F.#2014R01763

SDD:CRH/PWB

16 M 0893

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- x

UNITED STATES OF AMERICA

- against -

DMITRII ALEKSANDROVICH KARPENKO
also known as "Simon Fox,"
and ALEXEY KRUTILIN
also known as "David Powell,"

Defendants.

- x

TO BE FILED UNDER SEAL

COMPLAINT AND
AFFIDAVIT IN SUPPORT OF
APPLICATION FOR
ARREST WARRANT

(T. 18, U.S.C. §§ 371 and 2;
T. 50, U.S.C. § 1705)

EASTERN DISTRICT OF NEW YORK, SS:

SUSAN RUIZ, being duly sworn, deposes and states that she is a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"), duly appointed according to law and acting as such.

Upon information and belief, in or about and between February 1, 2015 and October 5, 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants DMITRII ALEKSANDROVICH KARPENKO also known as "Simon Fox," and ALEXEY KRUTILIN, also known as "David Powell," together with others, did knowingly, intentionally and willfully export, and attempt to export, from the United States to Russia items on the United States Commerce Control List, to wit: (i) five (5) digital-to-analog converters; (ii) one-hundred and fifty (150) integrated circuits; (iii) forty-two (42) integrated circuits; and (iv) two-hundred and eight (208) integrated

circuits, without first having obtained a license from the Department of Commerce, in violation of Title 50, United States Code, Section 1705 and Title 18, United States Code, Section 2, and conspired to do the same in violation of Title 18, United States Code, Section 371.

(Title 50, United States Code, Section 1705; Title 18, United States Code, Sections 2 and 371).

The source of your deponent's information and the grounds for his belief are as follows:

1. I am a Special Agent with HSI and have been so employed since 2010. During my employment with HSI, I have participated in numerous investigations, during the course of which I have interviewed suspects and witnesses, conducted physical surveillance, executed court-authorized search and arrest warrants, and used other investigative techniques to secure relevant information regarding various crimes. As a result of my training and experience, I am familiar with techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

2. This affidavit is based upon my conversations with law enforcement agents, witnesses and others, as well as my examination of reports and records. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts obtained during the course of the investigation. Where the contents of documents and the actions, statements and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

I. APPLICABLE EXPORT REGULATIONS

3. Under the International Emergency Economic Powers Act ("IEEPA"), Title 50, United States Code, Sections 1701-1707, the President of the United States was granted authority to deal with unusual and extraordinary threats to the national security, foreign policy, or economy of the United States. 50 U.S.C. § 1701(a). Pursuant to that authority, the President may declare a national emergency through Executive Orders that have the full force and effect of law. Among other things, IEEPA empowers the President to issue regulations governing exports from the United States.

4. Pursuant to IEEPA, on August 17, 2001, the President issued Executive Order 13,222, which declared a national emergency with respect to the unusual and extraordinary threat to the national security, foreign policy, and economy of the United States in light of the expiration of the Export Administration Act ("EAA"), 50 App. U.S.C. §§ 2401-2420, which lapsed on August 17, 2001. 66 Fed. Reg. 44,025 (Aug. 22, 2001). While in effect, the EAA regulated the export of goods, technology, and software from the United States. Pursuant to the provisions of the EAA, the Department of Commerce ("DOC")'s Bureau of Industry and Security ("BIS") promulgated the Export Administration Regulations ("EAR"), 15 C.F.R. §§ 730-774, which contained restrictions on the export of goods outside of the United States, consistent with the policies and provisions of the EAA. See 15 C.F.R. § 730.2. In Executive Order 13,222, pursuant to IEEPA, the President ordered that the EAR's provisions remain in full force and effect despite the expiration of the EAA. Presidents have issued annual Executive Notices extending the national emergency declared in Executive Order 13,222 from the time period covered by that Executive Order through the present. See, e.g., 81 Fed. Reg. 52,587 (Aug. 8, 2016).

5. Under IEEPA, it is a crime to willfully violate, attempt to violate, conspire to violate, or cause a violation of any order, license, regulation, or prohibition issued pursuant to the statute. 50 U.S.C. § 1705(a). Willful violations of the EAR constitute criminal offenses under IEEPA, and carry a 20-year maximum term of imprisonment and up to a $1,000,000 fine. 50 U.S.C. § 1705(c).

6. Through the EAR, BIS reviews and controls the export from the United States to foreign countries of certain U.S. items. 15 C.F.R. §§ 734.2-.3. In particular, BIS has placed restrictions on the export and reexport of items that it has determined could make a significant contribution to the military potential or nuclear proliferation of other nations or that could be detrimental to the foreign policy or national security of the United States. Under the EAR, such restrictions depend on several factors, including the technical characteristics of the item, the destination country, the end user, and the end use.

7. The most sensitive items subject to EAR controls were identified on the Commerce Control List, or "CCL," set forth in Title 15, Code of Federal Regulations, part 774, Supplement Number 1. Items listed on the CCL were categorized by Export Control Classification Number ("ECCN"), each of which had export control requirements depending on destination, end use, and end user.

