



**U.S. Department of Justice**

*United States Attorney  
Eastern District of New York*

DMB:DSS/HLJ/DR  
F.#2012R00387

271 Cadman Plaza East  
Brooklyn, New York 11201

October 3, 2012

By ECF

The Honorable George C. Hanks, Jr.  
United States Magistrate Judge  
Southern District of Texas  
515 Rusk Avenue  
Houston, TX 77002

Re: United States v. Alexander Fishenko, et al.  
Criminal Docket No. 12-626 (SJ) (E.D.N.Y.)

Dear Judge Hanks:

The government submits this letter in support of its motion for a permanent order of detention with respect to defendants Alexander Fishenko, Alexander Posobilov and Viktoria Klebanova (collectively, the "defendants") in the above-captioned case. The defendants are scheduled to appear before the Court today for arraignment on a 25-count indictment charging them with, inter alia, exporting advanced microelectronics to Russia, including to Russian military and intelligence agencies, without obtaining required licenses, in violation of the Arms Export Control Act ("AECA") and the International Emergency Economic Powers Act ("IEEPA"). All three defendants are also charged with obstruction of justice, and Fishenko is charged with acting as an unregistered agent of the Russian government by illegally procuring these technologies. For the reasons set forth below, defendants Fishenko, Posobilov and Klebanova pose a significant risk of flight, and therefore no combination of bail conditions would ensure their continued appearance.

I. Background

A. The Scheme

The investigation that gave rise to the instant charges began in approximately July 2010, and has involved extensive court-authorized electronic surveillance of the defendants' telephone and email communications. The investigation has revealed that Fishenko acted as an agent of the Russian government by illegally procuring sophisticated microelectronics for Russian government agencies, including military and

intelligence agencies, through his Houston-based corporation Arc Electronics, Inc. ("Arc"), of which he is President and Chief Executive Officer. For national security reasons, the export of these microelectronics is controlled by the Department of Commerce ("DOC") and the Department of State. The microelectronics, which included microcontrollers, microprocessors, static random access memory chips and analog-to-digital converters, have applications in a wide array of military systems, including radar and surveillance systems, missile guidance systems and detonation triggers. An analysis of publicly available information reveals that Russian-made anti-ship missiles, as well as the developmental iteration of the MiG 35 fighter jet, use U.S.-origin memory chips and microprocessors similar, and in some cases identical, to those supplied by the defendants. The Russian military is currently undergoing a large-scale modernization campaign, and many of the sophisticated electronics necessary for electronic weapons systems, including those exported by the defendants, cannot be purchased in Russia and often can only be purchased from United States-based companies.

Communications intercepted during the investigation revealed that a large portion of the technology exported by the defendants was destined for Russian military and intelligence agencies. Indeed, an analysis of Arc's accounting data revealed a striking similarity between fluctuations in Arc's gross revenues and the Russian Federation's defense spending over the last several years. In addition, a letter recovered during the course of the investigation revealed that the end user of the electronics exported by Arc was the Federal Security Service ("FSB"), Russia's domestic intelligence agency (attached hereto as Exhibit A). Specifically, an FSB electronics production laboratory sent the letter complaining that certain microchips purchased from Arc through an affiliate of defendant Apex System, L.L.C. ("Apex"), a Moscow-based firm of which Fishenko is also a principal, were defective and needed to be replaced. The Apex affiliate then forwarded the letter to Arc for replacement of the microchips.

Fishenko conducted this illicit procurement activity through Arc, a Houston-based corporation owned by Fishenko and his wife, and through Apex. In addition to Fishenko, seven Arc employees have been charged with a variety of export violations and related offenses. During the time period of the conspiracy, Posobilov acted as Arc's director of procurement, and Klebanova was an Arc salesperson. The investigation has revealed that the defendants systematically evaded export laws and defrauded U.S. manufacturers and suppliers by lying about the actual end users and intended applications of the microelectronics they sought to

purchase. In addition, Arc often concealed its function as an exporter and re-seller, falsely claiming on its website and directly to suppliers that it manufactured benign commercial products such as traffic lights, when in fact it manufactured no goods whatsoever.

Arc has been in operation since at least 1998. Since 2002, Arc has earned approximately \$50 million in gross revenue by exporting microelectronics and other advanced technology to Russia. Although Arc has sent hundreds of shipments containing thousands of controlled parts to Russia, neither Arc nor its associated entities, principals and employees have ever obtained an export license from the DOC or the Department of State.

