UNITED STATES DISTRICT COURT
FOR THE
DISTRICT OF VERMONT

UNITED STATES OF AMERICA	)
	) No. 2:15-CR-15-1, 2 (WKS)
v.	)
	) (18 U.S.C. §§ 371, 1030(a)(2), 1030
MOHAMMED SAEED AJILY and	) (c)(2)(B)(iii), 1343, & 2; 22 U.S.C. §§
MOHAMMED REZA REZAKHAH,	) 2778(b)(2) & (c); 22 C.F.R. §§ 121.2,
Defendants	) 123.1, 127.1; 50 U.S.C. § 1705; 31
	) C.F.R. §§ 560.203 and 560.204)

SUPERSEDING INDICTMENT

The Grand Jury Charges:

Count One

INTRODUCTION

At all times relevant to this indictment:

1. Arrow Tech was a Vermont-based engineering consulting and software company that did business in interstate and foreign commerce. Arrow Tech's primary product was PRODAS (Projectile Rocket Ordnance Design and Analysis System), a proprietary software that assists users in, among other things, aerodynamics analysis and design for projectiles from bullets to GPS guided artillery shells. PRODAS was designated as a "defense article" on the United States Munitions List under the International Traffic in Arms Regulations.

2. Arrow Tech marketed its products, including PRODAS, through its website. Depending on customization and customer support packages, PRODAS typically sold for between $40,000 and $800,000.

3. In order to obtain a copy of the software, customers downloaded a locked version of the software from Arrow Tech's website and received a special hardware key, or "dongle," with a code to allow access to the software. Arrow Tech's website informed foreign customers that "Arrow Tech software shipped outside of the United States requires an Export License approved by the United States State Department."

4. MOHAMMED REZA REZAKHAH was a citizen of Iran and worked as a computer hacker and software "cracker," (i.e. someone who breaks protective encryption to allow the use of restricted software). REZAKHAH and co-conspirator Nima Golestaneh operated under the company name "Dongle Labs" to sell customers the capability to circumvent these types of protections on a variety of software packages. REZAKHAH also conducted other hacking and cracking activities at the direction of MOHAMMED SAEED AJILY. REZAKHAH frequently relied upon servers obtained by co-conspirator Nima Golestaneh in order to conduct his illicit online activities.

5. MOHAMMED SAEED AJILY was an Iranian businessman who used a group of hackers and crackers, including REZAKHAH, to obtain software in contravention of Western sanctions against Iran for the Iranian market, including for Iranian military and government entities. AJILY did so through multiple companies, including Andisheh Vesal Middle East Company. In addition to payment, he received certificates of appreciation for his work from several of the Iranian government and military entities.

CONSPIRACY

6. From at least as early as August 2007 through at least May 2013, in the District of Vermont and elsewhere, the defendants MOHAMMED REZA REZAKHAH and MOHAMMED SAEED AJILY knowingly and willfully conspired with each other and others known and

unknown to the grand jury, including Nima Golestaneh, to intentionally access protected computers without authorization and thereby obtain information from the protected computers where the value of the information obtained exceeded $5,000.00, in violation of 18 U.S.C. §§ 1030(a)(2) and 1030(c)(2)(B)(iii).

OBJECT OF THE CONSPIRACY

7. It was the object of the conspiracy that the defendants MOHAMMED REZA REZAKHAH and MOHAMMED SAEED AJILY would access computers without authorization in order to obtain software, and would sell and redistribute the software in Iran, a country against which the United States has economic sanctions, and elsewhere outside of the United States. In many instances, including PRODAS, the sale and redistribution of such software was in violation of United States sanctions and export licensing requirements.

MANNER AND MEANS OF THE CONSPIRACY

8. It was part of the conspiracy that MOHAMMED SAEED AJILY would task MOHAMMED REZA REZAKHAH and others with obtaining or cracking particular pieces of software for him to market and sell.

9. It was further a part of the conspiracy that Nima Golestaneh, a known co-conspirator, would acquire access to servers, including a Canadian server ("Server 1") and a Dutch server ("Server 2"), knowing that they would be used, among other things, to obtain unauthorized access to other computers.