II. THE INVESTIGATION

8. HSI, in conjunction with the DOC, the Federal Bureau of Investigation ("FBI"), and the Department of Defense, Defense Criminal Investigative Service ("DCIS"), is conducting an investigation into the activities of the defendants, and others known and unknown for illegally exporting items to Russia without a license from the DOC, in violation of IEEPA and the EAR, and conspiring to do the same.

9. The investigation has revealed that, between approximately February 2015 and the present, DMITRII ALEKSANDROVICH KARPENKO also known as "Simon Fox," ("KARPENKO") and ALEXEY KRUTILIN, also known as "David Powell," ("KRUTILIN") and additional co-conspirators have obtained export-controlled technology by, among other things, lying about the location of the end-users of the technology, and knowingly exporting, or attempting to export, the technology to Russia without a license from the DOC.

10. The conspiracy to obtain and illegally export controlled items includes KARPENKO, KRUTILIN, an individual identified as "Alexey Barysheff" ("ALEXEY BARYSHEFF" or "BARYSHEFF"), and other known and unknown individuals who, based on the evidence described below, appear to be located in the United States, Russia and Finland, and who are attempting to acquire CCL items and other commodities from various U.S.-based manufacturers. The scheme includes the use of at least two Brooklyn, New York-based "front companies," identified as "BKLN Spectra, Inc." ("SPECTRA") and "UIP Techno Corp." ("UIP TECHNO").

A. The Scheme to Obtain License-Controlled Technology for Illegal Export

11. SPECTRA is a company that identifies a residence in Brooklyn, New York as its physical address. According to public records, BARYSHEFF resides at the SPECTRA address in Brooklyn. Surveillance by investigating agents further confirmed that BARYSHEFF was using that locations as a residence.

12. SPECTRA operates the websites "www.bkspectra.com" and "www.bkspectra.us." The two websites associated with SPECTRA are hosted by GoDaddy,

a web hosting and email services company. According to its websites, SPECTRA purports to be involved in "the supply of electronics and electronic equipment."

13. According to records provided by GoDaddy, the services that it provides to SPECTRA—which include web hosting, domain name registration, and the ability to create and use multiple email addresses—were paid for by BARYSHEFF and another individual. The website and associated hosting services were purchased from GoDaddy on or about February 12, 2015.

14. According to publicly-available records, SPECTRA was registered on or about February 18, 2015 with the New York State Department of State, by BARYSHEFF. The address provided in the filing, located in Brooklyn, New York, is the same address listed on the SPECTRA websites.

15. UIP TECHNO is a company that also identifies a location in Brooklyn, New York as its physical address.

16. UIP TECHNO operates the websites "www.uiptechno.com." According to its website, UIP TECHNO purports to be involved in "development and implementation IT for industrial projects." Like SPECTRA, the website associated with UIP TECHNO is hosted by GoDaddy, and the services were also paid for by BARYSHEFF.

17. According to publicly-available records, UIP TECHNO was registered on September 28, 2015 with the New York State Department of State, by BARYSHEFF. The entity address information provided in the filing, located in Brooklyn, New York, is the same address listed on the UIP TECHNO website.

18. As described more fully below, KARPENKO and KRUTILIN claim to be employees of UIP TECHNO. However, according to records provided by the New York

State Department of Labor, BARYSHEFF is the only listed employee of SPECTRA and UIP TECHNO. BARYSHEFF is also identified as the "President" and "owner" of both companies.

19. BARYSHEFF is dual citizen of the United States and Russia, who is originally from Russia.

20. Based on my training and experience, I know that illegal procurement schemes will often use U.S.-based front companies to purchase and attempt to purchase license-controlled technology or as the purported ultimate end-users of license-controlled technology in an effort to circumvent U.S. export laws, because CCL items destined for end-users in the United States do not require an export license. Then, once the U.S.-based front company receives CCL items, they illegally export them from the U.S. without the required export license.

21. Consistent with this experience, and as described more fully below, this investigation has revealed that KARPENKO, KRUTILIN, BARYSHEFF and other individuals associated with SPECTRA and UIP TECHNO engaged in a scheme where they would do the following: (1) send email communications from email accounts associated with SPECTRA (i.e., from email accounts ending in "@bkspectra.com") or UIP TECHNO (i.e., from email accounts ending in "@uiptechno.com") to a U.S. based manufacturer or distributor of license-controlled technology; (2) ask to purchase certain electronic components, some of which were license-controlled; (3) when asked to provide information about the end-user of the technology, respond with false information – including fraudulent written documentation – about a U.S.-based end-user, ostensibly in order to avoid a request

for an appropriate export license; (4) purchase the technology; and (5) knowingly export the technology without the appropriate license from the DOC.

B. Example Transaction #1: Illegal Export of Digital-to-Analog Converters

22. According to information obtained from a Minnesota-based corporation involved in the sale of electronic components ("COMPANY-1"), on or about October 28, 2015, an individual who identified himself via an email communication as BARYSHEFF, using the email account "j.reed@bkspectra.com," placed a web-based order with COMPANY-1 for certain electronic components, including five digital-to-analog converters (the "converters").