Arc typically received requests for microelectronics and other high-tech goods from Russian procurement firms via email. Arc employees then contacted various U.S.-based manufacturers and distributors (the "suppliers") via email to inquire about price and availability of the desired goods. When the suppliers responded, they often notified Arc if the item was subject to export controls and also requested end use information, including the identity of the ultimate recipient of the technology and the nature of the intended application. Arc often provided false end use information to induce the suppliers to sell the requested components and to avoid further scrutiny. In addition, Arc often sent the components to Russia via transshippers located in Finland, Canada and Germany, and obtained payments from Russian procurement firms via wire transfers through shell companies located in countries such as the British Virgin Islands, Panama and Belize. Arc's principal port of export during the course of the conspiracy was John F. Kennedy International Airport in the Eastern District of New York.

#### B. Obstruction of Justice

In August and September 2011, Fishenko, Posobilov, Klebanova and others obstructed an anticipated DOC inquiry by falsifying documents and deleting records pertaining to two shipments of controlled transistors to Apex. Following the two exports at issue, the manufacturer requested verification that the parts were sent to the end user provided. Recorded communications reveal that, when pressed, Fishenko made conflicting statements regarding the application of the parts. Fishenko ultimately claimed that the parts were intended for a Russian ground-based GPS system that would check for vehicles on a civilian airport runway. After several attempts to understand the actual end use of the parts, and the nature of the end users, the manufacturer advised Fishenko and Posobilov that it would be

filing a Voluntary Self Disclosure ("VSD") with the DOC regarding the illegal export of these parts and recommended that ARC do so as well.

Subsequently, Fishenko, Posobilov and Klebanova began an extensive effort to falsify documents and other items relating to the transactions in preparation for the VSD and a potential investigation by the DOC. Shortly after the initial call with the manufacturer, Posobilov spoke to co-defendant Dmitriy Shegurov, an Apex executive. Posobilov asked Shegurov if the end user Arc had previously provided, "Experimentalny Zavod," was real. Shegurov said he would check, and explained that "they" bought the components under the name of a "layer" company. Shegurov told Posobilov that he would "explore the ground to make it look real if all of it is a lie, or will take contact information if all of it is true." Posobilov responded that they didn't have another choice, because "if they start providing a different end user they will be f\_cked." That same day, Fishenko emailed co-defendant Sergey Klinov, the CEO of Apex, and requested that he provide backdated documents pertaining to the transaction, as well as a letter from Experimentalny Zavod affirming that the components were used for a civilian application. Fishenko further directed Klinov to remove all references to the Russian military from Apex's website "especially from the English section." Thereafter, Fishenko and Shegurov created a false end user certification purporting to be from Experimentalny Zavod. In addition, Apex's website was changed to remove references to the Russian military, including images of missiles and military aircraft, as well as a certificate stating that Apex's affiliate Arsenal was a certified supplier of electronics to the Russian Ministry of Defense (attached hereto as Exhibit B).

On August 19, 2011, in a telephone conversation with an Arsenal employee, Klebanova told the employee that all emails from Arsenal had been deleted and that Arsenal should not be mentioned in any future emails to Arc. On September 30, 2011, Klebanova reiterated this warning in an email to multiple Apex and Arsenal employees, and requested that they not reference anything to do with the Russian military in future emails. On September 27, 2011, ARC filed a VSD with the DOC, which was signed by Fishenko.<sup>1</sup> The VSD falsely stated: "Since delivery, we understand that the [p]roducts have remained under the control of

---

<sup>1</sup> Although Arc styled its submission as a "Voluntary Self Disclosure," as noted above Arc filed the submission only after having been informed by the manufacturer that the manufacturer intended to submit a disclosure regarding these transactions to the DOC.

the intended end-user, and have been used only to produce civil inland radar airport traffic control systems." However, as set forth above, Fishenko had actively fabricated the end use documentation for the shipments and knew that the statements in the VSD were false.

## II. The Indictment

On September 28, 2012, a grand jury in the Eastern District of New York returned an indictment charging Arc, Apex, Fishenko, Posobilov and Klebanova, along with eight co-defendants, with conspiring to violate IEEPA and AECA, and to commit wire fraud, in violation of 18 U.S.C. § 371. Fishenko, Posobilov and Klebanova were also charged with multiple substantive IEEPA violations, in violation of 50 U.S.C. § 1705, and obstruction of justice, in violation of 18 U.S.C. § 1512(c). Finally, Fishenko was charged with a substantive AECA violation, in violation of 22 U.S.C. §§ 2778(b)(2) and 2778(c), conspiring to commit money laundering, in violation of 18 U.S.C. §§ 1956(a)(2)(A) and (h), and acting as an unregistered agent of the Russian government, in violation of 18 U.S.C. § 951.