10. It was further a part of the conspiracy that MOHAMMED REZA REZAKHAH would use the servers Golestaneh acquired to conduct unauthorized computer intrusions so that the intrusions would be more difficult to trace.

11. It was further a part of the conspiracy that MOHAMMED REZA REZAKHAH, Nima

Golestaneh and others would use a variety of names and email addresses to further conceal their identities and their association with the computer intrusions.

12. It was further a part of the conspiracy that MOHAMMED REZA REZAKHAH would use servers Nima Golestaneh acquired to gain unauthorized access to Arrow Tech's computers despite Arrow Tech's security precautions.

13. It was further a part of the conspiracy that MOHAMMED REZA REZAKHAH would use the unauthorized access to Arrow Tech's computers to steal PRODAS and other proprietary information and to transmit such software and information to Server 2.

14. It was further a part of the conspiracy that MOHAMMED SAEED AJILY would market and sell software, including Arrow Tech's PRODAS, in Iran and elsewhere outside the United States once it was acquired by the conspiracy.

OVERT ACTS

15. In furtherance of the conspiracy, on or about August 23, 2007, MOHAMMED SAEED AJILY tasked MOHAMMED REZA REZAKHAH with cracking software on behalf of an Iranian customer.

16. In furtherance of the conspiracy, on or about January 4, 2012, MOHAMMED SAEED AJILY offered software for sale from Andisheh Vesal Middle East Company, including a version of Arrow Tech's PRODAS. In describing PRODAS, AJILY noted that he could provide the software to Iranian purchasers without obtaining the necessary licenses from the United States Government.

17. In furtherance of the conspiracy, on or about January 4, 2012, MOHAMMED SAEED AJILY advertised what he referred to as his group of software hackers and crackers and their ability to circumvent Western sanctions against Iran by hacking the servers of software

manufacturers and cracking software protections in order to obtain software for Iranian entities, including government entities and purported research centers and military production industries, all in contravention of Western sanctions against Iran. Such entities included, but were not limited to, Malek Ashtar Defense University, Tehran University, Sharif Technical University, Khvajeh Nasir University, and Shiraz Electro Optic Industry.

18. In furtherance of the conspiracy, from at least as early as April 2012, Nima Golestaneh acquired access to servers, including Server 1 and Server 2, knowing that they would be used, among other things, to obtain unauthorized access to other computers.

19. In furtherance of the conspiracy, on or about July 31, 2012, MOHAMMED SAEED AJILY tasked MOHAMMED REZA REZAKHAH with obtaining software from a Western company specializing in aerospace control and simulation technology.

20. In furtherance of the conspiracy, on or about October 22, 2012, MOHAMMED REZA REZAKHAH sent a wire communication from Server 1 located outside the United States to Arrow Tech's website hosted in Vermont, transmitting computer commands designed to provide unauthorized access to Arrow Tech's computers.

21. In furtherance of the conspiracy, on or about October 22, 2012, MOHAMMED REZA REZAKHAH sent a wire communication from Server 2 located outside the United States to Arrow Tech's website hosted in Vermont transmitting computer commands designed to provide unauthorized access to Arrow Tech's computers.

22. In furtherance of the conspiracy, on or about October 22, 2012, MOHAMMED REZA REZAKHAH sent a wire communication from a third computer located outside the United States to Arrow Tech's website hosted in Vermont transmitting computer commands designed to provide unauthorized access to Arrow Tech's computers.

23. In furtherance of the conspiracy, on or about October 22, 2012, MOHAMMED REZA REZAKHAH obtained unauthorized access to at least one Arrow Tech computer in Vermont.

24. In furtherance of the conspiracy, on or about October 22, 2012, MOHAMMED REZA REZAKHAH sent a wire communication from an Arrow Tech computer in Vermont to Server 2 outside the United States transmitting version 3.6.5 of PRODAS, a version that had been in existence since only in or around June 2012, and other proprietary information.

25. In furtherance of the conspiracy, on or about April 8, 2013, MOHAMMED SAEED AJILY offered software for sale, including Arrow Tech's PRODAS, using marketing materials similar to those used on or about January 4, 2012.

