to USG Agent 1, who accepted the request. On or about the same day, the Imposter Account sent USG Agent 1 a message with an attachment that appeared by its name to be a .jpg image file. The attachment was in fact a .zip file containing malware. Had USG Agent 1 opened that file, it would have launched malware that would have provided the Cyber Conspirators with covert, persistent access on USG Agent 1's computer and any associated network.

j. On or about March 8, 2015, the Cyber Conspirators, using the Imposter Account, sent a friend request to USG Agent 4, who, believing the Imposter Account to be legitimate, accepted the request.

k. On or about March 12, 2015, the Cyber Conspirators, using the Imposter Account, sent a message to USG Agent 4 asking for help opening a photo album that the Imposter Account claimed would not run on "her" laptop. USG Agent 4, having learned that the Imposter Account was not legitimate, defriended the account.

l. On or about March 10, 2015, the Cyber Conspirators, having designed the Imposter Account to appear legitimate, caused USG Agent 5 to "friend" the Imposter Account and, thereafter, to vouch for the Imposter Account by adding it to a private Facebook group composed primarily of USG Agents. By joining the group, the Cyber Conspirators obtained greater access to information regarding USG Agents.

m. On or about May 10, 2015, the Cyber Conspirators, using the Imposter Account, sent separate messages to USG Agents 2, 6, 7, and 8. Each of the messages contained a link that appeared to be associated with an international news outlet, and, in sending the link, the Cyber Conspirators asked if the article was about the recipient. If clicked, the link would have directed the recipients to a page controlled by the Cyber Conspirators.

Spearphishing Messages

n. On or about May 17, 2015, the Cyber Conspirators designed a "fake email" message that, on its face, appeared to come from USG Agent 7, with an email address that contained the true name of USG Agent 7 followed by "@ogn.af.mil," which is a USG domain name. The Cyber Conspirators' purpose in designing this type of fake email was to deceive recipients into believing that they had received an email from USG Agent 7, when in fact the message had been sent by the Cyber Conspirators.

o. On or about May 22, 2015, the Cyber Conspirators designed another fake email that, on its face, appeared to originate from "mail@facebook.com," with the subject "Reset Password," and a message that was designed to trick the recipient into unwittingly providing his or her true Facebook account credentials to the Cyber Conspirators.

(**Conspiracy to Commit Computer Intrusions**, in violation of Title 18, United States Code, Sections 371 and 1030)

COUNT FIVE
(Attempt to Commit a Computer Intrusion Causing Damage)

57. The grand jury realleges and incorporates by reference the General Allegations set forth in this Indictment and paragraphs 51-56 of Count Four.

58. From in or around December 2014 to at least in or around May 2015, **MASOUMPOUR**, **MESRI**, **PARVAR**, and **PARYAR**, and other individuals whose identities are known and unknown to the grand jury, aiding and abetting each other and others, without authorization, knowingly attempted to cause the transmission of programs, information, codes, and commands, to wit, an attachment that was designed to connect to a server and install malware capable of establishing covert, persistent access, by **MASOUMPOUR**, **MESRI**, **PARVAR**, and **PARYAR**, on the computer and associated network of the intended recipients, who were USG Agents, and, as a result of such conduct, intentionally attempted to cause damage without authorization to protected computers, and where the offense did cause and would, if completed, have caused: loss aggregating at least $5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer; damage affecting a computer used by or for an entity of the United States government in furtherance of the administration of justice, national defense, or national security; and damage affecting at least 10 protected computers during a one-year period.

(**Attempt to Commit a Computer Intrusion Causing Damage to a Protected Computer**, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(B)(i) & (ii) and 2)

COUNT SIX
(Attempt to Commit a Computer Intrusion Obtaining Information)

59. The grand jury realleges and incorporates by reference the General Allegations set forth in this Indictment and paragraphs 51-56 of Count Four.

60. From in or around December 2014 to at least in or around May 2015, **MASOUMPOUR**, **MESRI**, **PARVAR**, and **PARYAR**, and other individuals whose identities are known and unknown to the grand jury, aiding and abetting each other and others, without authorization, intentionally attempted to access a computer without authorization, in order to obtain information from a protected computer, and from a department and agency of the United States, the value of which information exceeded $5,000.

(**Attempt to Commit a Computer Intrusion Obtaining Information From a Protected Computer**, in violation of Title 18, Unites States Code, Sections 1030(a)(2)(B) & (C), (c)(2)(B)(iii) and 2)

COUNT SEVEN
(Aggravated Identity Theft)

61. The grand jury realleges and incorporates by reference the General Allegations set forth in this Indictment and paragraphs 51-56 of Count Four.

62. From in or around December 2014 to at least in or around May 2015, **MASOUMPOUR**, **MESRI**, **PARVAR**, and **PARYAR**, and other individuals whose identities are known and unknown to the grand jury, aiding and abetting each other and others, did knowingly transfer, possess, and use without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated under Title 18, United States Code, Section 1028(c), namely, attempt to commit computer intrusion, in violation of Title 18, United States Code, Section 1030, knowing that the means of identification belonged to another real person.

(**Aggravated Identity Theft**, in violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), and 2)

A TRUE BILL

[redacted]

FOREPERSON

Jessie K. Liu /DAC

Attorney of the United States in
and for the District of Columbia