## III. Argument

Fishenko, Posobilov and Klebanova each have strong ties to Russia and pose a significant risk of flight if they were to be released pending trial. Pursuant to the Bail Reform Act, 18 U.S.C. §§ 3141, et seq., the Court may order a defendant detained pending trial upon a determination that the defendant is either a danger to the community or a risk of flight. See 18 U.S.C. § 3142(e) (detention appropriate where "no condition or combination of conditions would reasonably assure the appearance of the person as required and the safety of any other person and the community"). A finding of risk of flight must be supported by a preponderance of the evidence. See United States v. Fortna, 769 F.2d 243, 250 (5th Cir. 1985); United States v. Chimurenga, 760 F.2d 400, 405 (2d Cir. 1985). The Bail Reform Act specifies four factors to be considered in the detention analysis: (1) the nature and circumstances of the crimes charged; (2) the history and characteristics of the defendant; (3) the seriousness of the danger posed by the defendant's release; and (4) the evidence of the defendant's guilt. See 18 U.S.C. § 3142(g). In the instant case, consideration of the factors under the Bail Reform Act warrants detention.

As to the first factor, the offenses charged in the indictment involve conduct that directly impacts the national security of the United States. In addition, the defendants face substantial sentences. If convicted of the charges currently

pending against them, the defendants face up to 5 years' imprisonment for conspiracy, 20 years' imprisonment for each substantive export violation and 20 years' imprisonment for obstruction of justice. Fishenko also faces up to 20 years' imprisonment for money laundering, and up to 10 years' imprisonment for acting as an unregistered agent of the Russian government. The government estimates that Fishenko faces a U.S. Sentencing Guidelines range of 121-151 months' imprisonment, based solely on the export violations, obstruction of justice and role enhancements. The government estimates that Posobilov's Guidelines range is 108-135 months' imprisonment and Klebanova's Guidelines range is 78-97 months' imprisonment.

Moreover, as evidenced by their obstruction of justice, the defendants have demonstrated their willingness and ability to impede the judicial process. Accordingly, upon their release they are likely to disregard any conditions of bail set by the Court and attempt to collude with co-conspirators or destroy or conceal evidence. Finally, as set forth in greater detail below, each of the defendants has substantial ties to Russia, and the evidence of their guilt is overwhelming.

A. Alexander Fishenko

1. Fishenko's Ties Abroad Render Him a Significant Flight Risk

Fishenko was born in what was, at the time, the Soviet Republic of Kazakhstan, and graduated from the Leningrad Electro-Technical Institute in St. Petersburg, Russia. He immigrated to the United States in 1994, and initially worked at a Circuit City in the Houston area. In 1998, he founded Arc in Houston. Fishenko became a naturalized citizen of the United States in 2003. Notably, in his initial asylum application Fishenko stated that he had no prior military experience. However, he claimed elsewhere that he served in a Soviet military intelligence unit in Berlin in the 1980s. Although he has lived in the United States since he immigrated, Fishenko has maintained significant and continuing ties with Russia.

Fishenko has valid Russian and U.S. passports and travels overseas frequently. Indeed, Fishenko has travelled abroad every year since at least 1996, and typically makes two to three international trips per year. Overall, Fishenko has traveled to Russia and/or Europe twenty-six times since 1996. In fact, Fishenko just returned from a two-week trip to Russia on September 24, 2012. In addition, Fishenko has significant ongoing personal and professional ties with Russia. He is in frequent email and telephone contact with over a hundred business

associates at procurement firms located in Russia. Fishenko's mother and sister currently live in Kazakhstan. Fishenko's wife, who is co-owner of Arc and also a naturalized U.S. citizen from Russia, also holds a valid Russian passport.

As set forth above, in addition to owning and operating Arc, Fishenko is also part owner of Moscow-based Apex. While the investigation has revealed that Fishenko derives substantial income from Apex's operations, he appears to maintain those assets in Russia. For example, on September 23, 2011, Fishenko spoke via telephone to two Apex employees regarding a recent visit to Moscow. Fishenko stated that "his annual visit encouraged people in all departments to compile reports" and that he "expected reports to be ready for his visit." Fishenko complained that he was owed a large amount of money from Apex and couldn't "be Apex's sponsor any longer." In addition, on November 1, 2011, Fishenko sent an email to another Apex employee stating that he was owed \$10,000 in dividends and \$30,000 from certain orders and instructed the employee to put \$10,000 on his "card" and \$30,000 into his personal account. Based on the context of these conversations and an analysis of Fishenko and Arc's domestic bank accounts, it appears that much of the income derived from Apex's operations has not been transferred to the United States. In addition, Fishenko maintains bank accounts in Singapore. Fishenko's access to funds overseas increases the likelihood that he will attempt to flee.