23. A digital-to-analog converter is an electronic device used to convert digital signals to analog form. Depending on their specifications, digital-to-analog converters have a wide range of applications and can be used in commercial devices including music players, televisions, mobile phones, as well as military radar systems and oscilloscopes.

24. According to a DOC license determination, a license is required to export the converters to certain foreign countries, including Russia. The converters are license-controlled for national security and anti-terrorism reasons.

25. COMPANY-1 sent an email to the email account being used by the individual who identified himself as BARYSHEFF. The email requested more information about SPECTRA, and the end user for the converters.

26. In response, an individual operating the email account associated with BARYSHEFF stated that SPECTRA was an "independent distributor," that "this particular order is for domestic use," and offered to complete an end user statement.

27. On or about November 6, 2015, an individual operating the email account associated with BARYSHEFF submitted an end user statement to COMPANY-1. The document identified a company in North Carolina as the end user of the converters, and provided the name of an employee as the "ultimate consignee."

28. The company identified in the end user statement provided by BARYSHEFF subsequently informed law enforcement that it had no business with SPECTRA, and had never employed anyone with the name listed on the statement.

29. COMPANY-1 subsequently emailed the individual identifying himself as BARYSHEFF, and stated that the converters "would require a license from the US Department of Commerce if it were being exported to certain regions of the world."

30. On or about November 10, 2015, COMPANY-1 shipped the converters to the address in Brooklyn, New York associated with SPECTRA.

31. On or about November 23, 2015, SPECTRA shipped a package of items to a company located in Finland. According to the shipping records associated with this package, the package included a quantity of five items identified as "IC Analog Converter" with part number "A-9139BC." The serial number associated with the five license-controlled converters ordered by SPECTRA is AD9139BCPZ.

32. As mentioned above, certain commodities, like the converters purchased from COMPANY-1, require a license to be exported to Russia, but not to certain other countries like Finland. Based on my training and experience, I have learned that criminal enterprises will use countries like Finland, because of its proximity to Russia and lack of similar licensing requirements, as a transshipment point for products ultimately destined for Russia. The license-controlled technology is typically shipped from a U.S.-

based front company (e.g., SPECTRA or UIP TECHNO) to a freight forwarder in the country without licensing requirements (e.g., Finland) and then re-exported to the country with licensing requirements (e.g., Russia) without obtaining the requisite export license.

33. Indeed, according to an investigation performed by the DOC Office of Export Enforcement, Finland is a known intermediate destination for the shipment of items with end users in Russia. Additionally, the Finnish company identified by SPECTRA in the shipping records is known to be a company that acts as an intermediate shipper to Russia.

34. The DOC has advised that no license has ever been obtained by anyone for the analog-to-digital converters that were exported by BARYSHEFF.

C. Example Transaction #2: Illegal Export of Integrated Circuits

35. On or about November 18, 2015, an individual operating an email account associated with SPECTRA sent email communications to a New York-based business (COMPANY-2), which requested a quote for, among other things, integrated circuits.

36. Generally speaking, integrated circuits are sets of electronic circuits on one small plate of semi-conductor material, normally silicon. Integrated circuits are used in virtually all electronic equipment today, from computers and mobile phones to aircraft, missile, and space programs.

37. After receiving a quote for the items from COMPANY-2, on or about December 18, 2015, an individual operating the email account j.reed@spectra.com provided COMPANY-2 with a purchase order for some of these items. The email account used to send this purchase order is the same email address that was used by BARYSHEFF to

purchase the five analog-to-digital converters described above, which were subsequently exported without the required license.

38. On or about December 21, 2015, in response to requests from COMPANY-2, an individual operating the same SPECTRA email account submitted an end-use certificate, which indicated that the items being purchased by SPECTRA were for domestic use only. On or around December 23, 2015, the individual operating that email account further indicated that the end user was a company located in Pennsylvania.

39. Subsequently, the company located in Pennsylvania confirmed to law enforcement that they are not the end user of the products.

40. On or about January 13, 2016, SPECTRA purchased one-hundred and fifty (150) integrated circuits from COMPANY-2.

41. According to a DOC licensing determination, a license is required to export these integrated circuits to certain foreign countries, including, but not limited to, Russia. Further, according to the DOC, the integrated circuits are license-controlled for national security and anti-terrorism reasons.

42. On or about May 2, 2016, a representative from COMPANY-2 notified the DOC that the integrated circuits purchased by SPECTRA had been received from the manufacturer. On that same day, DOC agents met with COMPANY-2 and took possession of all 150 integrated circuits.

43. On the same day, COMPANY-2, in consultation with the DOC, contacted SPECTRA via the email address previously identified as being used by BARYSHEFF. Among other things, COMPANY-2 notified the user of the email address associated with BARYSHEFF that the 150 integrated circuits had been received from the

manufacturer, and asked SPECTRA to confirm that none of the information previously provided in connection with the order had changed. In addition, COMPANY-2 specifically notified SPECTRA that the integrated circuits in question would require a license from the DOC before the parts could be shipped outside of the United States.