(18 U.S.C. § 371)

Count Two

1. The Grand Jury repeats and realleges paragraphs 1 through 5 and 7 through 25 of Count One of this Indictment.

2. On or about October 22, 2012, in the District of Vermont and elsewhere, the defendants MOHAMMED REZA REZAKHAH and MOHAMMED SAEED AJILY intentionally accessed, and aided and abetted the accessing of, a computer without authorization, and thereby obtained information from a protected computer where the value of the information obtained exceeded $5,000.00.

(18 U.S.C. §§ 1030(a)(2) and(c)(2)(B)(iii) & 2)

Counts Three – Six

1. The Grand Jury repeats and realleges paragraphs 1 through 5 and 7 through 25 of Count 1 of this Indictment.

2. From at least as early as April 2012 through at least May 2013, the defendant MOHAMMED REZA REZAKHAH, MOHAMMED SAEED AJILY, and others known and unknown to the grand jury, including Nima Golestaneh, intended to devise a scheme to defraud Arrow Tech and other software companies, and to obtain property from Arrow Tech and other software companies by means of materially false and fraudulent pretenses, representations, and promises.

3. On or about the following date, in the District of Vermont and elsewhere, the defendant MOHAMMED REZA REZAKHAH, MOHAMMED SAEED AJILY, and others known and unknown to the grand jury, including Nima Golestaneh, knowingly caused to be transmitted by means of wire communication in interstate and foreign commerce, and aided and abetted the causing of such transmission, the following signals and sounds in furtherance of the scheme to defraud:

COUNT	DATE	WIRE COMMUNICATION
3	October 22, 2012	From Server 1 outside of the United States to Arrow Tech's website hosted in Vermont, transmission of computer commands designed to provide unauthorized access to Arrow Tech's computers
4	October 22, 2012	From Server 2 outside of the United States to Arrow Tech's website hosted in Vermont, transmission of computer commands designed to provide unauthorized access to Arrow Tech's computers

5	October 22, 2012	From a computer outside the United States to Arrow Tech's website hosted in Vermont, transmission of computer commands designed to provide unauthorized access to Arrow Tech's computers
6	October 22, 2012	From an Arrow Tech computer in Vermont to Server 2 outside of the United States, transmission of proprietary software and other proprietary information

(18 U.S.C. §§ 1343 & 2)

Count Seven

1. The Grand Jury repeats and realleges paragraphs 1 through 5 and 7 through 25 of Count One of this Indictment.

2. The Arms Export Control Act ("AECA"), 22 U.S.C. § 2778, authorized the President of the United States, among other things, to control the export of "defense articles." 22 U.S.C. § 2778(a)(1). AECA also gave the President the authority to designate items as "defense articles." Id. As a practical matter, that task was performed by the Department of State ("DOS"), with the concurrence of the Department of Defense, through regulations that were promulgated by the DOS's Directorate of Defense Trade Controls ("DDTC"). 22 C.F.R. Parts 120.1 and 120.2. The regulations promulgated by the DDTC were known as the International Traffic in Arms Regulations ("ITAR"), and specify items that are designated as defense articles. 22 C.F.R. Parts 120 – 130. All defense articles were identified by category in a portion of the ITAR that is known as the "United States Munitions List." Any person seeking to export defense articles listed in the ITAR must request and obtain a license from the DOS before doing so.

3. At no time relative to this Indictment did defendants MOHAMMED REZA REZAKHAH, MOHAMMED SAEED AJILY, or any co-conspirators, including Nima Golestaneh, request or obtain the required license from the Department of State for the export of PRODAS.

4. From at least as early as January 2012 through at least May 2013, in the District of Vermont and elsewhere, the defendants MOHAMMED REZA REZAKHAH and MOHAMMED SAEED AJILY knowingly and willfully exported and caused to be exported, and attempted to export and caused to be exported, from the United States through the Netherlands to Iran, Arrow Tech's PRODAS software, which was designated as an ITAR-controlled defense article on the

United States Munitions List, without having first obtained from the Department of State the required license for such export or written authorization for such export. MOHAMMED REZA REZAKHAH and MOHAMMED SAEED AJILY did so by transmitting PRODAS from the United States via the Internet and by disclosing PRODAS to foreign persons, including themselves.