## 2. The Evidence of Fishenko's Guilt is Overwhelming

During the course of the investigation, hundreds of Fishenko's pertinent email and telephone communications have been recovered. These communications constitute devastating evidence of Fishenko's illegal procurement for the Russian government. Fishenko has made many statements indicating his intent to evade U.S. export controls and to obfuscate the true end use and end users of the microelectronics he exported.

For example, on September 24, 2009, Fishenko engaged in an email exchange with an employee of a Russian procurement firm. Fishenko requested that the employee get an end user document from a Russian factory "in a more presentable format." The next day, the employee responded and attached a new end user statement, explaining, "This letter is pure forgery. I made it using a copy machine." This pattern of blatant fraud continued for years. On January 19, 2012, Fishenko discussed obtaining controlled components with another electronics broker. Fishenko stated that he had not attempted to apply for an export license because he did not want to invite scrutiny. Fishenko told the distributor that, if he did apply for a license, the response

might be "Sure, you can sell it, but we will keep an eye on you." Fishenko added, "Well, seriously. Why would I do that?" In addition, on January 27, 2012, Fishenko spoke via telephone with an employee at another Russian procurement firm, and asked him to avoid informing Arc employees when the Russian company falsified end user information. Fishenko stated, "[i]f you are making it up, make it up pretty, correctly, and make sure it looks good."

Fishenko has also repeatedly tried to conceal Arc's procurement function for the Russian military. For example, on March 23, 2012, Fishenko directed an employee of a Russian procurement firm to "make sure that our guys don't discuss extra information, such as this is for our military client." In addition, Fishenko has referenced his ties to Russia's intelligence services. For example, in an October 24, 2011 conversation with another Russian electronics broker, Fishenko and the broker discussed an individual who worked at the broker's firm who, they believed, had been an intelligence officer with the FBI. Fishenko stated that the man was "our [type of] person, 'zakinuty kazachok.'" "Zakinuty kazachok" (literally "thrown Cossack") is a Russian colloquialism for "spy" or "secret agent."

Finally, no bail package could adequately secure Fishenko's release. Fishenko's U.S. properties and his domestic bank accounts are subject to forfeiture as proceeds of these offenses. Therefore, posting these properties as collateral for a bond would provide little assurance of Fishenko's continued appearance.

## B. Alexander Posobilov

### 1. Posobilov's Ties Abroad Render Him a Significant Flight Risk

As the procurement manager of Arc, Posobilov had day-to-day supervisory control over Arc's illicit business activities. Notably, Posobilov was arrested on October 2, 2012 immediately prior to boarding a flight to Singapore en route to Hong Kong and, ultimately, Russia. Posobilov entered the United States in 2001 and became a naturalized U.S. citizen in 2008. He joined Arc in 2004. Posobilov traveled to Russia twice in 2012. Posobilov has a former wife and daughter who live in Azerbaijan, and a daughter in Italy, and previously held a passport from Azerbaijan. If Posobilov were placed on electronic monitoring, that monitoring would not prevent him from fleeing the country, but would merely notify the Pretrial Services Agency that Posobilov had fled after he had done so. Moreover, there is an Azerbaijani embassy in Mexico, and if Posobilov were to flee



there, he could obtain--or renew--his passport and travel from there to Russia, Azerbaijan or elsewhere.

2. The Evidence of Posobilov's Guilt is Overwhelming

Posobilov has also made explicit statements that demonstrate his intent to evade export laws and defraud suppliers. For example, on April 4, 2011, Posobilov exchanged emails with a U.S. vendor regarding an order for certain parts. Posobilov indicated that the parts were for "fishing boat radar equipment" and provided the name and address of a Russian end user. The vendor informed Posobilov that the requested parts required an export license for Russia and indicated that, therefore, the vendor would need a more complete end use statement. Posobilov then forwarded this exchange to the Russian procurement firm, instructing them to coach the end user to complete the end use declaration in such a manner as to facilitate obtaining the controlled component. Posobilov wrote, "[m]ake sure that those are fishing boats, and not fishing/anti-submarine ones... Then we'll be able to start working." In addition, in a telephone conversation on November 3, 2011 with an employee of a Russian procurement firm, Posobilov stated that a U.S. vendor had requested end user information for a particular order. The procurement agent replied that it would be "difficult to provide" such information because his client was "a serious military enterprise." The procurement agent further explained that the part was an electronic filter to be used in a "training simulator." Posobilov then responded that he had "an end user for this kind of thing" and he would provide an end user himself.