44. On or about May 4, 2016, COMPANY-2 received an email response from the email address associated with BARYSHEFF, which stated, in sum and substance, that the previously provided information was correct and requested that the parts be shipped to the address in Brooklyn, New York that is both the listed address for SPECTRA and the residence of BARYSHEFF.

45. On or about May 5, 2016, agents from the DOC rendered inoperable the 150 integrated circuits obtained from COMPANY-2. On or about May 6, 2016, the Honorable Robert M. Levy, United States Magistrate Judge for the Eastern District of New York, issued a warrant authorizing federal law enforcement agents and technicians assisting in the above-described investigation to install a tracking device in a package containing the 150 integrated circuits obtained from COMPANY-2 that was to be sent to SPECTRA. See Case No. 16-M-428 (filed under seal).

46. On or about May 9, 2016, DOC agents packed the inoperable integrated circuits and the tracking device into a package addressed to the address for SPECTRA (the residence of BARYSHEFF), and delivered the package to United Parcel Service ("UPS"). Thereafter, UPS delivered that package to SPECTRA's address in Brooklyn, New York.

47. On or about May 10, 2016, BARYSHEFF was observed leaving the Brooklyn, New York address associated with SPECTRA with the package believed to contain the 150 integrated circuits. A short while later, BARYSHEFF and another individual

were seen taking the package into a second location in Brooklyn, New York, which was subsequently identified as the offices of UIP TECHNO. Later that same day, BARYSHEFF was observed leaving the UIP TECHNO location without the package believed to contain the 150 integrated circuits.

48. On or about May 11, 2016, BARYSHEFF was observed returning to the UIP TECHNO location. A short while later, BARYSHEFF was observed leaving that location with the package believed to contain the 150 integrated circuits.

49. BARYSHEFF was observed traveling with the package believed to contain the 150 integrated circuits to a shipping company located in Brooklyn, New York. BARYSHEFF later left the shipping company location without the package.

50. On or about May 12, 2016, the package believed to contain the 150 integrated circuits was picked up from the shipping company location by a DHL delivery truck. After the package was placed in the DHL delivery truck, federal law enforcement agents identified themselves to the DHL driver and asked to see the package. The DHL driver directed the agents to the package.

51. Agents were able to observe the shipper and addressee information on the outside of the package. The listed shipper was SPECTRA, and the listed addressee was a business with an address in Moscow, Russia.

52. On May 17, 2016, pursuant to a search warrant authorized by Magistrate Judge Peggy Kuo of the Eastern District of New York, law enforcement agents seized the package being shipped by SPECTRA. The package contained the 150 inoperable integrated circuits, which were not supposed to be exported without a license from the DOC.

53. The DOC has advised that no license has ever been obtained by anyone for the integrated circuits that were attempted to be exported by BARYSHEFF.

54. On or about May 26, 2016, federal law enforcement agents spoke to BARYSHEFF over the phone, and subsequently conducted an in-person, non-custodial interview with BARYSHEFF, regarding the integrated circuits that had been seized. During these two conversations, BARYSHEFF admitted, in sum and substance and in part, that (1) he is the "owner" and "boss" of SPECTRA; (2) he is responsible for receiving and shipping orders; (3) he ships items internationally, and that some customers are located in Russia; and (4) he had heard of export license requirements, but claimed that he did not think they applied to his work.

D. Additional Scheme to Illegally Export Additional Controlled Technology

55. On or about and between March 22, 2016 and October 5, 2016, BARYSHEFF, KARPENKO, and KRUTILIN, together with others, conspired to acquire additional CCL items for the purpose of illegally exporting them.

56. On or about March 30, 2016, HSI received a report from a U.S.-based business of a suspicious request for a quote from an individual claiming to be an employee of UIP TECHNO named "David Powell." As explained below, "David Powell" was later identified by investigating agents as the electronic identity for KRUTILIN.

57. KRUTILIN (claiming to be "David Powell") specifically requested quotes from the U.S.-based company for three parts: UT69151CDXEWCX (5962R9466311QYX); UT54ACS164245SEIUCC (5962R9858006VXC); and UT6325XCC (5962R0422901QXC). These items are all integrated circuits designed for space applications.

58. Previously, on or about March 22, 2016, KRUTILIN had sent an email to the U.S.-based company indicating that his company, UIP TECHO, was working to purchase technology on behalf of a U.S.-based company located in California. Three days later, KRUTILIN provided an End Use Certificate ("EUC") which identified the California company as the end user for the parts that UIP TECHNO was attempting to purchase.

59. On or about, April 4, 2016, the U.S.-based company directed KRUTILIN, via an email communication, to an HSI undercover agent ("UC-1") who was posing as a sales representative for an independent distributor of the U.S.-based company.

i. First Order of License-Controlled Technology

60. On or about, April 5, 2016, UC-1 emailed a quote to KRUTILIN, offering to sell the three parts that KRUTILIN had previously sought to purchase from the U.S.-based company.