(22 U.S.C. §§ 2778(b)(2) & (c), 22 C.F.R. §§ 121.1, 123.1, 127.1, & 18 U.S.C. § 2)

Count Eight

1. The Grand Jury repeats and realleges paragraphs 1 through 5, and 7 through 25, of Count One of this Indictment.

2. The International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701-1706, authorized the President of the United States ("the President") to impose economic sanctions on a foreign country in response to an unusual or extraordinary threat to the national security, foreign policy or economy of the United States when the President declares a national emergency with respect to that threat. Pursuant to the authority under the IEEPA, the President and the executive branch have issued orders and regulations governing and prohibiting certain transactions with Iran by U.S. persons or involving U.S.-origin goods.

3. Beginning with Executive Order No. 12170, issued on November 14, 1979, the President found that "the situation in Iran constitutes an unusual and extraordinary threat to the national security, foreign policy and economy of the United States and declare[d] a national emergency to deal with that threat."

4. On May 6, 1995, the President issued Executive Order No. 12959, adopting and continuing Executive Order No. 12170 (collectively, the "Executive Orders"), and prohibiting, among other things, the exportation, re-exportation, sale, or supply, directly or indirectly, to Iran of any goods, technology, or services from the U.S. or by a U.S. person. The Executive Orders authorized the U.S. Secretary of the Treasury to promulgate rules and regulations necessary to carry out the Executive Orders. Pursuant to this authority, the Secretary of the Treasury promulgated the Iranian Transactions and Sanctions Regulations ("ITSR"), implementing the sanctions imposed by the Executive Orders.

5. The ITSR generally prohibited any person from exporting or causing to be exported from the U.S. any goods, services or technology without having first obtained an export license from

the U.S. Department of the Treasury, Office of Foreign Assets Control ("OFAC"), which is located in the District of Columbia. The ITSR imposed, among others, the following prohibitions:

> Section 560.203 - Prohibition of any Transaction to Evade or Avoid the Embargo and any Attempt to Violate the Embargo:
>
> Any transaction by any United States person or within the United States that evades or avoids, or has the purpose of evading or avoiding, or attempts to violate, any of the prohibitions contained in this part is hereby prohibited.
>
> Section 560.204 - Prohibition of any Sale or Supply of any Goods, Technology, Services to Iran or the Iranian Government:
>
> Except as otherwise authorized [by a license issued by OFAC], the exportation, . . . sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any goods, technology, or services to Iran or the Government of Iran is prohibited, including the exportation, . . . sale, or supply of any goods, technology, or services to a person in a third country undertaken with knowledge or reason to know that:
>
> Such goods, technology, or services are intended specifically for supply . . . or re-exportation directly or indirectly, to Iran or the Government of Iran . . . .

6. The Iran Trade Embargo and the ITSR were in effect at all times relevant to this Indictment.

7. At no time relevant to this Indictment did defendants MOHAMMED REZA REZAKHAH, MOHAMMED SAEED AJILY, or any co-conspirators including Nima Golestaneh, apply for, receive, or possess a license from OFAC to export goods, technology, or services to Iran of any kind.

8. From at least as early as January 2012 through at least May 2013, in the District of Vermont and elsewhere, the defendants MOHAMMED REZA REZAKHAH and MOHAMMED SAEED AJILY did knowingly and willfully violate and attempt to violate the embargo against

Iran by exporting and attempting to export software, including the PRODAS software, from the United States to Iran without first having obtained the required licenses and authorizations from the U.S. Department of the Treasury's OFAC.

(50 U.S.C. § 1705, 31 C.F.R. §§ 560.203 and 560.204, & 18 U.S.C § 2)

A TRUE BILL

[redacted]

FOREPERSON

for Eric S. Miller

ERIC S. MILLER
United States Attorney
Burlington, VT
April 21, 2016