C. Viktorina Klebanova

1. Klebanova's Ties Abroad Render Her a Significant Flight Risk

Klebanova also has significant incentive to flee given the penal consequences she faces and her strong ties to Russia. Klebanova is also a naturalized U.S. citizen from Russia, maintains a valid Russian passport and her mother currently lives in Russia. Klebanova traveled to Russia as recently as 2011. Like Posobilov, if Klebanova were on electronic monitoring, that monitoring would not prevent her from fleeing the country, but would merely notify the Pretrial Services Agency that she had fled after she had done so.

2. The Evidence of Klebanova's Guilt is Overwhelming

As with Fishenko and Posobilov, the evidence against Klebanova is overwhelming and includes extensive electronic surveillance. Klebanova has made multiple statements indicating her intent to evade U.S. export controls and her willingness to break the law. As set forth above, Klebanova obstructed justice by repeatedly advising Apex personnel to scrub their emails of military references. Specifically, Klebanova noted that she would be forced to delete any emails that referenced the military from her inbox "so there would not be any history."

On multiple occasions, Klebanova explicitly described Arc's scheme to evade export laws during intercepted exchanges. For example, on March 9, 2012, Klebanova and an employee of Apex exchanged emails, which were copied to Fishenko and Posobilov, in which Klebanova stated, "the problem is that the [U.S.] manufacturer forbids [U.S. electronics suppliers] from selling their products to us . . . however there is one 'but,' if there is a stock/price listed on the website, then both distributors will 'close' their eyes and let us buy the parts via the internet." Similarly, on March 14, 2012, Klebanova replied to an email from an employee of a Russian firm who had asked why Arc did not provide a quote on a particular component. Klebanova responded by explaining, "Unfortunately, [the U.S. suppliers] have a requirement from a manufacturer that bans them from selling . . . positions to us because we export everything. This problem existed for years and we haven't been able to do anything about it yet. However, if you can see prices and stock on the sites of both manufacturers, they 'look the other way' and let us buy positions online. But, just to reiterate - if some of the info is missing on the web-site, there is no sense in requesting anything- they will refuse [to sell]."

Given the overwhelming evidence against Klebanova, her history of obstruction and her strong ties overseas, a permanent order of detention is warranted.

IV. Conclusion

For the reasons set forth above, the government respectfully requests that the Court enter a permanent order of



Утверждено  
Начальник ОМТО в/части 35533  
С.В. Багалин  
«18» 02 2011 года

АКТ

Технического состояния микросхем ADG819BRT,  
закупленных в ЗАО «Арсенал».

Бойсковая часть 35533 в ноябре месяце 2010 года в фирме «Арсенал»  
закупила 320 микросхем ADG819BRT (счет 105.06.1).

В процессе монтажа и проверки изделий была выявлена  
неработоспособность данных микросхем, чем была вызвана необходимость  
технического исследования.

В результате визуального и рентгеновского исследования было  
установлено следующее:

1. Все 320 микросхем имеют маркировку на лицевой стороне SNB.
  2. На обратной стороне микросхем данного типа маркируется номер партии. Номер партии у всех микросхем в одной партии должен быть одинаковым. На самом деле на 14 демонтированных микросхемах имеется маркировка - 0513, 0437, 0438, 0417, 0448, 0443, 0428, 0426.
  3. В ходе рентгенографического исследования 14 демонтированных микросхем выявлено отсутствие следов сварки выводов на части микросхем (фотографии прилагаются).
- В результате выше изложенного можно сделать вывод, что партии в 320 микросхем является контрафактной и подлежит замене у поставщика.