61. Between April 5, 2016 and April 19, 2016, UC-1 negotiated the price of the products requested by KRUTILIN. During these negotiations, UC-1 received emails from another email account associated with UIP TECHNO. Ultimately, the individual or individuals sending communications on behalf of UIP TECHNO (including KRUTILIN), agreed to purchase the following quantities of the three parts from UC-1 at the following prices:

UT69151CDXEWCX(5962R9466311QYX)	QTY: 7	$8,713.00 ea
UT54ACS164245SEI-UCC(5962R9858006VXC)	QTY: 31	$821.00 ea
UT6325XCC(5962R0422901QXC)	QTY: 11	$5,938.00 ea
	Total:	$151,760.00

62. According to a DOC license determination, two of those parts (No. UT6325XCC(5962R0422901QXC) and UT54ACS164245SEI-UCC (5962R9858006VXC)) would require an export license to Russia, while the third part (UT69151CDXEWCX (5962R94663QYX)) does not require a license for export to Russia.

63. On or about, April 21, 2016 and April 27, 2016, an individual operating an email account associated with UIP TECHNO sent emails to UC-1, indicating that UIP TECHNO had sent wire transfers for $75,880.00 and $31,000 to UC-1, as the first two payments for the parts that UIP TECHNO had ordered.

64. On or about, April 22, 2016, UC-1 informed the individual operating the UIP TECHNO email account that he/she needed to complete a new end user certification for the parts that UIP TECHNO had ordered. On that same day, the individual operating the UIP TECHNO email account responded with an end user certificate that indicated UIP TECHNO was the purchaser, and again indicated that the end user was located in California. The document contained the following language:

> "We – the person or body named in Section 1 [UIP TECHNO] – certify that we are the end-user of the goods described in Section 2, which are to be supplied by [UC-1 COMPANY]. We further certify that we shall use the goods for the purposes described in Section 3; that the goods will not be used for any purpose connected with chemical, biological or nuclear weapons, or missiles capable of delivering such weapons; that they will not be re-exported or otherwise re-sold or transferred if it is known or suspected that they are intended or likely to be used for such purposes; that the goods will not be re-exported or otherwise re-sold to a destination subject to US, UN, EU or OSCE embargo where that act would be in breach of the terms of that embargo; and that the goods, or any replica of them, will not be used in any nuclear explosive activity or unsafeguarded nuclear fuel cycle."

65. On or about, May 19, 2016, investigating agents communicated with a senior employee of the California company listed as the end user by KRUTILIN, who confirmed that the end user certificate that UIP TECHNO submitted was false. Indeed, the California company was not the ultimate consignee for the above mentioned parts, and it has never purchased parts through UIP TECHNO.

66. On or about and between August 10, 2016 and August 12, 2016, UC-1 wrote to the email address for "David Powell" at UIP TECHNO, and informed KRUTILIN that UC-1's supervisor (in actuality, a DCIS undercover agent, hereafter "UC-2") had contacted the California company given by CC-1 as the end user, and discovered that company had never heard of UIP TECHNO.

67. During that same period, UC-1 emailed KRUTILIN and told him, in sum and substance and in part, that because of the potential of making a significant amount of money, UC-1's company was considering whether or not to continue doing business with UIP TECHNO in spite of learning about the submission of fraudulent end user information. UC-1 further stated, in sum and substance and in part, that if the company provided UIP TECHNO with the parts, UC-1's company would want to be "protected" because the deal was not a "normal legal order," and that there would need to be additional compensation.

68. On August 16, 2016, KRUTILIN (identifying himself as "Powell") responded to UC-1, via a Skype text communication, and wrote, in part, "We really can make much money on such orders…We really respect you and your company…We would never tell anyone about our cooperation because it's risky for both of us. Please let us know the best way of keeping everything in secret. You said you should be compensated for the risk, please tell me how. What exactly you want us to do? I guess you would like to get an

extra cost for the parts from the order. Let's discuss it." KRUTILIN further wrote, in part "We can guarantee, we never show any invoices or emails to any legals [sic] with you. Moreover, we never had any problems, and we are trying to do everything very carefully, If you want us to get some agreement regarding covering legal cost, it might happen. We will certainly agree with that if necessary we also can do some extra cautions like wiring money not to USA. As there will be big money soon. Let me know the compensated price…"

69. On August 17, 2016, KRUTILIN (identifying himself as "Powell") spoke over the telephone with UC-2, the undercover law enforcement agent posing as UC-1's supervisor. During this call, the following conversation occurred (in sum and substance, except where quoted, and in part):

a. KRUTILIN indicated that he wanted to continue doing business with UC-1 and UC-2, and assured UC-2 that he could "protect your company not to disclose any information." KRUTILIN also stated, in part, "because, you know we are not working for the first day. We try to do it very carefully, so we can guarantee we will never show any invoices or emails to any legal persons with you and we have never had any problems regarding the orders, parts, exported parts so we are trying to do everything very carefully."

b. UC-2 told KRUTILIN that he needed a new end user statement, because they had confirmed the first one was false and this meant UC-2 could no longer deny knowledge if questioned. KRUTILIN stated he would send a new document "with an absolutely new company. Also connected to satellite development or something like that. I hope that sounds ok for you?"

c. UC-2 asked KRUTILIN where UIP TECHNO was exporting the parts. KRUTILIN stated he could not divulge the location without first getting permission from his boss. UC-2 also asked if KRUTILIN's customer "knows the process they are going through is not the legal way of doing this?" KRUTILIN indicated that they did understand this. UC-2 also stated he wanted to "make sure that you and your customer know exactly what we are doing so that you know how sensitive this is, that its not legal doing it this way so that if anyone has any problem that everyone is looking out for everyone else. So that

nothing comes back to us." KRUTILIN responded and said, "I think there is no connection with your company. If something happens, we will not tell anyone that we are connected with you. Because it is risky for both us and you, why should we do that? I think its not right, its no way, ya. Anyway, it won't happen." KRUTILIN further stated, "we do have our own network that's why we are working for so many months and years."

d. UC-2 asked KRUTILIN, "So you have been doing this same type of deal for a while then?" KRUTILIN confirmed that they had, and also stated, "We don't do this for the first time. We have a network of companies in the US and Canada. We are connected to each other and we help each other. We have agents that help with exported parts to export them to Europe. We have been working with that for several years."

e. UC-2 ended the phone conversation by stating that UIP TECHNO's order and planned export would be "violating US criminal law and I don't want any problems coming back to me or my company." KRUTILIN responded, "Ya, I understand that…I apologize I didn't get back to you earlier. I just needed time to think and discuss with my boss. So that's great. Thank you for the conversation. Have a great day."

70. On or about August 18, 2016, an individual claiming to be "Simon Fox," operating the email account "simon@uiptechno.com" emailed UC-1 and attached a new end user statement for the parts discussed by KRUTILIN. The new end user statement indicated the parts were for a different company located in California.

71. As explained below, investigating agents subsequently learned that KARPENKO was posing as Simon Fox.

72. On or about September 6, 2016, HSI shipped 7 pieces of UT69151CDXEWCX to UIP located at 2101 Avenue Z, Brooklyn, NY 11235. This part, which as noted above can be exported without a license, was shipped to UIP TECHNO for the purpose of determining the scope of the export and logistics network of the criminal conspiracy.

73. On or about September 8, 2016, UC-1 sent KRUTILIN a Skype text message that read, "We want to make sure you can get these parts out with no problem before we send the rest. If Customs or the FBI stops your package [we] will cancel the rest of the order and the other order and return your funds…If you get these parts to your customer with no problem then we know you are clean and have a good network. You need to gain [UC-2's] trust and that is not easy. You need to do things his way but once he trusts you everything will change. The alternative is to have a sloppy person that will get all of us caught and put in jail." On the same day, KRUTILIN (acting as "Powell") wrote back, "We have already shipped the package to the customer. Let's just wait. So what evidence of the delivery will you need?" UC-1 requested a tracking number.

74. On or about September 14, 2016, KRUTILIN (as "Powell") sent a Skype message to UC-1 indicating he sent the package to his customer via Scandinavian Airlines (SAS) airway bill tracking number: 117-90110845.

75. On or about September 15, 2016, investigating agents obtained shipping documents related to KRUTILIN's shipment. The documents included a shipper's letter of instruction ("SLI"), which was signed by BARYSHEFF on September 13, 2016. The SLI identified the shipper as SPECTRA. The ultimate consignee was identified as a company located in Finland. The shipping documents also included a warehouse receipt that listed the shipper as SPECTRA.

76. As noted above, based on my training and experience, I know that individuals engaged in the illegal export of licensed technology will utilize countries like Finland (which does not require the same license) as a transshipment point for items that are ultimately destined for Russia.

77. Additionally, investigating agents have learned that, in a separate investigation, HSI and DCIS undercover agents met in December 2015 with a target of the investigation who was illegally shipping controlled items from the United States to Russia. During that meeting, the target of the investigation explained to the undercover agents that he shipped them to another company in Finland where they are then smuggled into Russia without the proper export license required. Subsequently, in August 2016, HSI agents involved in this separate investigation learned, pursuant to a federal search warrant of the target's Skype account, that he had been directed to use the same Finland company used by SPECTRA and UIP TECHNO to transship controlled technology to Russia.

ii. Second Order of License-Controlled Technology

78. On May 17, 2016, KRUTILIN (acting as "Powell") sent a request for a quote to UC-1 for two satellite components (161 of one, and 29 of another) manufactured by a U.S. company. As with the first order by KRUTILIN, these items are integrated circuits intended for space applications.

79. According to a DOC license determination, both parts would require an export license to Russia.

80. On May 24, 2016, UC-1 provided a quote of $61,960.00 for the parts. On June 23, 2016, UC-1 received an email from "Irene Mitchel, Purchasing Specialists," using the email address "Irene@UIPTechno.com." The individual operating that email address indicated that he or she was ready to place an order for these parts, and attached a purchase order for quantities of 172 and 36 of the parts, as well as a sales contract. The sales contract identified BARYSHEFF as the "Buyer" and as the "General Manager."

81. On June 29, 2016, UC-1 emailed Mitchel a proforma invoice which included the new order price for the increased quantity. The value of the order was $68,000.00.