Председатель комиссии

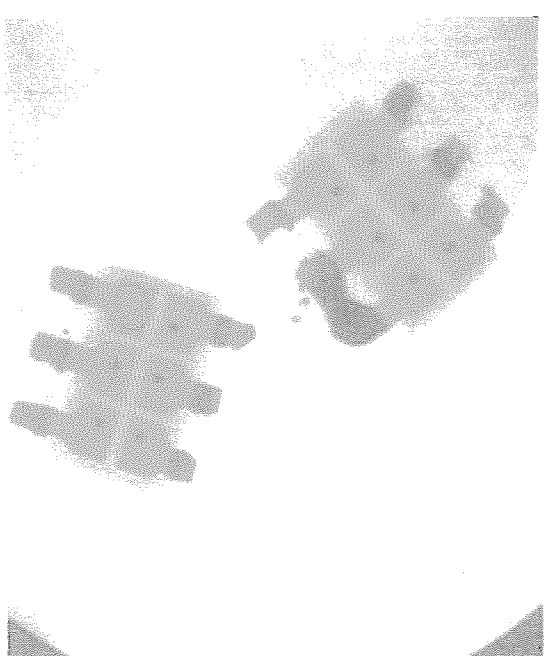
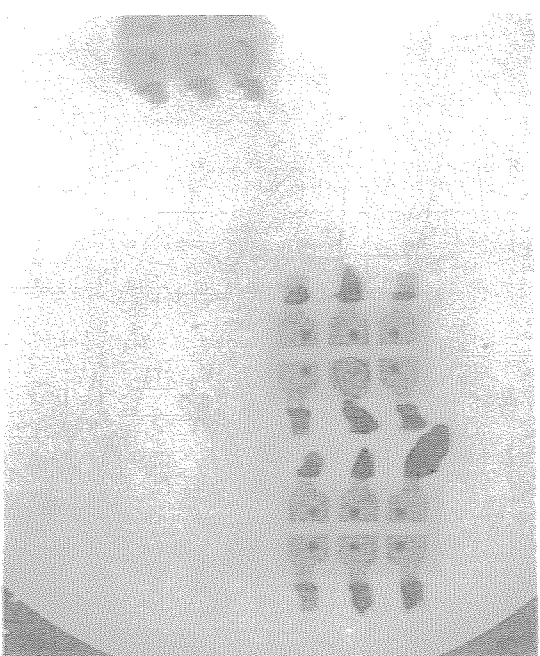
В.М. Евтисов

Члены комиссии

А.А. Петровичев

З.И. Ручаева

*(Handwritten signatures and numbers)*  
270211



Approved by  
S. V. Balanin,  
OMTO Head of military division 35533  
On 07/27/2011

Findings regarding the technical condition of  
ADG819BRT microchips purchased from JSC Arsenal.

In November of 2010 Military Installation # 35533 has purchased 329 microchips ADG819BRT from Arsenal company (account 105.06.1).

During installation and testing of the products it has been determined that the microchips do not work, therefore a technical assessment was initiated.

The following was determined as a result of a visual and an x-ray assessments:

1. All 320 microchips have marking "SNB" on the front side .
2. The batch number for the this kind of microchips is marked on the back side. The batch number should be the same for all microchips on one tape. In reality, 14 dismantled microchips have the following markings: 0513, 0437, 0438, 0417, 0448, 0443, 0428, 0426.
3. During the x-ray assessment of the 14 dismantled microchips no signs of welding of the outputs to the parts of microchips were found (photos are attached).

As a result of the above findings the conclusion was made that batch 32D of the microchips is defective and needs to be replaced by the supplier:

Committee Chair	[Signature]	V.M. Yevitsov
Committee Members	[Signature]	A.A. Petrovichev
	[Signature]	Z. I. Ruchayeva



System of Voluntary Certification  
of the radio-electronics, electric radio products and materials for military use  
“VOYENELECTROCERT”  
# *POCC RU*, 0001, 04 UT 000

---

THE CENTRAL AGENCY OF THE “VOYENELECTROCERT” SYSTEM  
FSE “22 CISRT of the Russian Ministry of Defense”

---

THE CERTIFICATE

Mytishchi City. #. SVS.01.423.0710.08, dated 5/19/2008.

is issued to the Joint Stock Company (closed type) “Arsenal”  
26 General Belov Street, office 19, Moscow, 115583.  
(full address)

This is to certify that the elements of the quality systems and performed functions  
meet the requirements of the GOST RV 20.57.412 and RD V 319.010  
(partially applicable to the basic elements of purchasing/supply products)

The company has rights to purchase and deliver foreign and domestic products for  
assembling of the military use machinery as a secondary supplier of the articles listed in  
Addendum (integral part of this Certificate.)

Valid until 05/19/2009.

Head of the Central Agency  
“Voyenelectroncert” System

Seal

[Signature]: A.A. Borisov.

FSE Chief of “22 CISRT  
of the Russian Ministry of Defense”