82. On July 8, 2016, Mitchel emailed UC-1 a copy of a wire transfer document, which showed that a wire transfer for $68,000.00 was sent from UIP TECHNO to UC-1.

83. On July 11, 2016, UC-1 emailed a blank end use certificate to the individual or individuals at UIP TECHNO he was communicating with, and informed UIP TECHNO the document must be completed before the parts are ordered. The email to UIP TECHNO specifically read: "I have attached your invoice showing you have paid in full. **Since these parts are export controlled, I will need to provide an EUC when I place the order to show they are being used in the US.** I have attached the EUC but you can also find it on our website under the documents tab. **If these parts are being exported, I will also need a BIS711, which is also on our website, in order to start the BIS export license application.**" (emphasis added).

84. On July 12, 2016, "Mitchel" emailed UC-1 the completed end user certification. The document indicated UIP TECHNO was the consignee and the end user was identified as a company in California.

85. On July 12, 2016, UC-1 emailed Mitchel and KRUTILIN an order acknowledgement. The document showed the parts were ordered and also identified they were export controlled by the DOC. Mitchel responded to the email and requested that UC-1 correct the quantity from 32 to 36.

86. On July 27, 2016, a DCIS agent sent a package via FedEx to UIP TECHNO at the company address in Brooklyn, New York, which contained a cashiers check (a purported "rebate check") for $1,944.00, a copy of the signed contract, a pamphlet for UC-1's purported business, and a toy rocket with UC-1's purported business logo. According to the delivery receipt the package was delivered to UIP TECHNO on August 28, 2016 at 2:30 p.m., and signed for by "A.LEX." Surveillance of UIP TECHNO at that time and date indicated the only person at that address was BARYSHEFF.

87. On July 28, 2016, the check was deposited into a Capital One Bank business checking account. According to records obtained from Capital One Bank, the authorized signer for the Capital One account is BARYSHEFF.

88. On July 29, 2016, UC-1 emailed Powell, Mitchel, and Fisher and informed them the delivery receipt showed the FedEx package was received by "A.LEX." UC-1 asked if they had in fact received the check. On August 1, 2016, Mitchel responded to the email and wrote, "We received the check." Mitchel also emailed UC-1 a copy of the contract. The contract was signed by BARYSHEFF.

iii. Identification of KARPENKO and KRUTILIN

89. On or about September 20, 2016, UC-1 and KRUTILIN (acting as "Powell") engaged in a Skype text conversation.

90. KRUTILIN told UC-1 that "We are planning several meetings in the USA very soon. And we would like to meet with you in Colorado" in order to "discuss all current issues and orders." KRUTILIN also told UC-1 that they planned to come to the state where the UC-1 business was located on October 5, 2016.

91. In response, UC-1 stated, in sum and substance and in part, that they were interested in meeting, and suggested that KRUTILIN could pick up the second order of license-controlled parts described above as part of the trip. KRUTILIN agreed that they would take possession of the parts when they met.

92. On or about September 22, 2016, KRUTILIN and UC-2 (UC-1's "supervisor" in the business) engaged in a follow-up telephone conversation that was recorded. During this telephone conversation, KRUTILIN (claiming to be "Powell"), stated the following, in sum and substance and part: (1) he was still planning to come for a meeting on October 5, 2016; (2) he would be coming with "Simon, the head of the department;" and (3) they had meetings with other suppliers in in other states.

93. Based on prior communications, investigating agents believe the "Simon" referenced by KRUTILIN is the person claiming to be Simon Fox in previous communications, and who investigating agents later determined to be KARPENKO.

94. Additionally, KRUTILIN asked when UC-1 would send the remainder of the first order of license-controlled parts that are described above. UC-1 stated "I have another customer that was working on getting stuff to the same place that you are sending the things and he did a lot of things that screwed things up so that we had problems with customs and commerce. And they started asking questions. So everything they were doing is focused on everything that he has done and his network of things so that is why I am being as cautious as I can I want to make sure that nothing comes back to me…" and also suggested that they pick up these license-controlled parts in person as well. KRUTILIN responded "Oh that would be also great, because that's kind of more comfortable for both you and us and not so dangerous. I would say, right?"

95. As part of the investigation, law enforcement agents obtained information from a law enforcement database indicating that, on or about October 1, 2016, KARPENKO, a 33-year-old Russian citizen, and KRUTILIN, a 27-year-old Russian citizen, arrived at John F. Kennedy International Airport ("JFK") in Queens, New York, aboard a flight from Russia. Law enforcement agents also learned that KARPENKO and KRUTILIN were scheduled to return to Russia on or about October 7, 2016.

96. On or about October 4, 2016, UC-2 received a Skype message from KRUTILIN (as "Powell") stating "Hi Robert! Me Simon will be in Colorado Springs tomorrow around 11:30 AM, pls confirm is this is ok for you? You can also advise convenient place to meet. I've tried to call your mobile, but nobody pick up the phone, my Mobile is 347-337-6250. Pls call me back at your convenience." UC-2 called the phone number later on that same date, spoke to KRUTILIN (as "Powell"), and confirmed the meeting that they were still meeting on October 5, 2016.

97. As part of the investigation, investigating agents discovered that KARPENKO and KRUTILIN took a domestic flight to Denver, Colorado on or about October 3, 2016, and rented a vehicle.

98. On or about October 4, 2016, KARPENKO and KRUTILIN attempted to enter Peterson Air Force Base in Colorado Springs, Colorado. After interacting with U.S. military security, KARPENKO and KRUTILIN left the base.

99. Subsequently, investigating agents learned from U.S. military security that KARPENKO and KRUTILIN had attempted to gain access to Peterson Air Force Base, and that security had denied them access. Military security provided investigating agents with copies they had made of Russian passports provided by KARPENKO and KRUTILIN

when they tried to gain access, which were in their respective names. Security also provided a copy of a business card that was found along with the passports; the business card was for "David Powell" of UIP TECHNO.

100. On or about October 5, 2016, UC-2 and another law enforcement officer acting in an undercover capacity as involved in "logistics" for the purported business ("UC-3") met with KARPENKO and KRUTILIN. At this meeting, KARPENKO identified himself as "Simon Fox" and KRUTILIN identified himself as "David Powell," and both confirmed that they were the same individuals who had previously been communicating with UC-1 and UC-2. Further, UC-2 recognized KRUTILIN's voice as "David Powell" from prior telephone conversations. Both KARPENKO and KRUTILIN spoke conversant English, and the undercover law enforcement officers had no difficulty understanding either of them.

101. During the same meeting, in sum and substance and in part, UC-2 and UC-3 told KARPENKO and KRUTILIN that they were nervous about the plan to provide them with these items, that the technology was typically used for satellites, and that it would be illegal to export them without a license. UC-2 and UC-3 further stated that they understood that KARPENKO and KRUTILIN planned to export these items, and that the ultimate destination was Russia. KARPENKO and KRUTILIN both smiled and nodded affirmatively in response.

102. During the same meeting, UC-2 provided KARPENKO and KRUTILIN a document, which UC-2 explained in sum and substance was to protect the UC's business. The document was a letter to Simon Fox, which stated, in part that UIP TECHNO "will not export these devices unless all export documents and/or approved export

license is received for this order" and that the "devices may not be transferred, transshipped on a non-continuous voyage, or otherwise be disposed of in any other country, either in their original form or after being incorporated into other end-items, without the prior written approval of the U.S. Department of Commerce." UC-2 and UC-3 observed KARPENKO review the document, and sign it as "Simon Fox."

103. During the same meeting, UC-2 and UC-3 made reference to BARYSHEFF. In response, KRUTILIN stated, in sum and substance and in part, that BARYSHEFF was the "CEO" of UIP TECHNO, but that UC-2 and UC-3 would be dealing directly with KRUTILIN and KARPENKO. In sum and substance, KARPENKO agreed with this statement.

104. During the same meeting, UC-2 and UC-3 offered to send the purported license-controlled parts to the UIP TECHNO address in Brooklyn, New York, and KARPENKO and KRUTILIN agreed. KARPENKO and KRUTILIN explained to UC-2 and UC-3, in sum and substance, that the devices would remain in New York for approximately four-to-five days, then be shipped to Finland by way of Canada or Mexico. They further stated, in sum and substance, that they changed their shipping routes frequently to avoid detection.

III. CONCLUSION

105. Based on my training and experience, as well as the facts set forth in this affidavit, there is probable cause to believe that the defendants DMITRII ALEKSANDROVICH KARPENKO also known as "David Powell," and ALEXEY KRUTILIN, also known as "Simon Fox," together with others, did knowingly, intentionally and willfully export, and attempt to export, from the United States to Russia items on the

United States Commerce Control List, to wit: (i) five (5) digital-to-analog converters; (ii) one-hundred and fifty (150) integrated circuits; (iii) forty-two (42) integrated circuits; and (iv) two-hundred and eight (208) integrated circuits, without first having obtained a license from the Department of Commerce, in violation of Title 50, United States Code, Section 1705 and Title 18, United States Code, Section 2, and conspired to do the same in violation of Title 18, United States Code, Section 371.

106. It is respectfully requested that this Court issue and order sealing, until further order of the Court, all papers submitted in support of this application, including the application, the arrest warrant, and the complaint. I believe that sealing these documents is necessary because the defendant is currently at liberty and is believed to reside outside of the United States, and the government plans to effectuate an arrest when the defendant next enters the United States and/or seek extradition if the defendant is arrested in another country. Thus, the government seeks to seal the complaint and arrest warrant to ensure that the defendant does not learn that a complaint has been filed and an arrest warrant has been issued, and to prevent her from fleeing justice and avoiding arrest and prosecution.

WHEREFORE, your deponent respectfully requests that an arrest warrant be issued, and that the defendants DMITRII ALEKSANDROVICH KARPENKO also known as "David Powell," and ALEXEY KRUTILIN, also known as "Simon Fox," be dealt with according to law.

SUSAN RUIZ
Special Agent
Department of Homeland Security
Homeland Security Investigations

Sworn to me before this
5 day of October, 2016

S/ Roanne Mann

THE HONORABLE ROANNE L. MANN
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK