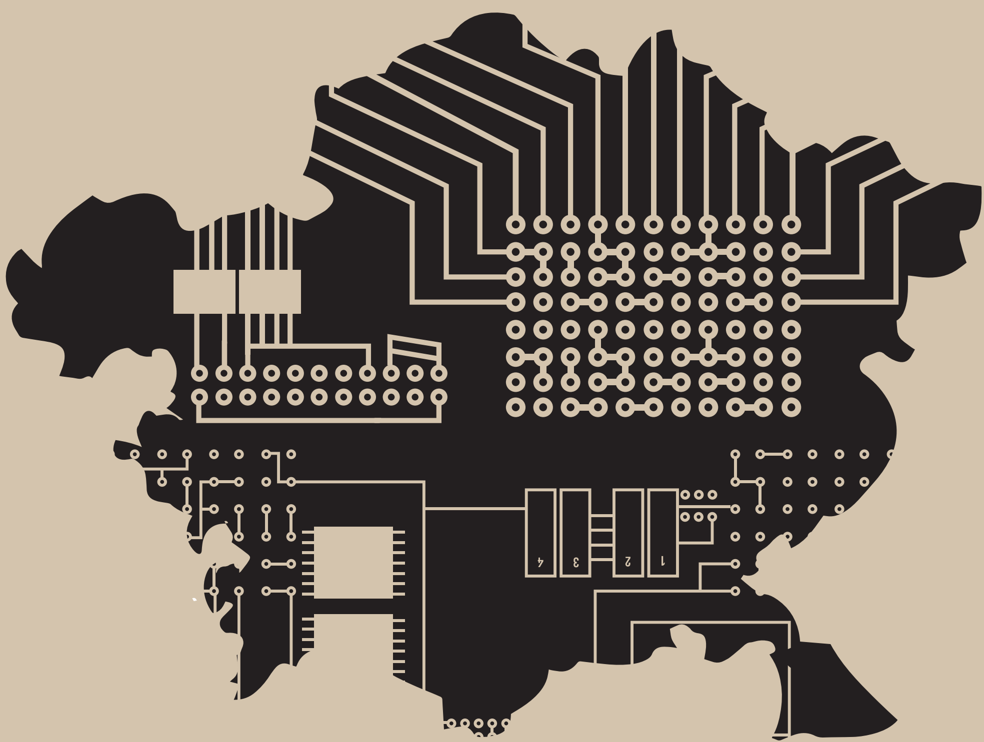
PRIVACY INTERNATIONAL

Private Interests: Monitoring Central Asia

Special Report



Private Interests: Monitoring Central Asia

November 2014

Privacy International would like to thank all those involved in the development of this report, including Andrei Soldatov for his technical advice, Scott Newton for his legal analyses, Citizen Lab, Open Society Foundations for their generous funding of this report, and all the individuals who shared their experiences, despite concern of reprisals, for making this report possible.

PRIVACY INTERNATIONAL

www.privacyinternational.org


עזרה ראשונה
Facing an Ethical Dilemma or
Corporate Responsibility Concern?
INTEGRITY • HUMILITY • PASSION • TRANSPARENCY • INNOVATION
THE VERINT WAY • THE VERINT CODE OF CONDUCT
Information Security • Fraud • Theft
Data Privacy • Health & Safety
Conflicts of Interest • Gifts & Entertainment
Environment • Discrimination • Harassment • Violence
Or any Other Illegal or Unethical Workplace Conduct
DISCUSS YOUR ISSUE WITH YOUR SUPERVISOR OR
CONTACT A VERINT RESOURCE LISTED ON THE GLOBAL CORPORATE RESPONSIBILITY PORTAL PAGE OR
ACCESS THE VERINT ETHICS HELPLINE:
Call the respective toll-free number listed under Reporting Complaints and Concerns on the Corporate Governance page of the Verint intranet at http://innervision
Verint.EthicsHelpLine.com
VERINT
URCR@Verint.com
Corporate Responsibility is Everyone's Responsibility
כיצד להשתמש במערכת ההדפסה?
PUSH

Table of Contents


ҚАЗАҚТЕЛЕКОМ
АҚПАРАТ
ИНФОРМАЦИЯ
Біздің тарифтеріміз
Наши тарифы стали
www.telecom.kz

List of Acronyms

CALEA	Communications Assistance to Law Enforcement Act
CC	Communications content
CIS	Commonwealth of Independent States
CM	Monitoring System (Kazakhstan)
CSP	Communications service provider
CSR	Corporate social responsibility
CSTO	Collective Security Treaty Organisation
DPI	Deep Packet Inspection
EMS	Interception Management System (Kazakhstan)
ETSI	European Technical Standards Institute
EU	European Union
GPRS	General Packet Radio Service
IAI	Israeli Aircraft Industries
ICT	Information communication technology
IDF	Israel Defense Forces
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPO	Initial Public Offering
IRI	Intercept-related information
ISP	Internet service provider
ISS World	Intelligence Support Systems World
IT	Information technology
KGB	Soviet Committee for State Security
KNB	National Security Committee (Kazakhstan)
LEA	Law enforcement agency
LEMF	Law Enforcement Monitoring Facility
LGBT	Lesbian, Gay, Bisexual and Transgender
LI	Lawful Interception
LIMS	Lawful Interception Managment System
LTE	Long-Term Evolution
MMS	Multimedia Messaging Service
NATO	North Atlantic Treaty Organisation
NGO	Non-governmental organisation
NSN	Nokia Siemens Networks
OEM	Original Equipment Manufacturer
OSCE	Organisation for Security and Cooperation in Europe
PGO	Prosecutor General's Office (Kazakhstan)
PSTN	Public Switched Telephony Network
PU	Punkt Upravlenia
RATS	Regional Anti-Terrorist Structure
R&D	Research and development
SCO	Shanghai Cooperation Organisation
SIP	Session Initiation Protocol
SMS	Short Message Service
SNB	National Security Service (Uzbekistan)
SORM	System of Operative Investigative Measures
UN	United Nations
UNICON	State Unitary Enterprise Scientific Engineering and Marketing Researches Center (Uzbekistan)
VoIP	Voice Over Internet Protocol
WA	Wassenaar Arrangement


TEHNOLOGIÝALAR
MERKEZI

Introduction

State surveillance has historically played a central and well-documented role in Central Asia. The region is characterised by authoritarian systems of governance wherein entrenched power elites exercise dominance over political and economic affairs. As technological means of conducting surveillance advance, Central Asian states are engaging in the wide-scale surveillance of the telecommunications, internet activity, and electronic devices of the civilian population in order to consolidate political control, silence dissent, and undermine the enjoyment of individuals' human rights.

While regimes in the region recognise the role that modern information communication technologies and telecommunications networks can play in economic development, they also perceive the threat to centralised state power that modern telecommunications and access to platforms and high-speed networks represent. For human rights activists, political movements, minority groups, labour representatives, and others, these technologies enhance their ability to organise, and to build knowledge, capacity, and support. Communications technologies have transformed the production, dissemination and acquisition of news, data, analysis, and opinion, and have emboldened democratic accountability and democratisation. As a consequence, efforts to improve telecommunications infrastructure and attract foreign investment in Central Asia have been accompanied by the expansion of state censorship and electronic surveillance.

The electronic surveillance capabilities of various Central Asian regimes have been provided by a range of commercial actors, including manufacturers of telecommunications equipment, communications service providers (CSPs), and surveillance companies that directly market and sell products and services to the region's law enforcement and intelligence agencies. These products and services facilitate a legal and technological architecture based on a Russian model known as the System of Operative Investigative Measures (known by the Russian acronym SORM), which enables state authorities in Central Asia to directly access commercial telecommunications networks and to obtain individuals' data.

Further, some countries are equipped with sophisticated surveillance capabilities that allow the monitoring of communications on a mass scale. These surveillance capabilities are centralised and accessed by security agencies in monitoring centres, located across the region, allowing agents to intercept, decode, and analyse the private communications of thousands of people simultaneously. While monitoring centres are used across the world for law enforcement and intelligence gathering purposes, in the absence of a strong legislative framework and a rigorous oversight regime, they can facilitate sweeping violations of human rights.

This report identifies some of the local and multinational companies involved in the provision, brokerage and maintenance of monitoring centres in the region, and the technical and legal infrastructure that enables their use. It also includes testimonies from activists and journalists who have been subjects of state surveillance. The five republics that constitute the Central Asian region (Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan) provide a unique backdrop to the examination of the surveillance technology industry: the region contains some of the most authoritarian systems of governance in the world with repressive state authorities increasingly seeking to clamp down on internet and telecommunications freedoms, and despite massive human rights issues within all of the countries, there are currently few trade restrictions stopping companies from empowering these state authorities with surveillance technology.

It is important to establish that this report focuses on domestic electronic surveillance for ostensibly law enforcement or national security purposes, and not on foreign or military intelligence collection.

The purpose of this report is to foster an effective policy and legislative response to the developing global surveillance industry by highlighting specific types of actors and technologies. Case studies are provided summarizing some of the ways in which surveillance affects people in the region and how it undermines human rights, but the report is not a comprehensive review of the surveillance capabilities or legislative framework in the region. Rather, this report aims to advance understanding of how the surveillance technology industry and other actors operate and how they are facilitating electronic surveillance by authoritarian States in a manner that puts at risk the enjoyment of human rights. An appropriate response is multilayered: a list of recommendations is presented for commercial actors involved in facilitating electronic surveillance, and for policy makers working across different governmental and multilateral levels.

State surveillance can only legitimately be exercised where the means and ends of surveillance are prescribed by law. Surveillance must only be conducted within a robust legislative framework that stipulates an appropriate system of safeguards and oversight, and in keeping with international human rights law, particularly the principles of necessity and proportionality.

The Snowden leaks and subsequent calls for reforms within the Five Eyes countries have revealed the extent to which unrestrained technological capabilities can overwhelm weak legislative constraints and oversight mechanisms, even in countries with established regulatory systems of checks and balances. In authoritarian and repressive systems of governance, the potential for such surveillance capabilities to be used for political control and abuses of human rights is clear.

The arbitrary surveillance of electronic communications and the monitoring of online activity not only undermines the enjoyment of human rights, but also threatens to undermine progress by reinforcing established power structures, and depriving actors for change of essential tools for communication and organisation. It compromises the fundamental human right to privacy and other rights which depend upon it, including the rights to freedom of expression and assembly, and puts the security of users at risk, potentially making them vulnerable to arbitrary detention, torture, and killings. Perversely, therefore, while new communications channels have the potential to accelerate societal, economic, and political change in regions like Central Asia, they may also facilitate increased opportunities for intrusive surveillance that undermines the benefits gained.


CYB
ER
GYM

Executive Summary

Testimonials taken by Privacy International attest to the use by Central Asian governments of electronic surveillance technologies to spy on activists and journalists, domestically and abroad, in order to clamp down on dissent and to reenforce their political control.

Two multinational technology companies, Verint Israel and NICE Systems, have been supplying monitoring centres to both Kazakhstan's KNB and Uzbekistan's SNB, two security agencies widely implicated in human rights abuses. The monitoring centres allow them direct, unchecked access to the telephone calls and internet activity of the civilian population on a mass, indiscriminate scale.

Verint attempted to facilitate Uzbek authorities' interception of encrypted SSL traffic using fake certificates, based on technology provided by US-based company Netronome. If this had been successful, it would have allowed authorities unprecedented access to private communications.

Germany-based companies Trovicor and Utimaco, and a number of Russian companies, have also marketed monitoring centres to governments in the region.

Kazakhstan has distributed monitoring nodes known as Punkt Upravlenias which facilitate access to networks via the SORM interception regime. The installation of these nodes was tendered to local companies but was likely supplied by foreign surveillance companies.

Numerous surveillance techniques can be employed by PUs, and have been marketed and supplied to Kazakhstan by Russian and US-based companies.

Documents show how various local companies acting as re-sellers and distributors for manufacturers abroad compete as prime bidders in tenders for surveillance projects.

Foreign and domestic communications service providers have provided Central Asian governments with direct access to their networks in return for permission to operate.

Large telecommunications equipment manufacturers, on whose hardware the networks are based, have adapted their technology in order to facilitate government access to communications.

As first identified by Toronto-based Citizen Lab, invasive software used to hijack devices, manufactured by Italy-based company Hacking Team and UK/Germany-based company Gamma, appear to be in use in Uzbekistan and Turkmenistan respectively. International institutions and individual states with interests in Central Asia have been actively encouraging increased surveillance and censorship capabilities in the region.

The legal framework governing electronic surveillance in Central Asia is inadequate to ensure compliance with international human rights standards.

Recommendations

To companies selling electronic surveillance equipment to government agencies for the purpose of law enforcement or intelligence gathering; communications service providers; and telecommunications equipment manufacturers:

— Do not export a product if the beneficial end-user cannot be clearly identified or if they have a documented record of human rights abuse that is likely to be enabled by the product.

— Do not export a product if there is no clear legal framework or oversight mechanism governing its use within the country of destination.

— Stipulate clear end-use assurances in contractual agreements with customers encompassing strong human rights safeguards and protecting against their arbitrary and unlawful use. Carry out a periodic review and refuse to carry out maintenance, training, or updates if the end-use does not conform to these contractual obligations.

— Develop internal policies relating to re-sellers and distributors, and include provisions in contractual agreements ensuring their adherance to export control regulations and to the developer's own human rights provisions.

— Original Equipment Manufacturers (OEMs) should ensure that the company incorporating their equipment adheres to export control regulations and to the OEM's own human rights provisions.

— Carry out due-diligence and Know Your Customer checks on any potential beneficial end-users.

— Commit to and publish strong Corporate Social Responsibility committments conforming to the 'Respect' principle of the United Nations' Guiding Principles on Business and Human Rights.

— Initiate an annual review of adherence to Corporate Social Responsibility committments and international human rights standards and publish outcomes. Included within this must be strong transparency measures containing, to the greatest extent possible, a list of all end-users.

To communications service providers and telecommunications equipment manufacturers:

— Exhaust all available national and international legal avenues to challenge government policies and practices which undermine international human rights law.

— Do not sell products or services to a market in which the human rights record of the government, and a lack of meaningful oversight over electronic surveillance activities, means that products and services will be used to further undermine international human rights standards.

— Refuse to comply with any government requests for access to networks and to subscribers' data which conflict with international human rights law.

— Do not allow or facilitate security agencies' access to networks if the relevant legal and regulatory framework does not provide for meaningful oversight of security agencies' activities.

— Develop a policy on the minimum legal framework, regulatory and technological safeguards, and standards of oversight that must be evident in an end-user destination before the CSP or telecommunciations equipment manufacturer would agree to provide network services or infrastructure. Examples of possible requirements may include stipulation that agencies provide copies of warrants prior to any interception and information about actual intercepts conducted, or that CSPs retain the ability to challenge the interception activities of authorities where there is an unsubstantiated cause, and retain powers to notify subscribers of activities taking place.

— Publish policies in relation to these issues and report on how networks and subscribers' data are accessed by authorities, and what form of oversight exists.

— Take action through industry initiatives to collectively put pressure on governments to improve technological and legal safeguards in Lawful Interception and other electronic surveillance practices.

To multilateral institutions, foreign governments, and export control authorities:

— Do not approve the export of listed surveillance technologies where there is a risk they will be used for internal repression or to otherwise undermine human rights, or if there is no clear legal framework governing the use of the item.

— Ensure initiatives to develop telecommunications infrastructure in Central Asia carry strong prerequisites for reform of legal frameworks and oversight mechanisms pertaining to electronic surveillance, and respect for international human rights standards.

— Call upon states to respect international human rights standards when authorising exports of electronic surveillance technology.

— Commit to and implement agreements on export control measures related to electronic surveillance technologies. While some measures have already been taken at the Wassenaar Arrangement (WA), this does not mean that national governments and regional institutions such as the EU should not pursue their own solutions. Any effective agreement must also include non-WA participating states China and Israel.

— Identify products that can be subjected to export licensing without harming security research or otherwise impact negatively on the development of the ICT sector. A solution could include not just the addition of a product on a national or multilateral export control regime control list, but also end-use and end-user stipulations.

— Ensure strong human rights criteria are included in export control provisions that are specific to surveillance technologies. Human rights criteria should take into account the state's legal framework, oversight mechanisms, and respect for international human rights standards, and the end-user's record regarding the use of electronic surveillance.

— Given the amount of training, maintenance, and software updates needed for surveillance technologies to work, subject transfers of technology and technical assistance to licensing restrictions.

— Work within export control regimes, and with multilateral institutions, and other states to identify and mitigate challenges to applying and enforcing export control regulations on surveillance technologies, particularly regarding brokering, re-export, incorporation, and diversion challenges.

Human Rights & the Political Situation in Central Asia

The countries that make up the Central Asian region (Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan) share some common characteristics, but are largely ethnically, historically, socially, economically, and politically distinct. While this report focuses on the region as a whole, it is important to be mindful of these differences, and to note that each state's adherence to international human rights standards is disparate. While there are serious human rights concerns in all five states, this report focuses on Kazakhstan and Uzbekistan, as it is in these two countries that the use of communications technology, and corresponding proliferation of electronic surveillance, are most widespread.

Since their independence from the Soviet Union in 1991, democratisation has proved a slow process in the Central Asian republics. Political systems have remained steadfastly authoritarian and dictatorial. Nursultan Nazarbayev has been President of Kazakhstan since 1991, while Askar Akayev held the post of President of Kyrgyzstan from 1991 until the Tulip Revolution in 2005, since which time Kyrgyzstan has faced political and ethnic turmoil. Emomalii Rahmon has been in effective power in Tajikistan since 1994, and President Gurbanguly Berdymukhamedov won the most recent election in Turkmenistan in 2012 with a 97 per cent share of the vote without any meaningful opposition.[1] Islam Karimov has held the post of President of Uzbekistan since its independence in 1991. The Organisation for Security and Cooperation in Europe (OSCE), which monitors elections and of which all five republics are members, has found severe democratic deficiencies in all of the most recent presidential elections in each country.[2]

Kazakhstan

Human Rights Watch, in its 2014 World Report, noted that "Kazakhstan's poor human rights record continued to deteriorate in 2013,"[3] citing as a cause overly broad laws that allow for the suppression of free speech, dissent, and freedom of assembly and religion. Torture remains commonplace.[4]

1 "Turkmenistan's President Re-elected With 97% of Vote", New York Times, 13 February 2012, available at http://www.nytimes.com/2012/02/14/world/asia/berdymukhammedov-re-elected-president-of-turkmenistan.html

2 For final reports, see http://www.osce.org/odihr/elections

3 "Human Rights Watch World Report 2014", Human Rights Watch, 2014, available at http://www.hrw.org/sites/default/files/wr2014_web_0.pdf

4 "Human Rights Watch World Report 2014", Human Rights Watch, 2014, available at http://www.hrw.org/sites/default/files/wr2014_web_0.pdf

During unrest in 2011, security forces used excessive force; they fired on crowds, resulting in some 15 people dying and over 100 more being injured. In the aftermath of the violence, many report being stripped naked and beaten for several hours in order to extract confessions.[5] Civil society activists and prominent members of the political opposition were imprisoned. Opposition groups and independent media outlets and journalists were harassed, and often forced to close.

Kyrgyzstan

Torture and ill-treatment, according to the UN Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment, remains "widespread" in Kyrgyzstan.[6] Human rights defender Azimjon Askarov, whose trial was '"marred by serious violations of fair trial standards," is serving a life sentence, while authorities refuse to investigate his credible claims of torture.[7] Ethnic violence that erupted in 2010 has led to the disproportionate targeting of ethnic minorities, while, according to Amnesty International, authorities have failed "to impartially and effectively investigate the June 2010 violence and its aftermath and provide justice for the thousands of victims of serious crimes and human rights violations, including crimes against humanity."[7] Further, gender-based violence remains a 'long-standing' problem, and LGBT groups face police extortion, beating, and sexual violence.[9]
In 2007 journalist Alisher Saipov was murdered by as yet unidentified killers; independent online news agencies have been subject to censorship.[10]

Tajikistan

In Tajikistan torture and ill-treatment of detainees in order to obtain confessions is widespread. Amnesty International reports that state authorities use ''electric shocks, boiling water, suffocation, beatings, and burning with cigarettes...rape and threats of rape in relation to female and male detainees, as well as psychological torture."[11]

5 "Amnesty International Report 2013: The state of the world's human rights", Amnesty International, 2013, available at http://files.amnesty.org/air13/AmnestyInternational_AnnualReport2013_complete_en.pdf

6 Report of the Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment - Mission to Kyrgyzstan, Juan E. Méndez, UN Human Rights Council, 2012, available at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G12/106/04/PDF/G1210604.pdf?OpenElement

7 "Human Rights Watch World Report 2014", Human Rights Watch, 2014, available at http://www.hrw.org/sites/default/files/wr2014_web_0.pdf

8 "Amnesty International Report 2013: The state of the world's human rights", Amnesty International, 2013, available at http://files.amnesty.org/air13/AmnestyInternational_AnnualReport2013_complete_en.pdf

9 "Human Rights Watch World Report 2014", Human Rights Watch, 2014, available at http://www.hrw.org/sites/default/files/wr2014_web_0.pdf

10 "Human Rights Watch World Report 2014", Human Rights Watch, 2014, available at http://www.hrw.org/sites/default/files/wr2014_web_0.pdf

11 "Amnesty International Report 2013: The state of the world's human rights", Amnesty International, 2013, available at http://files.amnesty.org/air13/AmnestyInternational_AnnualReport2013_complete_en.pdf

A human rights monitoring organisation was recently forced to close, and it remains a criminal offence to criticize the President or government representatives [12] Popular websites, including social media, are subject to periodic censorship, while the LGBT community are subject to discrimination and beatings by police.[13]

Turkmenistan

Turkmenistan is one of the most repressive countries in the world. There are reports of torture and ill-treatment of alleged criminals by security forces, which treatment includes "electric shocks, asphyxiation, rape, forcibly administering psychotropic drugs, deprivation of food and drink and exposure to extreme cold."[14] Human rights defenders in-country and abroad, and their families, are subject to harassment and threats.[15] Male homosexuality is punishable by up to 20 years in prison.[16] There is no credible political opposition and power is concentrated in the presidential administration. Independent media is non-existent, and those media outlets that do exist are used as vehicles for state propaganda. Freedom House ranks Turkmenistan 196 out of 197 countries for freedom of the media,[17] with North Korea placing last. Turkmenistan is currently listed as a 'Country of Human Rights Concern' by the UK Government.[18]

12 "Human Rights Watch World Report 2014", Human Rights Watch, 2014, available at http://www.hrw.org/sites/default/files/wr2014_web_0.pdf

13 "Human Rights Watch World Report 2014", Human Rights Watch, 2014, available at http://www.hrw.org/sites/default/files/wr2014_web_0.pdf

14 "Amnesty International Report 2013: The state of the world's human rights", Amnesty International, 2013, available at http://files.amnesty.org/air13/AmnestyInternational_AnnualReport2013_complete_en.pdf

15 "Turkmenistan (2010-2011) Situation of Human Rights Defenders, International Federation for Human Rights, updated as of May 2011, available at http://www.fidh.org/en/eastern-europe-central-asia/Turkmenistan,766/TURKMENISTAN-2010-2011

16 "Corporate report Turkmenistan - Country of Concern", Foreign & Commonwealth Office, updated 16 October 2014, available at https://www.gov.uk/government/publications/turkmenistan-country-of-concern/turkmenistan-country-of-concern

17 "Press Freedom Rankings", Freedom House, 2014, available at https://freedomhouse.org/report/freedom-press-2014/press-freedom-rankings#.VGEUTHnMBsB

18 "Human Rights and Democracy 2013-2014", Foreign & Commonwealth Office, 2014, available at http://www.hrdreport.fco.gov.uk

Uzbekistan

In Uzbekistan, torture and ill-treatment of detainees is regarded by the International Committee of the Red Cross (ICRC) as 'systematic'. This led to the ICRC deciding to cease prison visits in 2013 for lack of cooperation.[19] Methods of torture include "beating with batons and plastic bottles, hanging by the wrists and ankles, rape, and sexual humiliation."[20] It is estimated that possibly thousands of prisoners are being held in Uzbekistan on political grounds.[21] Human rights activists, civil society, and journalists face excessive harassment, including questioning, beatings, and house arrest.[22] Amnesty International reported in 2013 that journalists and human rights defenders are subject to routine monitoring by uniformed and plain-clothes security officers, questioning, house arrest, and beatings by law enforcement officers or people suspected of working for the security services.[23] Freedom of association, assembly, and the work of civil society is extremely restricted.[24] Independent and foreign-owned media is subject to severe restriction, and publicly insulting the President is punishable by up to five years in prison.[25] Freedom House ranks Uzbekistan ahead of Turkmenistan and North Korea for press freedom.[26] Adults and children are forced en-masse into labour to pick cotton during the harvest. Indeed in 2009 all of the Central Asian republics were listed by the US Department of Labor as using child labour. Uzbekistan is currently listed as a 'Country of Human Rights Concern' by the UK Government.[27]

19 "Human Rights Watch World Report 2014", Human Rights Watch, 2014, available at http://www.hrw.org/sites/default/files/wr2014_web_0.pdf

20 "Human Rights Watch World Report 2014", Human Rights Watch, 2014, available at http://www.hrw.org/sites/default/files/wr2014_web_0.pdf

21 "Uzbekistan 2013 Human Rights Report", US State Department, 2013, available at http://www.state.gov/documents/organization/220622.pdf

22 "Amnesty International Report 2013: The state of the world's human rights", Amnesty International, 2013, available at http://files.amnesty.org/air13/AmnestyInternational_AnnualReport2013_complete_en.pdf

23 "Amnesty International Report 2013: The state of the world's human rights", Amnesty International, 2013, available at http://files.amnesty.org/air13/AmnestyInternational_AnnualReport2013_complete_en.pdf

24 "Uzbekistan 2013 Human Rights Report", US State Department, 2013, available at http://www.state.gov/documents/organization/220622.pdf

25 "Uzbekistan 2013 Human Rights Report", US State Department, 2013, available at http://www.state.gov/documents/organization/220622.pdf

26 "Press Freedom Rankings", Freedom House, 2014, available at https://freedomhouse.org/report/freedom-press-2014/press-freedom-rankings#.VGEUTHnMBsB

27 "Human Rights and Democracy 2013-2014", Foreign & Commonwealth Office, 2014, available at http://www.hrdreport.fco.gov.uk

International Context

There are significant foreign interests in Central Asia. Foreign interests are driven by securing access to the republics' commodities, capitalising on their high geographically strategic value, and minimizing threats from foreign states and non-state actors. A number of Central Asian countries are large exporters of natural resources, particularly crude oil and natural gases from the Caspian Sea Basin, as well as precious metals and other commodities such as cotton. The region is of renowned geo-strategic value and was the scene of the 'Great Game' between imperialist Russian and British forces during the 19th century. The close proximity of Iran, Afghanistan, China, Russia, and the Middle East, as well as perceived and real issues of domestic terrorism and other non-state threats, such as drug trafficking, all combine to mean that the region is of significant strategic interest to foreign actors. As foreign governments seek to develop their trade and security links, they invest in critical infrastrastructure, encourage security cooperation and provide political support to Central Asian regimes. In doing so they often overlook significant human rights abuses in the countries.

Securing access to the region's commodity exports is a key driver of foreign policy positions with respect to the Central Asian countries: Kazakhstan, Turkmenistan and Uzbekistan hold an estimated 700 trillion cubic feet of proven natural gas reserves, which is among the largest reserves in the world. At over 30 billion barrels, the proven oil reserves in the region are estimated to be only slightly below those of the US.[28] Uzbekistan's economy is largely based on commodities: in 2012 it was the world's 14th largest producer of natural gas;[29] ninth largest producer of gold;[30] and a significant manufacturer of cotton. Turkmenistan holds the world's fourth-largest reserve of natural gas.[31] Kazakhstan is a significant producer of crude oil. In 2013, it was thought to be the 18th largest producer in the world,[32] while Kyrgyzstan relies mostly on agriculture and precious metals, and Tajikistan on cotton and aluminium.[33]

28 "BP Statistical Review of World Energy", British Petroleum, June 2013 cited in "Central Asia: Regional Developments and Implications for U.S. Interests", Jim Nichol, Congressional Research Service, March 21 2014, pp. 48, available at http://fas.org/sgp/crs/row/RL33458.pdf

29 "The World Factbook", Central Intelligence Agency, available at https://www.cia.gov/library/publications/the-world-factbook/rankorder/2249rank.html

30 "Gold", Micheal W. George, U.S. Geological Survey, February 2014, available at http://minerals.usgs.gov/minerals/pubs/commodity/gold/mcs-2014-gold.pdf

31 "Turkmenistan, gas and stability: Elsewhere in Turkestan", The Economist, 9 July 2009, available at http://www.economist.com/world/asia/displaystory.cfm?story_id=14009121

32 "Kazakhstan", U.S. Energy Information Administration, October 28 2013, available at http://www.eia.gov/countries/country-data.cfm?fips=kz

33 "U.S. Relations With Tajikistan", U.S. Department of State, 10 February 2014, available at http://www.state.gov/r/pa/ei/bgn/5775.htm

Regional Support for Surveillance

Internal security and political stability continue to be cited by governments in Central Asia as factors justifying expansion of surveillance and censorship practices. These claims echo those made by the two biggest economic actors and political powers in the region, China and Russia.

China's role in the region is linked to economic and security interests, and has been increasing. China it is now the biggest trading partner of all the Central Asian states, excluding Uzbekistan.[34] China's security priorities in the region involve curtailing extremist elements and the threat of Uighur separatist groups, countering any threats caused by the withdrawal of ISAF troops from Afghanistan, and minimizing political instability within the region.[35] Border security and transnational crime are also issues for Beijing, with Xinjiang province sharing a 2,760km border with Kazakhstan, Kyrgyzstan, and Tajikistan.

China was a founding member of the Shanghai Cooperation Organisation (SCO) in 2001, together with Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan, allowing it to exercise its security interests in the region with Russian acquiesce. The SCO was initially used by China to resolve its lingering border disputes in the region, but today the SCO facilitates the development of regional military, security and economic cooperation, including joint military exercises, programmes for tackling non-state threats such as terrorism, drug trafficking and separatism, and energy cooperation initiatives. Its explicit aims are to focus on countering the 'three evils' of extremism, separatism, and terrorism in the region.[36]

34 "Rising China, sinking Russia", The Economist, September 14 2013, available at http://www.economist.com/news/asia/21586304-vast-region-chinas-economic-clout-more-match-russias-rising-china-sinking

35 "China's Central Asia Problem", International Crisis Group, 27 February 2013, available at http://www.crisisgroup.org/en/regions/asia/central-asia/244-chinas-central-asia-problem.aspx

36 The Executive Committee of the Regional Counter-Terrorism Structure, Shanghai Cooperation Council, available at http://www.sectsco.org/EN123/AntiTerrorism.asp

The SCO has made efforts to encourage members to counter perceived threats from ICTs and to coordinate responses. In 2011, it adopted *Rules of Conduct in the Field of Safeguarding International Information Security*, seeking to enhance cooperation among states in addressing "the common threats and challenges in the information space" by "curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment."[37] In turn, the permanent representatives to the UN of China, Russia, Tajikistan and Uzbekistan proposed that the same rules be endorsed by the UN General Assembly in the form of a resolution. In addition to recognising the need to counter the 'three evils', it also stipulates that it is a state's right and responsibility to control and monitor internet technologies on their territories, and that cooperation between state and private companies is essential to combat cyber threats.[38]

An analysis by the Human Rights Initiative of China reports how the SCO also acts as a platform for intelligence-sharing between members, including through the use of shared databases, and lists of individuals and supporters deemed relevant to the goal of countering terrorism, separatism, and extremism. Both Kazakhstan and Uzbekistan have stated in reports to the UN Security Council that they use SCO lists for monitoring, denying entry to, and sharing intelligence on specific individuals.[39] SCO members contribute intelligence drawn from various sources, including internet and telecommunications networks, to various Regional Anti-Terrorist Structure (RATS) databases. At one point it was envisaged that the databases would be used to record up-to-date locations of specific individuals and to identify individuals who possess the 'intent' to engage in criminal activity.[40] In September 2014, a meeting of the SCO RATS Executive Committee in Uzbekistan agreed to create a group of experts "to reveal and prevent use of internet for terrorism, separatism and extremism in 2015-2016."[41]

37 "Central Asia: Censorship and Control of the Internet and Other New Media1", Brigitte Dufour and Farid Tuhbatullin, International Partnership for Human Rights, Turkmen Initiative for Human Rights and Other Partner Organizations, FOCUS March 2012 Vol. 67, available at http://www.hurights.or.jp/archives/focus/section2/2012/03/central-asia-censorship-and-control-of-the-internet-and-other-new-media1.html#n5

38 "The Complexities of Central Asian Cyber Security", Nuria Kutnaeva, Journal of European Security and Defense Issues Vol. 5 Issue 2, 2014, p. 18, available at http://www.academia.edu/7287652/Regional_Cyber_Security

39 "Counter-Terrorism and Human Rights: the Impact of the Shanghai Cooperation Organization", Human Rights in China, 2011, p. 88, available at http://www.hrichina.org/sites/default/files/publication_pdfs/2011-hric-sco-whitepaper-full.pdf

40 "Counter-Terrorism and Human Rights: the Impact of the Shanghai Cooperation Organization", Human Rights in China, 2011, available at http://www.hrichina.org/sites/default/files/publication_pdfs/2011-hric-sco-whitepaper-full.pdf

41 "SCO RATS Council holds session in Dushanbe", UzDaily, 19 September 2014, available at http://www.uzdaily.com/articles-id-29281.htm

As former republics of the Soviet Union, Central Asian republics retain linguistic, cultural, and political ties with modern Russia. Russia regards the region as within its post-Cold War sphere of influence. In Central Asia, it seeks to limit and reverse the eastward expansion of NATO, and consolidate its international political power through gas and other energy exports, and political, security, and trade cooperation. Russia regards regime stability as its highest security priority in the region; Uzbekistan and Kazakhstan, the two largest military powers in the region, face various internal threats, and Russia is the dominant provider of military and security assistance for these and other Central Asian states.[42] Uzbekistan, Tajikistan, Kazakhstan, and Kyrgyzstan are members of the Commonwealth of Independent States (CIS), a regional cooperation bloc established after the break-up of the Soviet Union, which includes Russia. Russia is also seeking to develop the Eurasian Economic Community, a free trade area including itself and the Central Asian republics, excluding Turkmenistan, which would further trade and economic cooperation and reinforce its role in the region. Tajikistan, Kazakhstan, and Kyrgyzstan meanwhile are also members of the Collective Security Treaty Organisation (CSTO), a military alliance including Russia and several former Soviet Republics (Uzbekistan withdrew in 2012).

Similar to the SCO, the CSTO is also seeking to develop regional cooperation in the field of surveillance in order to counteract the perceived threat of political instability posed by social media platforms and ICTs. The Moscow Times quoted a source from within the CSTO claiming that "in the modern environment there is an infrastructure that allows for creating destabilizing situations in any, even the most trouble-free country..." and that "experts of the highest level" within the organisation were already working on this.[43] In his keynote speech to an informal CSTO summit in 2011, Kazakhstan's President Nursultan Nazarbaev spoke of the need to develop an "impregnable wall" to counter any threat posed to the region from the use of ICTs. [44]

42 "External Support for Central Asian Military and Security Forces", Dmitry Gorenburg, Stockolm International Peace Research Institute and Open Society Foundations, January 2014, available at http://www.sipri.org/research/security/afghanistan/central-asia-security/publications/SIPRI-OSFno1WP.pdf

43 "CSTO wants to monitor the internet to prevent a repeat of Arab revolutions", The Moscow News, 13 September 2011, available at http://themoscownews.com/society/20110913/189040987.html

44 "CSTO Moves Into The Information Age", Roger McDermott, Radio Free Europe Radio Liberty, 4 September 2011, available at http://www.rferl.org/content/commentary_csto_moves_into_information_age/24317363.html

According to an analysis[45] in per Concordiam, a journal produced by the Marshall Center, in 2010 the CSTO adopted regulations to develop cooperation in the field of information security among members, with a particular focus on combatting extremism and terrorism. Operations throughout 2009-2010 resulted in more than 2,000 websites being identified as containing material considered to incite ethnic and religious hatred, following which some 600 sites were suspended.[46] In 2011, the organisation adopted a secret document which recognised the role that social media platforms played in the organisation of protests in Russia.[47] Experts suggest that the CSTO coordinates operations to close websites that are "working against the state," and that "the work on information counteraction is one of the priorities of the CSTO's activity."[48]

45 "The Complexities of Central Asian Cyber Security", Nuria Kutnaeva, Journal of European Security and Defense Issues Vol. 5 Issue 2, 2014, pp. 18, available at http://www.academia.edu/7287652/Regional_Cyber_Security

46 "The Complexities of Central Asian Cyber Security", Nuria Kutnaeva, Journal of European Security and Defense Issues Vol. 5 Issue 2, 2014, pp. 18, available at http://www.academia.edu/7287652/Regional_Cyber_Security

47 "Russia's Surveillance State", Andrei Soldatov and Irina Borogan, World Policy Journal Vol. XXX N. 3 Fall 2013, available at http://www.worldpolicy.org/journal/fall2013/Russia-surveillance

48 "CSTO Moves Into The Information Age", Roger McDermott, Radio Free Europe Radio Liberty, 4 September 2011, available at http://www.rferl.org/content/commentary_csto_moves_into_information_age/24317363.html

Surveillance in Central Asia

As electronic surveillance practices evolved through the Cold War and alongside the commercialisation of digital networks, Soviet and Russian domestic surveillance laws and techniques developed separately from those in the US and in European countries. In the US and Europe, legislation and protocols were established to regulate government access to telecommunications networks in the form of Lawful Interception. The 1994 Communications Assistance for Law Enforcement Act (CALEA) established a regime within the US, while technical protocols were enacted across Europe under the auspices of the European Telecommunications Standards Institute (ETSI). Modern electronic surveillance techniques in the Central Asian republics have been primarily influenced by those of Russia: as the various former Soviet republics shared similar intelligence practices and structures, and relied on the same telecommunications equipment and infrastructure, many, including the Central Asian republics, adopted surveillance models and similar regimes to Russia's System of Operative Investigative Measures (SORM).[49] SORM was put into practice across Russia in the early 1990s and provides an architecture by which law enforcement and intelligence agencies can obtain direct access to data on commercial networks. SORM-1, put into place in the early 1990s, allows for access to telephone and mobile networks. SORM-2, implemented in 1998, applies to IP traffic, and SORM-3 to interception of all communications media, providing quick access[50] and long-term storage for a period of three years.[51]

For the SORM architecture to work as a whole, there are three types of commercial actors involved, each of which is generally focused on providing different types of products and services.

The first type of commercial actor is the manufacturer of telecommunications equipment that forms the basis of a network. This includes equipment such as switches and exchanges used to connect traffic between lines, as well as other hardware and services which ensure telecommunications infrastructure, as a whole, is able to support different networks and services.

The second type of commercial actor is the communications service provider (CSP) which manages a network and charge subscribers for certain services, such as internet, mobile and fixed-line telephony services. CSPs are themselves responsible for ensuring that their networks function and that their activities are in line with the national legislation of the country in which they are operating. This invariably

49 "Lawful interception: the Russian approach", Andrei Soldatov and Irina Borogan, Privacy International, 4 March 2013, available at https://www.privacyinternational.org/news/blog/lawful-interception-the-russian-approach

50 Norsi-Trans available at http://www.norsi-trans.ru/pcategory/sorm-123/

51 "Lawful interception: the Russian approach", Andrei Soldatov and Irina Borogan, Privacy International, 4 March 2013, available at https://www.privacyinternational.org/news/blog/lawful-interception-the-russian-approach

includes statutory requirements that the CSP facilitates access by law enforcement and security agencies to their networks and to their subscribers' data. SORM requires Internet Service Providers (ISPs), one type of CSP, to keep a detailed record of their subscribers' internet activity and, if necessary, to install the hardware necessary for doing so. Under SORM in Kazakhstan, for example, this information includes details regarding users' identities, data regarding specific visits, and details concerning the traffic being transmitted.[52]

The third type of commercial actor is the surveillance company that directly markets and sells products and services for law enforcement purposes. These companies provide 'solutions' intentionally designed to enable state agencies to intercept, analyse, or disseminate data from networks for law enforcement or intelligence purposes.

Surveillance companies sell electronic surveillance solutions either directly to governments or particular agencies, or to CSPs in order that the CSPs can meet their statutory obligations. Some CSPs therefore contract surveillance companies at their own expense, and incorporate electronic surveillance solutions within their networks. Some large manufacturers of telecommunications equipment also sell solutions or specific components for the purpose of electronic surveillance. CSPs also purchase equipment from telecommunications equipment manufacturers both to ensure that their networks function, and to guarantee that their networks can enable access to state agencies.

Authorities ensure that CSPs provide access to their networks by making operating licenses contingent on cooperation. The key feature of Lawful Interception models, including SORM's, is that CSPs and equipment manufacturers are required to ensure that their network and equipment is comptaible and made accessible to a Law Enforcement Monitoring Facility (LEMF) from which analysts request, receive, store, and analyse intercepted data. The capabilities of these monitoring centres vary widely; some are used to simply request information from a CSP related to a telephone call, while others are used to intercept and view the IP activity and communications of an entire nation. In the SORM model, a Punkt Upravlenia (PU) acts as a monitoring node used to manage the interception process, although in Central Asia they are connected to the networks of specific CSPs and can be used to intercept smaller networks and discrete numbers of subscribers.

52 "Kazakhstan", OpenNet Initiative, 2010, pp. 188, available at https://opennet.net/sites/opennet.net/files/ONI_Kazakhstan_2010.pdf

Throughout Central Asia, the various successor agencies to the Soviet KGB continue to act as the lead agencies within the republics' intelligence architecture.[53] In Kazakhstan, for example, it is the successor agency to the KGB, the National Security Committee (KNB), which has procured monitoring centres, despite legislation stipulating that the Ministry of Internal Affairs, the Financial Police, and other agencies all have the authority to interfere with private communications.[54] Such agencies, often comprised at senior level by former KGB officers, are still characterised by the practices and culture of the KGB.[56] This legacy has also led to their centralisation, and exclusive governance under the control of the executive, specifically the president. A significant point of their focus as a result is to monitor the activities of dissidents, human rights activists, journalists, and powerful local and foreign business people.[56]

Profile

KNB

Established in 1992 to replace the KGB after the break up of the Soviet Union, the National Security Committee (KNB) is Kazakhstan's interior intelligence agency and is directly accountable to the president. Its mandate includes counter-espionage, counter-terrorism, the provision of governmental cryptographic capabilities, and the development and implementation of public policy. Headed since 2010 by one of the leaders of one of Kazakhstan's elite factions, Nurtai Abykayev, it is composed of Joint Chiefs of Staff, national counterintelligence services, the Border Guard, and special purpose military units.[57] Barlau, Kazakhstan's foreign intelligence agency, was formerly controlled by the KNB, but was replaced in 2009. Jane's Intelligence Digest argues that Barlau was "heavily involved in monitoring dissidents and expatriates abroad" due to the KNB being "primarily a political and internal security agency."[58]

53 "Central Asian Security Post-2014. Perspectives in Kazakhstan and Uzbekistan", Roger N McDermott, Danish Institute for International Studies, 2013, pp. 9, available at http://subweb.diis.dk/graphics/Publications/Reports2013/RP2013-12-McDermott-Kazakhstan_web.jpg.pdf

54 "Kazakhstan", U.S Department of State, 2011, pp. 10, available at http://www.state.gov/documents/organization/186676.pdf

55 "Central Asian Security Post-2014. Perspectives in Kazakhstan and Uzbekistan", Roger N McDermott, Danish Institute for International Studies, 2013, available at http://subweb.diis.dk/graphics/Publications/Reports2013/RP2013-12-McDermott-Kazakhstan_web.jpg.pdf

56 "Central Asian Security Post-2014. Perspectives in Kazakhstan and Uzbekistan", Roger N McDermott, Danish Institute for International Studies, 2013, pp. 9, available at http://subweb.diis.dk/graphics/Publications/Reports2013/RP2013-12-McDermott-Kazakhstan_web.jpg.pdf

57 Security Sector Reform in Central Asia, Erica Marat, The Geneva Centre for the Democratic Control of Armed Forces, 2012, DCAF, available at http://www.dcaf.ch/Publications/Security-Sector-Reform-in-Central-Asia

58 "Syrbar: Kazakhstan's new Foreign Intelligence Service", Jane's Intelligence Digest, 9 March 2009, released on Wikileaks on February 19 2013, available at https://wikileaks.org/gifiles/docs/63/63743_kazakhstan-s-new-foreign-intelligence-services-.html

Profile

KNB

The KNB is heavily involved in clamping down on dissent in Kazakhstan. Amnesty International documents "frequent reports of Committee of National Security (KNB) officers violating human rights, including by resorting to torture and other ill-treatment, ostensibly in pursuance of [countering terrorism and other threats to national security], including to obtain confessions."[59] Ramazan Yesergepov, an investigative journalist, editor, and labour rights advocate was arrested by KNB agents for the collection and publication of state secrets after publishing an article entitled "Who Rules the Country: the President or the Kazakh National Security Committee?". His trial and subsequent treatment has been roundly condemned by numerous human rights organisations.

In 2009, a former defence minister accused the KNB of intercepting his and other members of the Kazakh parliament's phone calls.[60] In 2012, KNB officers were accused of being involved in the coercion of testimonies of 37 defendants accused of organising mass protests by using violence, psychological pressure, suffocation, and other forms of ill-treatment.[61]

Profile

SNB

The National Security Service (SNB) is currently Uzbekistan's lead intelligence agency and one of its most powerful entities. Established in 1991 as the successor agency to the KGB, it reports directly to the president with a mandate to concentrate on internal security and counter-espionage. Its mandate also includes working on the development of technical measures related to national security, such as standardisation, licensing, and certification in the field of encryption. The SNB's head, Rustam Inoyatov, and its senior officials, are described as some of the most highly influential factions within Uzbekistan.
The SNB recently consolidated its position in Uzbekistan by taking control over one of its rival factions, the Ministry of Interior Affairs. As a result, the SNB now controls the police. Inoyatov's second-in-command was also made head of

58 "Syrbar: Kazakhstan's new Foreign Intelligence Service", Jane's Intelligence Digest, 9 March 2009, released on Wikileaks on February 19 2013, available at https://wikileaks.org/gifiles/docs/63/63743_kazakhstan-s-new-foreign-intelligence-services-.html

59 "Kazakhstan. Submission to the United Nations Commission Against Torture", Amnesty International, 2014, available at http://www.amnesty.org/en/library/asset/EUR57/002/2014/en/17b29f06-32a1-4a4a-bb38-e605a140550f/eur570022014en.pdf

60 "The Global Intelligence Files - Central Asia Intelligence", Wikileaks, 19 February 2013, available at https://wikileaks.org/gifiles/docs/54/5475076_central-asia-intelligence-.html

61 "Kazakhstan: Submission to the UN Committee Against Torture", Human Rights Watch, October 2014, available at http://www.hrw.org/news/2014/10/20/kazakhstan-submission-un-committee-against-torture

Profile

SNB

the President's personal security service.[62] Inoyatov is described by the US Embassy as being "one of two or three top power brokers in Uzbekistan," and as a "key gatekeeper to President Karimov and a decider of issues large and small that do not necessarily fall under a strictly intelligence purview."[63] He is touted as a possible successor to the incumbent and ageing President Karimov. Karimov's daughter, Gulnara Karimova, presumed successor to her father, is reportedly currently under house arrest, and claims that the SNB is engaging in a smear campaign against her.[64] According to correspondence seen by Privacy International, Gulnara Karimova claims to have become a target for electronic surveillance.

The SNB have been roundly condemned for wide-scale abuses of human rights. The 2005 Andijan Massacre, which took place outside of the SNB headquarters building, saw SNB officers fire indiscriminately at civilian crowds, killing hundreds. Survivors and refugees have been subsequently targeted by the SNB and placed under extensive surveillance.[65]

Human rights activists complain of brutal treatment at the hands of the SNB. For example, Gulshan Karaeva, a human rights activist who in 2012 published a report detailing efforts by the SNB to make her into an informant, was subjected to a series of physical attacks and threats.[66]

The SNB tightly controls all forms of media in Uzbekistan. The OpenNet Initiative reports that SNB officers frequently visit ISPs and internet cafes to monitor compliance.[67] The SNB also polices the output of traditional media outlets and journalists.

62 "Uzbekistan's Feuding Family Elite", Inga Sikorskaya, Institute for War and Peace Reporting, 31 January 2014, available at http://www.refworld.org/publisher,IWPR,,UZB,52f0afbe4,0.html

63 "Cable reference id: #08TASHKENT610 - Ambassador's May 28 Meeting With Uzbek Intelligence Chief", 30 May 2008, published on Wikileaks on 1 September 2011, available at https://cablegatesearch.wikileaks.org/cable.php?id=08TASHKENT610&q=nss%20uzbekistan

64 "Gulnara Karimova replies to property claims", UzNews, 26 December 2013, available at http://www.uznews.net/en/politics/24761-gulnara-karimova-replies-to-property-claims

65 "Saving its Secrets. Government Repression in Andijan", Human Rights Watch, 2008, available at http://www.hrw.org/sites/default/files/reports/uzbekistan0508webwcover.pdf

66 "Universal Periodic Review: HRW Submission on Uzbekistan - Submitted in October 2012", Human Rights Watch, updated in April 2013, available at http://www.hrw.org/news/2013/04/19/universal-periodic-review-hrw-submission-uzbekistan-submitted-october-2012

67 "CIS Overview", OpenNet Initiative, 2010, available at https://opennet.net/research/regions/cis

Testimonies

Privacy International identified activists and journalists currently living in Central Asia, and those in exile ouside the region, who believe that they have been targeted by state electronic surveillance in an effort to silence them. It is clear that the authorities' perceived and actual surveillance capabilities have led to a culture of self-censorship in Central Asia. For example, surveillance targets in Turkmenistan attest that the threat of reprisals on the part of the government for even minor disobedience is so great that they could not risk Privacy International publishing their testimonies, even anonymously. One of the few remaining human rights advocates in the country, Natalia Anurova, informed Privacy International that very little communication is occurring by electronic means within Turkmenistan as a result of government surveillance and censorship techniques.

The following case study on individuals who have been surveilled in Uzbekistan shows how they and their communications have been targeted. Their accounts vividly demonstrate the inherent danger of equipping such authorities with sophisticated mass or intrusive surveillance technologies. Where individuals have provided their consent, we have revealed their identities. In all other cases, we have concealed identities for security reasons.

Case Study: Uzbekistan

Numerous journalists and activists living in Uzbekistan and outside of it, in exile, report that their communications have been monitored. Uzbek authorities appear to be monitoring phones calls and emails of Uzbeks working on what state authorities perceive to be politically sensitive topics, often using transcripts of private communications in criminal proceedings against them. In some cases, authorities also appear to have obtained access to VoIP communications such as Skype. While the methods and stories vary, the accounts evidence the politically-motivated nature of surveillance in Uzbekistan.

The main targets of the SNB's electronic surveillance efforts are business leaders with perceived political influence and members of the political elite. Human rights activists and journalists are targeted where they are considered a viable threat to the regime.

In 2013, when the SNB arrested Nabidzan Dzurabaev for allegedly attempting to topple the government, his wife enlisted the help of Mamur Azimov, a local human rights lawyer. Azimov in turn contacted Talib Yakubov, an Uzbek human rights campaigner in France. The three men discussed Dzurabaev's case on Skype repeatedly. The SNB summoned Dzurabaev's wife and ordered her to stop passing information to Yakubov in France, or face jail time. Azimov was also summoned to the SNB offices, and ordered not to communicate with either Mr. Yakubov or Mr. Dzurabaev's wife. Azimov claims that a transcript of his mobile phone conversations for the entire month of May 2013 was produced at his sentencing, despite not being under formal investigation until 30 May.

In several cases Uzbek authorities appear to have obtained transcripts of Skype conversations. In the autumn of 2013, Kudrat Rasulov, a young Uzbek journalist, contacted two exiled Uzbek opposition politicians and human rights activists, Tulkin Koraev and Mukhamad Solikh. The three viewed a documentary about corruption and non-violent resistance on YouTube,[68] which Rasulov later forwarded to his friends in Uzbekistan. On 27 December 2013, Rasulov was found guilty of transmitting undesirable content over Skype and Facebook with the intention to destabilize the state and political order. He is serving an eight-year sentence as a result.

In 2012, in another case involving Skype, Fazliddin Zayniddinov, based in Uzbekistan, used Skype to contact Mukhamadsalikh Abutov, a political blogger and a religious leader who had immigrated to Sweden after serving a jail sentence. They discussed religious subjects. Some months later Zayniddinov was jailed, and in May 2013 was featured in a state sponsored YouTube documentary that accused Zayniddinov of paying Abutov US$100 to topple the Uzbek government.[69] According to them both, they had had no contact with each other except by Skype.

Communications surveillance complements physical spying and other intelligence gathering techniques in Uzbekistan. In the case of Alex Sherm and several of his family members, communications surveillance and physical monitoring came close to destroying their lives. From 2002 to 2004, while Sherm was First Deputy Assistant Treasurer of the Uzbek National Treasury, he accused a group of other ministers of sending the country into financial ruin. During this time, he suspected that his phone calls and emails were being monitored. His wife was writing an academic dissertation that required her to meet with foreign political entities and ambassadors; the SNB described these meetings to him in great detail, suggesting that his wife was also being monitored. Sherm believes that the extent of detail cited by the SNB agents shows that his home phone and his computer were being monitored. In 2004, he decided to leave everything behind – his family, friends, and career – to move to the United States. He even refrained from communicating with his family because he suspected they were monitored, on the basis of this past experience and because he had previously contacted one relative whose small business was subsequently damaged by an unexplained fire.

The surveillance of Sherm's calls – or of those of his interlocutors – combined with physical surveillance almost had deadly consequences. In 2011, he reported to the Human Rights Watch Uzbekistan Office Director that his family was being threatened and monitored. Human Rights Watch agreed to meet Sherm's family members, Gulnoza Rizaeva and Anvar Rizaev. The family and a Human Rights Watch employee communicated by mobile phones. Immediately following their meeting, Rizaev and Rizaeva were in a car crash. Other family members were also summoned to the SNB offices and questioned extensively regarding their correspondence with Human Rights Watch and Sherm. Sherm's family are issued summons by the SNB if Sherm attempts to contact them. He now prefers to keep away for their own safety.

68 "Қуролсиз кишининг озодлиги (ўзб.)", 10 November 2011, available at http://www.youtube.com/watch?v=sSdRF2QQc08

69 "Vatangadolar", 24 May 2012, available at https://www.youtube.com/watch?v=hQ7Lew98xNo

Mutabar Tadjibayeva, a lawyer, has had persons close to her killed following conversations with them. In May 2005, Tadjibayeva received a call to her cell phone by Sharif Shakirov; they discussed the massacre of protesters at Andijan then unfolding in eastern Uzbekistan. Tadjibayeva soon received another phone call from the counterterrorism department of the Uzbek Ministry of Internal Affairs. The agent told her she must remain at home for the next ten minutes, during which time she would receive a visit from SNB agents. At her home, SNB officers told her that she was not permitted to go to Andijan and placed her under house arrest. When she continued to circulate the information on Andijan via her mail.ru email account and mobile phone, Tadjibayeva received another phone call from the counterterrorism department telling her that should she not stop circulating this information she would be arrested and treated as a terrorism suspect.[70]

On 7 October 2005, Tadjibaeva was contacted by a United Arab Emirates-based correspondent for the UN's Integrated Regional Information Networks (IRIN). He asked to see all files related to the massacre, including evidence of gross violations of human rights by Uzbek authorities. Tadjibaeva disregarded the warnings she had received and provided IRIN with the files she possessed regarding the massacre, sending them from her mail.ru account. Tadjibayeva was arrested later that day. People featuring in the documents were contacted by SNB and testified against Tadjibayeva. She was then sentenced to five years and claims to have been tortured during her interrogation and detention. Tajibayeva's computer files were destroyed by the SNB during the trial. No alternative copy of the documents exists.

Tadjibayeva has good reason to suspect her communications are still being monitored by Uzbek authorities. Though she received asylum in France, Tadjibayeva claims that any time she speaks to individuals who need human rights assistance in Uzbekistan via phone, email or even internet programs like VoipGain, they are approached by SNB agents and pressured into ceasing communication with her. At the end 2013, Tadjibayeva used VoipGain to call the mobile of the Uzbekistan-based brother of a political prisoner[71] about financial support for families of political prisoners. A doctored version of the conversation was then made available to a pro-government media outlet via an SNB email account, according to a source with close knowledge of the incident.[72]

Privacy International spoke to Uzbek activists who claim to have had their Facebook and other social media accounts accessed and have been called in for questioning by SNB agents. Tulkin Karaev, an Uzbek human rights activist now living in Sweden after being forced to flee Uzbeikistan as a result of mounting pressure from the authorities and growing security concerns, suspects that a number of his devices and accounts have been hacked. His Gmail account has been repeatedly hijacked by what Karaev says can only be the SNB. Karaev had managed to reclaim his inbox through Gmail's recovery procedures only to find the inbox linked to an unfamiliar email address and

70 "Шерше ля фам для исламистов", War and Peace, 24 October 2009, available at http://www.warandpeace.ru/ru/commentaries/view/40600

71 Who cannot be named for security reasons.

72 Who cannot be named for security reasons.

an Uzbek number instead of his own Swedish number. When he confronted the owner of the unfamiliar address, the responder used aggressive language and attempted to blackmail Karaev, stating that he was now in possession of Karaev's entire Gmail archive as well as all contacts, which he would use as he pleased should Karaev continue to contact him. Karaev continues to receive dozen of SMS from Google's Gmail notifying him that someone is attempting to log into his account.

Farkhodon Mukhtarov of the Human Rights Alliance of Uzbekistan[73] struggles to single out specific examples of surveillance from his own experience. After the 13 May 2005 Andijan massacre in particular, Mukhtarov reports that monitoring and pressure on human rights campaigners increased substantially. Mukhtarov himself noticed that he was being followed. He tried to evade his surveillants by using multiple internet cafes in the course of one day in order not to endanger just any one e-cafe owner. In autumn 2006, when he was sure he was not being watched, he went to a trusted venue near the Guncha Cinema in the capital, Tashkent, and downloaded the anonymizer software "Анониммаус" in order to access content blocked in Uzbekistan. SNB agents raided the cafe two hours later, scanning the computers and quizzing the owners regarding the usage of the anonymizer. In 2008, Mukhtarov was arrested and sentenced to six years for alleged fraud. He served only two years following international pressure.[72] He claims many of his possessions vanished from his apartment during the preliminary investigation and that he has not been able the recover the email addresses he used at the time of his arrest.

72 "Uzbekistan: Activist's Release Shows Sustained Pressure Works", Human Rights Watch, 5 December 2010, available at http://www.hrw.org/news/2010/12/04/uzbekistan-activist-s-release-shows-sustained-pressure-works

Monitoring Centres

Monitoring centres with mass surveillance capabilities have been provided to both Kazakhstan and Uzbekistan by the Israeli branch of the US-based Verint Systems and by the Israel-based NICE Systems, according to confidential sources, whose accounts have been corroborated by Privacy International. These monitoring centres are capable of mass interception of telephone, mobile, and IP networks. Such a system means that the communications of every individual are within the reach of the security and law enforcement agencies. While some technical limitations to the ability to analyse intercepted material exist, future upgrades can be made using the enabling infrastructure. Training and technical support is also provided by NICE and Verint engineers to maintain the centres. Communication service providers operating in the region are required to subcontract to a local company to ensure the SORM functionality of their equipment, and to have their networks connected to the monitoring centres. CSPs do not have direct legal access to the monitoring centre, and are not informed of the activities taking place there, nor are they provided with a justification or legitimate authority when data on an individual user is requested.

Verint Israel's contracts in Central Asia are approved by the Israeli national security apparatus, to which Verint Israel has extensive ties.[75] In line with its wider global strategy, Israel seeks to build international support through economic and military ties, to build military and commercial relationships in order to generate revenue for its military and intelligence establishments, and to receive military and intelligence cooperation. The proximity of the Central Asian region to Israel itself, the fact that it consists of nominally Islamic countries, its proximity to Iran, and to the wider Middle East, all act as strong foreign policy incentives for Israel. Reports from 2012 indicate Kazakhstan is in negotiations with Israeli company Elbit to set up drone manufacturing in the country.[76] Israel and Kazakhstan formally signed a defense agreement in 2014 which will see increasing Israeli defense exports to the country.[77]

75 "Israeli Spy Companies: Verint and Narus", Richard Sanders, Press for Conversion, Spring 2012, Issue No. 66, available at http://coat.ncf.ca/P4C/66/spy.pdf; "Shady Companies With Ties to Israel Wiretap the U.S. for the NSA", James Bamford, 3 April 2012, Wired, available at http://www.wired.com/2012/04/shady-companies-nsa/all/1; O'Harrow, Robert, "No Place to Hide", Simon and Schuster, 2006, p297

76 "External Support for Central Asian Military and Security Forces", Dmitry Gorenburg, Stockholm International Peace Research Institute and Open Society Foundations, January 2014, available at http://www.sipri.org/research/security/afghanistan/central-asia-security/publications/SIPRI-OSFno1WP.pdf

77 "Israel Signs Defense Agreement With Kazakhstan", Ari Yashar, Israel National News, 21 January 2014 http://www.israelnationalnews.com/News/News.aspx/176567#.U9prnXkdtn0

Company Profile

Verint Israel

Verint Israel is the Israeli office of Verint Systems, a US-based Nasdaq-listed software and hardware manufacturer specialising in data analytics and intelligence solutions. Verint describes itself as "a global leader in Actionable Intelligence" providing "solutions for customer engagement optimisation, security intelligence, and fraud, risk and compliance" with "more than 10,000 organisations in over 180 countries [using] Verint solutions to improve enterprise performance and make the world a safer place." To the year ending January 2014, Verint posted revenue of US$910 million.[76]

Verint was originally part of Comverse Technology, but in 2013 it acquired Comverse's stake. Comverse Technology was founded in Israel by, among others, Jacob 'Kobi' Alexander, who in 2006 was involved in a serious options backdating scandal.[79] As reported by James Bamford, during the 2000s, Verint was involved in supplying the wiretapping equipment to Verizon during the National Security Agency warrantless wiretapping scandal.[80]

Verint's current focuses include 'Enterprise Workforce Optimisation,' which involves call centres and call centre optimization solutions, as well as 'Video and Situation Intelligence,' which includes advanced cameras and analytical tools typically used around critical infrastructure and for national security. As part of its 'Communications & Cyber Intelligence' section, Verint sells cyber security solutions, mobile tracking technology, off-the-air interception devices used to intercept mobile calls, and open source analytical tools. Its SkyLock system claims to be able to track the location of a mobile phone anywhere in the world.[81] Targeted at CSPs and law enforcement and intelligence agencies, Verint sells monitoring centres that "enable the interception, monitoring, and analysis of target and mass communications over virtually any network" which, according to Verint's website, are in use in more than 75 countries.[82]

76 Verint, Press Release, Verint Announces Fourth Quarter and Full Year Results, http://www.verint.com/assets/verint/documents/january-31-2014-earnings-press-release exhibit-99%201_3_31_14.pdf?_ga=1.84395997.57461801.1410275227

79 "In a Faded Wall St. Scandal, Lessons for a Current One", Solomon, S, 26 March 2013 available at http://dealbook.nytimes.com/2013/03/26/in-a-faded-wall-st-scandal-lessons-for-a-current-one/?_r=0

80 Bamford, James, "The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America", 2008, Knopf Doubleday Publishing Group 81 "For sale: Systems that can secretly track where cellphone users go around the globe" Timberg, Craig. Washington Post, August 2014, http://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html

82 "Verint to supply new Swiss spying system", Swiss Info, 15 January 2014, available at http://www.swissinfo.ch/eng/verint-to-supply-new-swiss-spying-system/37740006

Company Profile

NICE Systems

Originally a manufacturer of surveillance products for military users only, today NICE positions itself as "the worldwide leader of intent-based solutions that capture and analyze interactions and transactions, realize intent, and extract and leverage insights to deliver impact in real time."[84] Founded by seven former members of the Israeli Army,[85] it is based in Israel, though its shares are also traded on the US NASDAQ.

NICE has three main branches: NICE Enterprise, focusing on call centres and associated products including big data analytics and voice analysis, NICE Actimize focusing on analytical solutions for financial institutions to meet financial compliance requirements including anti-money laundering, and NICE Security. NICE Security offers video-based surveillance solutions and associated analytics, as well as electronic surveillance technologies including tools for the interception of satellite phones. NICE monitoring centres include capabilities to intercept, on a mass scale, telephone, mobile and IP data, and a location tracking centre that allows users to "Locate anyone, anytime, anywhere" via mobile phones.[87] NICE also markets various other analytical components that can be used in a monitoring centre, such as a Pattern Analyzer which aims to "identify behavior irregularities that may point to criminal or terrorist activities."[87]

NICE lists some 25,000 organizations in more than 150 countries as customers, including over 80 Fortune 100 companies. NICE Security lists the Statue of Liberty, Beijing Metro, New York Police Department, and the Eiffel Tower among its list of projects.[88] NICE's reported revenues in 2013 totalled US$951 million, a company record driven by "continued market demand and the growth of our analytics based advanced applications...in all business segments and geographies."[89] Haaretz reports that WikiLeaks disclosures show NICE "has technology that is used to monitor some 1.5 billion people."[90]

82 "Verint to supply new Swiss spying system", Swiss Info, 15 January 2014, available at http://www.swissinfo.ch/eng/verint-to-supply-new-swiss-spying-system/37740006

83 "Verint to supply new Swiss spying system", Swiss Info, 15 January 2014, available at http://www.swissinfo.ch/eng/verint-to-supply-new-swiss-spying-system/37740006

84 NICE Systems, Company Overview http://www.nice.com/company-overview

85 NICE Systems Newsletter, Volume 2, Issue 3, 2006, http://www.nice.com/news/newsletter/6_03s/anniversary.php

86 NICE Systems, Location Tracking, http://www.nice.com/intelligence-lea/location-tracking

87 NICE Systems, Pattern Analyzer, http://www.nice.com/intelligence-lea/pattern-analyzer

88 NICE Systems, Company Overview http://www.nice.com/company-overview

89 NICE Systems, NICE Reports Record Revenues and EPS for the Fourth Quarter and Full Year 2013, http://www.nice.com/nice-reports-record-revenues-and-eps-fourth-quarter-and-full-year-2013

90 "In Ex-Soviet States, Russian Spy Tech Still Watches You", Orr Hirschauge, Haaretz, 10 June 2013, limited access available at http://www.haaretz.com/business/.premium-1.528811

Kazakhstan's Monitoring Centres

Verint Israel and NICE Systems both maintain monitoring centres in Kazakhstan, contracted directly by the Kazakh National Security Committee (KNB). In Astana, the two monitoring centres are located in the same building on Kenesary Street. Both Verint Israel and NICE also provided and maintain monitoring centres in Almaty.

Verint Israel has had contracts in place with the KNB relating to monitoring centres since the early 2000s. The contracts were concluded by the KNB which is, itself, responsible for paying Verint. As a result, Verint is subject to less rigorous oversight and regulation in the country than CSPs and other contractors, which typically need operating licenses. Since the early 2000s, Verint Israel's monitoring centre has facilitated requests for telephone-based intercepts by the KNB. In 2012, the monitoring centre was upgraded to allow access to IP data via Deep Packet Inspection (DPI) techniques. DPI technology is commonly used to facilitate data flows through networks. Among its uses is traffic routing, the management of network congestion, scanning for malicious packets, and the collection of statistical information. As these techniques analyse and monitor traffic, they are, by design, suitable for electronic surveillance, and are widely used for electronic surveillance and censorship across the world. The 'depth' of DPI technology can vary widely – ranging from applications that can only identify limited metadata about traffic, to some technology that can read the content of communications. Generally, DPI can allow officers to query requests based on any selector, such as a user's IP address.

Verint describes its monitoring centres as being split into two functional areas: a 'back-end', consisting of the monitoring centre itself where analysts request and receive data, and a 'front-end' located within the telecommunications network itself, which intercepts the data before subsequently sending it to the monitoring centre.[91] Across Kazakhstan, network nodes used by communications services providers are fitted with taps that are then connected to the monitoring centre. Most commonly, a local company that is certified to ensure networks are compliant with SORM will carry out the installation and configuration of the cables. When a request for data is made at the monitoring centre, the appropriate front-ends of the system located within the network respond by intercepting the data and forwarding it on to the back-end.

The centre is managed and used by the KNB directly, though technical maintenance is carried out by two employees working directly for Verint based in Kazakhstan.

NICE Systems' services were contracted for by the KNB in 2013, when they were given a DPI project similar to Verint's. NICE's monitoring centre is located in the same building as Verint Israel's, directly across the hall.

91 Verint, Press Release,Verint Selected To Provide Law Enforcement Communications Interception Solution To A New Customer In Asia Pacific, July 2002, http://phx.corporate-ir.net/phoenix.zhtml?c=131043&p=irol-newsArticle_print&ID=312250&highlight=

Uzbekistan's Monitoring Centres

Both Verint Israel and NICE Systems also maintain monitoring centres in Uzbekistan. As opposed to telecommunications providers, which are required to have a license in order to operate in the country, Verint and NICE are exempt by virtue of being contracted directly by the SNB. These CSPs are required to make their networks directly accessible to the monitoring centre where each CSP has its own dedicated server rack to handle the information received from the network. The required servers are manufactured by large multinational server manufacturers and storage provided by Netapp and EMC.

Verint has provided a turn-key monitoring centre in Uzbekistan since the early 2000s based in Gazalkent district in the capital, Tashkent. Verint is contracted to provide not only the monitoring centre, but also technical maintenance, and has maintained it on an ongoing basis. Local IT specialists oversee the centre with the help of Verint employees. Verint and NICE employees travel to the Central Asian republics, where the monitoring centres are situated, and are accompanied by SNB agents at all times, while Uzbek authorities and technicians also come to Verint Israel's Tel Aviv office to see the development of projects.

The project initially focused on circuit-switched PSTN (telephone) interception, facilitating requests for metadata concerning a particular call from an individual person (known as Intercept Related Information (IRI)), or recording of calls (known as Communications Content (CC)). In 2012 Verint upgraded the monitoring centre with DPI capabilities allowing the centre to intercept internet data. Similar to Kazakhstan, such DPI capabilities would allow authorities access to a wide range of IP data.

Verint also provided a mediation device in 2012. One Verint mediation device, Star-Gate, receives intercepted information communication content and data from the access provider, converts the collected data format into the requisite format, and then delivers the data directly to the appropriate law enforcement agency.[92]

The number of targets for each telecom varies throughout the year. In 2013, the number of subscribers being targeted at any one time for IP-based interception was between 300 and 600, near the system's maximum capacity. The amount of targets for targeted circuit-switched based interception was in the thousands.

Verint has also attempted, at the request of the SNB, to provide an SSL man-in-the-middle capability (MITM) in order to gain access to SSL-encrypted communications, such as those now offered by default by Gmail, Facebook and other service providers. Netronome, an American company owned by Blue Coat was chosen to facilitate the replacing of the certificate. To use this capability a limited number of IP

92 See Comverse Infosys, "STAR-GATE Annex: Intercepting Packet Data Compliance with CALEA and ETSI Delivery and Administration Standards" available at http://www.quintessenz.at/doqs/000100002079/Verint%20-%20STAR-GATE,%20Interception%20of%20Packet%20Data%20.pdf

addresses are flagged and when traffic from those IP addresses passes through the tap, the packets are forwarded to the SSL device which MITMs the connection presenting a self-signed certificate. It is not known whether this capability is being deployed on a broad scale, or whether it has been reliably deployed.

Verint's monitoring centre in Uzbekistan is a highly secure facility guarded by armed guards. It also has heat detectors and video cameras installed to observe the perimeter outside. Both monitoring centres are located inside the police and military industrial district in Gazalkent District in Tashkent, Uzbekistan's capital.

Similar to Verint Israel, NICE Systems has also maintained a contract for a monitoring centre in Uzbekistan since the early 2000s, which was similarly upgraded to intercept IP data in 2012. The location of NICE's monitoring centre and the names of their on-site staffers in Uzbekistan are unconfirmed at this time.

The SNB has two different monitoring centres functionally carrying out the same tasks in order to, variously, cross-check the data obtained by the monitoring centres, balance and compare the results, see if one comes out on top of another, and to make the companies compete so that the SNB gets the best price.

Kyrgyzstan's Monitoring Centres

Kyrgyzstan likely uses monitoring centres supplied by a Russian developer. Russian manufacturers of monitoring centres have a particular advantage in Central Asia given their familiarity with the SORM architecture and with the telecommunications infrastructure and hardware. The Kyrgyz parliament's Defense and Security Committee decided in 2012 to use a Russian company to connect the telecommunications networks to a monitoring centre as it would be three times cheaper than a system offered by Verint.[93]

Tajikistan's Monitoring Centres

A 2010 document obtained by Privacy International shows that the German company Trovicor GmbH had marketed a monitoring centre "for all cellular networks" to the Ministry of the Interior of Tajikistan in 2009, though it is unknown if the sale went ahead. Trovicor's monitoring centres were previously sold by Siemens and then telecommunications equipment manufacturer Nokia Siemens Networks (NSN). NSN used to sell monitoring centres directly as part of its network infrastructure solutions. After becoming embroiled in controversy following its provision to Iran of a monitoring centre in 2009, the monitoring centre business was sold to a private equity fund and reincarnated as German-based Trovicor Intelligence Solutions.[94]

93 "In Ex-Soviet States, Russian Spy Tech Still Watches You", Andrei Soldatov and Irinia Borogan, Wired, 21 December 2012, available at http://www.wired.com/2012/12/russias-hand/all/

94 "In Ex-Soviet States, Russian Spy Tech Still Watches You", Andrei Soldatov and Irinia Borogan, Wired, 21 December 2012, available at http://www.wired.com/2012/12/russias-hand/all/

Also listed within the proposals was a “LIMS” solution. LIMS stands for Lawful Interception Management System, a device commonly used within monitoring centres and manufactured by the German company Utimaco. LIMS is a mediation platform which carries out administrative functions between the network nodes of CSPs and the monitoring centre. The functions include the storage of data, decoding, and the management of access rights.

Kazakhstan's Punkt Upravlenias (PUs)

Key

Monitoring Centre

PU Location

In addition to the monitoring centres sold directly to the KNB for their exclusive use, Kazakhstan's authorities also rely on distributed monitoring nodes called PUs to manage and access intelligence from smaller segments of the network. Within the Russian SORM architecture, the interception of networks is managed by a PU connected to switching nodes within the network and communication lines.[95] These PUs are purchased directly by CSPs and connected to their network. Typically, small local telecommunications companies act as the prime bidder for the supply of PUs, although they maintain commercial partnerships with several larger foreign-based companies which manufacture the necessary hardware. Several other companies certify, test, and maintain PUs throughout Kazakhstan.

95 "Lawful interception of messages: Approaches ETSI, CALEA and Lawful", B.C. Goldstein and B.C. Elagin, Journal Herald of communication, No. 3, 2007, available at http://files.iks.sut.ru/publications/2007-016.pdf

In 2013, TNS-Service, a Kazakh re-seller of telecommunications equipment, won a contract worth roughly €853,000 to supply a PU to Kazakhstan's largest and majority-state owned CSP, Kazakhtelecom. Connected to Kazakhtelecom's network, the centre facilitates the monitoring of the telephone calls of just under 180,000 subscribers in Aktobe, a major oil producing city, and over 520,000 subscribers in Almaty, Kazakhstan's largest city. It is intended that the monitoring system be able to support at least 100 simultaneous interceptions. The PU connects to digital switches produced by large international telecommunications equipment manufacturers. These switches are able to follow a range of interception protocols which allow authorities to access data, including the European ETSI protocol, the US CALEA, and Kazakhstan's own standard, or alternatively converters can be used to provide access.. The PU in Almaty subsequently connects to the switching system of Almaty Region, Jambyl, Kyzylorda, and South Kazakhstan Region, while the PU at Aktobe connects to the Mantistau, Atyrau, and West Kazakhstan Regions' switching systems.

According to tender documents, the PU centre consists of two components: an Interception Management System (EMS) and a Monitoring System (CM). The EMS serves as a centralized server for provisioning and managing interceptions, acting as an interface between agents and the intercepted material, storing and managing interceptions, and managing user access rights. It serves as a centralized control device connected to the switches and data network interfaces, and "must support a minimum of interfaces and protocols to intercept the following major manufacturers of communication and switching equipment: Alcatel Lucent, Nortel / Genband, Cisco, Ericsson, Nokia-Siemens, Huawei, Broadsoft, Juniper." The user interface also maintains a central database of all the intercepts requested, and provides a single point of initialization, administration, auditing, security monitoring and reporting.

Generally, CMs connect to the telecommunications network and are used to intercept the content of communications and data by conducting data collection and storage, and then preparing the intercepted material in the format required for the EMS. The CM is built around a central core in which all the data contents and processed intercepted data are stored and made available. It collects and decodes both audio information and IP data, providing for "an automated, constantly working mechanism to record any sound and intercepted packet content." The content of the intercepted messages is said to fall into one of two categories: audio communication (such as the sound of telephone conversations), and non-audio communication (such as text messaging or content faxing, etc.) as well as IP data (e-mails, web browser, etc).

"Reproduction, transcript, translation, review, reporting, and analysis" is then performed for processing audio and packet information, regardless of where the material was intercepted from within the telecommunications network.

According to tender documents, the entire PU system should also:

— Provide the user with a variety of tools to manage, select and view the collected information. For processing the recorded session, the system should provide the ability to choose the speed and direction of playback recordings or parts.

— Provide the user with a rewind/fast-foward function to enable the the user to go to the beginning or end of the track.

— Be equipped with a minimum of functions of the graphic equalizer, including the ability to remove noise and change the tone without changing the tempo record.

— Allow handlers to search by date / date and time.

— Allow handlers to search the data according to various fields of classification such as, labelling, status, and other attributes of the session.

— Provide handlers for the window automatically output a list of the most recent sessions over a period of time specified by the user.

— Have a field for the status of each individual session, which is automatically filled by the system.

— In playback mode, the screen should display a visual representation of the sound track before the interception system.

The system "must be designed for continuous operation without interruption, 24 hours a day, 365 days a year."The winner of the tender, TNS-Service, acts as a prime contractor, and is a re-seller for various commercial manufacturers of telecommunications equipment abroad.[96] Ronex and OTC Network, two other Kazakh telecommunications equipment re-sellers, also bid as part of the tender process. An archived version of TNS-Service's website from 2010 describes the company as having worked in the telecommunications industry since 2010 and having "all necessary licenses and permissions including a Permission for work connected with the Defense of State secrets and a License for delivery of special technical devices for the entities of operative-detection activity [SORM],"[97] and having had supplied and installed "various telecommunication equipment and special technical equipment" for the KNB.[98]

Tender documents show that a PU capable of intercepting the telephone calls of up to 8500 subscribers was sought in March 2014 by a subsidiary of the state-owned nuclear company Kazatomprom, as well as by Bailanys, a company that provides

96 For example: Tait, available at http://www.taitradio.com/our-partners/reseller-partners/europe-middle-east-africa

97 "About the company", TNS Service, available at http://web.archive.org/web/20100822023054/http://www.tns-service.kz/page.php?page_id=144&lang=1

98 See TNS Service website, available at http://web.archive.org/web/20100822023054/http://www.tns-service.kz/page.php?page_id=89&lang=1&parent_id=34

landline telephone services. The PU, to be delivered to Almaty, is to be connected to switches via E1 cables, and should contain a device for collection, and servers for storing and processing information. The tender specifies that the PU is to have several collection devices compatible with Odyssey-BPS-15, which belongs to a Kazakh surveillance company Pro-tech. Odyssey-BPS-15 functions within the broader PU to intercept 1 -15 E1 lines, according to Pro-Tech's website.[99] The only bidder for the tender, worth some €50,500, was Pro-Tech.

A tender for support services for SORM centres, including repair, lists some 34 switching centres across Kazakhstan as being engaged in the transmission of voice data to a PU.

In September 2012, Protei – a large provider of telecommunications equipment and services, including monitoring centres for SORM – completed installation of advanced network equipment for a Kazakh operator, Nursat, in conjunction with local company Ronex, which is listed as a sales partner. The installation involved the provision of SORM-compatible equipment for use on Nursat's network. Included was a softswitch in Almaty and IP-telephony gateways in 17 cities across Kazakhstan. Protei claims that a "key technical feature of the project was the implementation of functional SORM for the entire network using a single access point. The switch has a built in Switch5 SORM subsystem, which provides remote access to different segments of the network with the possibility of setting on a control in all regions." According to Protei, the centralised application has proved successful, and, as a solution, cost-effective for the provider.

Further surveillance systems and capabilities are then enabled, which transmit intercepted data to a PU. A system for the active monitoring of internet users was sought in 2013 for use in the PU in Almaty. The system transmits copies of targeted users' traffic to the PU, and is located on five telecommunications nodes on broadband infrastructure manufactured by Juniper, a large telecommunications equipment manufacturer.

Altel, another Kazakh CSP and Kazakhtelecom subsidiary, sought in 2011 to install an SMS interception system capable of intercepting SMS messages at a maximum rate of 200 per second and storing them for a minimum of three years. Re-sellers Ronex and OTC Networks both bid for the contract. The system integrates the PU interception system with a SMS Centre, a transport platform that allows operators to deliver SMS functionality across their networks.

The system responds to requests from the PU and then forwards intercepted messages back to it. It is to be able to:

— Record information in a database (the database);

99 "АПК 'Одиссей'", Pro-tech, available at http://www.pro-tech.kz/index.php/produkty/sorm-1/apk-odissej

— Allow for searching through the database by keywords, including phone number, IMSI, date and time of SMS sending and receiving, and any text contained in the SMS;

— Storage of information for the required time period in accordance with the technical requirements of the customer (not less than three years);

— Handle a traffic flow of at least 200 messages per second with the possibility of further expansion; and

— The timing of the selection parameters posts should be less than 30 seconds after receiving from the PU data on the parameters of selection.

Signatec marketed products include ALOE Systems' NetBeholder[100] and IP SORM January, manufactured by MFI-SOFT, fulfilling the functions of SORM-3.[101]

'NetBeholder' is produced and sold by the Canadian based ALOE Systems, which acts as an agent for MFI-SOFT. Consisting of both hardware and software, the system is marketed as "a high-end system for lawful interception that performs detection, monitoring, storage and analysis of all types of information circulating over IP networks - including web, email, Instant Messengers, VoIP and many more."[102]

'NetBeholder' is produced and sold by the Canadian based ALOE Systems, which acts as an agent for MFI-SOFT. Consisting of both hardware and software, the system is marketed as "a high-end system for lawful interception that performs detection, monitoring, storage and analysis of all types of information circulating over IP networks - including web, email, Instant Messengers, VoIP and many more."[102]

Once a subscriber is targeted via a selector consisting of, for example, an email, IP address, or keyword, the system's probes are used to copy and collect the relevant data before storing it in a database. NetBeholder passes intercepted information via a dedicated cable to a PU at a bandwidth of at least 10 Mbit/s for the volume of traffic processed more than 1 Gb/s.

'IP SORM January' is capable of intercepting all telephone calls, SMSs, MMSs, and internet activity and provides agencies with quick access via a PU. It is also capable of identifying the location of subscribers, of handling 100 simultaneous searches, and of storing intercepts for three years. This level of information means that it is able to store more than 10 terabytes of data, roughly equivalent to the US Library of Congress.

100 "АПК 'NetBeholder'", Pro-tech, available at http://www.pro-tech.kz/index.php/produkty/sorm-2/netbeholder

101 "ИС СОРМ 'Январь'", Pro-tech, available at http://www.pro-tech.kz/index.php/produkty/sorm-3/ls-sorm-yanvar

102 "Products", Net Beholder, available at http://web.archive.org/web/20110527205523/http://www.netbeholder.com/en/products.html

Riders on the SORM: The Role of CSPs

Communications service providers typically provide law enforcement agencies (LEAs) with access their networks and subscribers' data when operating in a country. However, the extent of access, and the circumstances under which and conditions on which it is provided, varies greatly depending upon the relevant legal and political context.

The growth of modern digital networks during the 1990s saw the introduction of legislation and protocols including CALEA and ETSI LI in the US and Europe respectively. The advent of these frameworks, aimed at ensuring security agencies had the same ability to intercept communications as they had in the age of the circuit-switched telephone, ensured that all telecommunications network equipment manufacturers and CSPs were henceforth obliged to design telecommunication infrastructure to be accessible by states.

As the demand for modern telecommunications infrastructure and operators has grown in emerging markets, American and European companies, accustomed to providing interception-ready products and services, were well placed to expand their operations abroad. However, whereas the development and provision of Lawful Interception capabilties by CSPs in the US and Europe has traditionally been in the context of robust legal constraints on state surveillance activities, the extension of such capabiltiies to emerging markets poses serious questions about the responsibilities of CSPs.

Furthermore, the direct access mandated under the SORM model represents a departure from American and European Lawful Interception protocols and a considerable challenge to the protection of individual human rights. In the Russian SORM model for circuit-switched networks, the PU is connected directly to node connections within the network. SORM thus allows states to intercept and analyse citizens' communications within a more limited system of checks and balances. As such, CSPs operating on SORM networks have little meaningful opportunity to monitor and control state agencies' interception activities and or mediate the access the state has to subscribers' data. According to Boris Goldstein, a professor at the Bonch-Bruevich State St. Petersburg University of Telecommunications and a leading expert on the technical aspects of SORM, while in the US and Europe CSPs play a more direct role in facilitating access, the functioning of SORM rests entirely on the PU and on the agency under which it is used, and avoids the requirement to establish judicial authority and permission of the CSP.[103]

103 "Lawful interception of messages: Approaches ETSI, CALEA and Lawful", B.C. Goldstein and B.C. Elagin, Journal Herald of communication, No. 3, 2007, available at http://files.iks.sut.ru/publications/2007-016.pdf

Foreign investors and CSPs operating in the region represent the only commercial entities realistically able to challenge unlawful or arbitrary access to their networks. Yet the direct form of access to CSPs' networks available to national security agencies under SORM means that these CSPs are limited in their ability to challenge state demands. Domestic CSPs in the republics, although dominant in large areas of the market, are largely state-owned and are therefore ill-placed to resist illegitimate and unnecessary access to their networks.

Kazakhstan (2012) [104]

Population	16,700,000
Fixed Line Subscribers	4,300,000
Mobile Subscribers	28,700,000
Fixed Broadband Subcribers	1,600,000
Mobile Broadband Subscribers	up to 7,000,000

Kazakhstan's telecommunications infrastructure is dominated by the majority state-owned Kazakhtelecom. According to Kazakhstan's communications law, all ISPs and telecommunications network operators are mandated to connect their networks to a public network owned by Kazakhtelecom.[105] Foreign companies are prohibited from owning or operating trunk cables used to carry large amounts of data.[106] Kazakhtelecom has a 93 per cent market share of the fixed-line market while its market

104 "An In-Depth Study of Broadband Infrastructure in North and Central Asia", Economic and Social Commission for Asia and the Pacific,January 2014, available at http://www.unescap.org/sites/default/files/Broadband%20Infrastructure%20in%20North%20and%20Central%20Asia%20FINAL%20_English.pdf

105 "Kazakhstan", OpenNet Initiative, 2010, pp. 187, available at https://opennet.net/sites/opennet.net/files/ONI_Kazakhstan_2010.pdf

106 "Doing business in Kazakhstan 2013, Reach, relevance and reliability", Deloitte TCF, 2013, pp.8, available at http://www.deloitte.com/

share of the fixed broadband market is above 75 per cent. Altel, a Kazakhtelecom subsidiary, was as of 2013 the only operator licensed to operate advanced LTE technology.

Other major CSPs with foreign-owned assets include: TeliaSonera, a Swedish-Finnish CSP and parent company of Kcell, which, as of 2012, had a 50 per cent market share of the mobile telephony market; Russian operator VimpelCom, whose market share stood at 32 per cent; and Swedish operator Tele2, whose share was 13 per cent.

Kyrgyzstan (2012) [107]

Population	5,600,000
Fixed Line Subscribers	490,000
Mobile Subscribers	6,800,000
Fixed Broadband Subcribers	150,000
Mobile Broadband Subscribers	2,000,000

Despite attempts to privatise the state-owned operator Kyrgyztelecom, it remains government-controlled and is the leading ISP with a 60 per cent market share. It is one of only two providers of fixed-line services, the other being Saima Telecom, which is majority owned by a consortium of Russian investors. Kyrgyztelecom has a market share of over 90 per cent of the fixed-line market.

Other major CSPs with foreign-owned assets include Russian-based VimpelCom and MegaFon, which both provide mobile telephony services and have a 40 per cent market share each.

107 “An In-Depth Study of Broadband Infrastructure in North and Central Asia”, Economic and Social Commission for Asia and the Pacific, January 2014, available at http://www.unescap.org/sites/default/files/Broadband%20Infrastructure%20in%20North%20and%20Central%20Asia%20FINAL%20_English.pdf

Tajikistan (2012) [108]

Population	8,000,000
Fixed Line Subscribers	400,000
Mobile Subscribers	6,500,000
Fixed Broadband Subcribers	6000
Mobile Broadband Subscribers	50,000

State-owned Tajiktelecom is the country's dominant fixed-line operator and is a major internet service provider in the country.

Several foreign CSPs operate in the mobile telephony market, including: Babilon-Mobile, with a 35 per cent market share; Tcell (a subsidiary of TeliaSonera) with 35 per cent; MegaFon with 21 per cent; and Beeline/Tacom (a subsidiary of VimpelCom) with a 9 per cent market share.

Turkmenistan (2012) [109]

Population	5,200,000
Fixed Line Subscribers	575,000
Mobile Subscribers	4,500,000
Fixed Broadband Subcribers	2000
Mobile Broadband Subscribers	10,000

108 "An In-Depth Study of Broadband Infrastructure in North and Central Asia", Economic and Social Commission for Asia and the Pacific, January 2014, available at http://www.unescap.org/sites/default/files/Broadband%20Infrastructure%20in%20North%20and%20Central%20Asia%20FINAL%20_English.pdf

109 "An In-Depth Study of Broadband Infrastructure in North and Central Asia", Economic and Social Commission for Asia and the Pacific, January 2014, available at http://www.unescap.org/sites/default/files/Broadband%20Infrastructure%20in%20North%20and%20Central%20Asia%20FINAL%20_English.pdf

Turkmenistan lags behind the rest of the region in its telecommunications infrastructure. State-owned Turkmentelecom enjoys a near-monopoly of all telecommunications services in Turkmenistan. It is the only available provider of fixed-line and fixed-internet services, while its subsidiary, Altyn Asyr, is the market leader in the provision of mobile services, having launched a 3G network in 2010 and 4G in 2013.[110] Restrictively expensive rates charged by Turkmentelekom limit internet usage rates, and all online activity in internet cafes is recorded by state authorities.[111]

MTS Turkmenistan, a subsidiary of Russia's Mobile Telesystems, is the only foreign mobile services provider operating in the country and provides mobile data services via GPRS. The Turkmen Ministry of Communications signed an agreement with the Indian company TATA Communications in 2008 connecting Turkmenistan to the internet backbone via the Transit-Asia-Europe fibre optic cable. It is connected to other CIS states through a microwave radio relay via leased connections to the Moscow internet gateway switch. An exchange in the capital, Ashgabat, switches international traffic through Turkey via satellite. Turkmenistan's first telecommunications satellite, developed by the French defence contractor Thales, is due to be launched at the end of 2014.

All media, traditional and electronic, is highly censored.[112] After conducting tests, the OpenNet Initiative concluded that Turkmenistan's use of pervasive filtering techniques meant its internet access is one of the most restricted in the world.[113] In 2014 Reporters Without Borders named Turkmentelekom an 'Enemy of the Internet'.

Uzbekistan (2012) [114]

Population	30,000,000
Fixed Line Subscribers	1,960,000
Mobile Subscribers	20,000,000
Fixed Broadband Subcribers	200,000
Mobile Broadband Subscribers	500,000

112 "A Sobering Reality: Fundamental Freedoms in Kazakhstan, Turkmenistan and Uzbekistan, Twenty years after the Soviet Collapse", 2012, available at http://www.chrono-tm.org/en/wp-content/uploads/Summary-Central-Asia-Report-March-2012.pdf

113 "CIS Overview", OpenNet Initiative, 2010, available at https://opennet.net/sites/opennet.net/files/ONI_CIS_2010.pdf

114 "An In-Depth Study of Broadband Infrastructure in North and Central Asia", Economic and Social Commission for Asia and the Pacific, January 2014

Despite some efforts to privatise and attract investment in the Uzbek telecommunications sector, state-owned Uzbektelecom remains the dominant provider and owner of infrastructure. Uzbektelecom has exclusive ownership of the international gateways which facilitate cross-border connectivity between the national network and is the only Tier-1 ISP, meaning that all incoming and outgoing internet traffic passes through its switches.[115] Uzbektelecom is also the dominant provider of fixed-line telephony.[116]

Vimpelcom was the market leader in the supply of mobile telephony in 2012 with a share of 51 per cent, followed by TeliaSonera which maintained a share of 48 per cent. Both Vimpelcom and TeliaSonera's activities relating to bribery in Uzbekistan are currently under investigation by various national authorities.[117]

In 2012, MTS's Uzbek subsidiary had its license revoked by Uzbek authorities for various regulatory breaches, including taxation violations, leading to the termination of its operations, bankruptcy and the loss of some nine million subscribers.[118] A settlement between MTS and the Uzbekistan authorities in July 2014 will see MTS recommence operations in Uzbekistan.

East Telecom, a subsidiary of the South Korea-based KT Corporation, also operates fixed internet and fixed-line telephony services in Uzbekistan.

OpenNet Initiative concluded that Uzbekistan's internet access is as tightly restricted as that of China's and Iran's,[119] and in 2014 Reporters Without Borders named Uzbekistan an 'Enemy of the Internet'.

115 "Republic of Uzbekistan" in "Safety on the Line, Exposing the myth of mobile communication security", Freedom House, 2012 available at http://www.refworld.org/pdfid/502a0c540.pdf

116 "An In-Depth Study of Broadband Infrastructure in North and Central Asia", Economic and Social Commission for Asia and the Pacific, January 2014, available at http://www.unescap.org/sites/default/files/Broadband%20Infrastructure%20in%20North%20and%20Central%20Asia%20FINAL%20_English.pdf

117 TeliaSonera, Update on investigations of TeliaSonera's investments in Uzbekistan, http://www.teliasonera.com/en/newsroom/press-releases/2014/3/update-on-investigations-of-teliasoneras-investments-in-uzbekistan/ and "TeliaSonera, Vimpelcom and Karimova face anti-corruption probe", Telegrography, March 2014 available at http://www.telegeography.com/products/commsupdate/articles/2014/03/13/teliasonera-vimpelcom-and-karimova-face-anti-corruption-probe/

118 "MTS Will Return to Uzbek Mobile Market After Two-Year Hiatus", lya Khrennikov and Yuliya Fedorinova, Bloomberg, 31 July 2014, available at http://www.bloomberg.com/news/2014-07-31/mts-will-return-to-uzbek-mobile-market-after-two-year-hiatus.html

119 "CIS Overview", OpenNet Initiative, 2010, available at https://opennet.net/sites/opennet.net/files/ONI_CIS_2010.pdf

Privacy International wrote to the CSPs concerning some of the finding of this report. Their responses can be found in the annex to this report.

Swedish operator Tele2 concedes that “intercept activities are carried out in a highly confidential manner and therefore are unbeknownst to Tele2 Kazakhstan.”[120] Their role is limited to “the installation of technical equipment for SORM, provision of access to the equipment for designated state authorities and collection and retention of personal information of subscribers, as well as submission of the information to them at their lawful request.” Tele2 is not allowed to see any warrants for interception.

TeliaSonera acknowledges “the concerns following legislative, administrative, license or law enforcement requirements to which we must adhere but which may impact individual’s privacy and freedom of expression” and that in Central Asia “companies do not have oversight over how the systems work and how surveillance data is obtained and used.” TeliaSonera’s position on unrestricted real time access is that “Governments should not have such access to our networks and systems.” TeliaSonera considers that it “should retain operational and technical control” despite the apparent difficulty of their doing so in Central Asia.

Vimpelcom, which is majority owned by Russia’s Alfa Group and Norway-based CSP Telenor and operates in Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan, acknowledges that human rights concerns exist where governments are perceived to be using surveillance for political purposes rather than for reasons of public safety and that “the current situation is challenging and far from ideal.” Vimpelcom states that legal frameworks exist which allow “certain government agencies to access networks and data through relevant technologies on the basis of legal approvals in which the CSP has no involvement and where it has no ability, legally or technically, to obstruct or challenge.” Concerning its operations in Kazakhstan, Vimpelcom attests that “Kazakh legislation requires CSPs to install certain data collection/ processing equipment on telecommunications networks and facilitate direct access to the national security agency to such equipment and data, which leaves no room for the Business Unit to control or challenge such activities.”

120 “Privacy and Sorm”, Tele2, available http://www.tele2.com/Our-Responsibility/social/user-safety/privacy-and-sorm/

Telecommunications Equipment Manufacturers

Modern telecommunications infrastructure is made up of various networks and hardware, produced by numerous manufacturers, which are then used to transmit data and enable services. Equipment manufacturers may be contracted to provide variously large-scale network equipment to enable specific networks, or smaller components to facilitate transmission across networks and enable specific services. While the purpose of most equipment is to enable networks and not surveillance, in general, vendors will take into consideration national law enforcement requirements and ensure that their equipment is capable of fulfilling surveillance requirements. In certain circumstances, if equipment is not directly compatible with SORM requirements, converters are used to ensure functionality. Locally-based companies, licensed and certified to ensure SORM compliance, act as prime bidders for SORM-related contracts and as re-sellers, sourcing hardware and software, and ensuring that network components are SORM compliant.

Kazakhstan

Telecommunications equipment is either sold SORM-compatible or is subsequently made SORM-compatible by a company specialising in SORM certification. All SORM providers and distributors must be certified by various governmental bodies. One such company, Ronex, provides SORM-related certification and SORM installations to the Kazakh telecom industry. In addition to certification, Ronex also produces converters that are used to ensure switches and other equipment are SORM compliant. Ronex "has been working in the area of implementing functions for providing special law enforcement support system (SORM) since 2003." According to Ronex, there are currently "over 76 SORM converters operating on the networks of major service providers such as AO Ksell, AO Kazakhtelecom, AO Altel, TOO Mobile Telecom Service, etc."[121] Ronex lists subsidiaries of two of the world's largest telecommunications equipment manufacturers, Alcatel Kazakhstan and Ericsson Kazakhstan, as customers for SORM converters.[122] Ericsson confirmed in writing to Privacy International that, since its Lawful Interception Management System does not conform to the SORM requirement, it works with Ronex as a third party to ensure their systems are accessible to law enforcement.

Numerous local companies compete for SORM-related contracts in Kazakhstan with either a local CSP acting as the direct customer, or Samruk Kazana, the state-owned investment fund that owns Kazakhtelecom. These companies are sub-contracted by the CSP and serve as middlemen, ensuring the SORM functionality of network equipment and procuring the necessary technology and working as partners and

121 "Отдел СОРМ", Ronex Security, available at http://www.ronex.kz/index.php/2013-12-26-07-41-31

122 "Quick reference sheet", Ronex Security, available at http://www.ronex.kz/index.php/2013-12-25-08-15-11/2013-12-26-08-20-50

re-sellers with a number of foreign-based equipment manufacturers and providers of surveillance technology. Kazakh-based companies that have responded to SORM-related tenders issued by Kazakhtelecom, its subsidiary Altel, or Samruk Kazana, include:

— Zhetisu Networks Technologies;
— Ronex Security;
— Alatau Service;
— Pro-tech;
— Network Technologies;
— IP Lobastovaa;
— Eklo-Service;
— Arlan and Net Systems;
— TNS Service;
— Timir;
— Newstech Distribution;
— Arlan Si; and
— MDS Company.

Kazakhstan's technical architecture implementing SORM is based on intercepting communications and data from telecommunications switches and other network elements based across the country. From numerous SORM-related tenders, it is apparent that Kazakh telecommunications infrastructure relies on a substantial number of hardware network devices sold by the French company Alcatel-Lucent. These products, such as the S-12 switch, are used not only to transmit data but also to transmit data to PUs and monitoring centres for electronic surveillance. Alcatel confirmed to Privacy International in writing that its French-Chinese subsidiary, Alcatel Shanghai Bell, supplied SORM compatible S12 equipment in 2009 to Kazakhstan.

Telecommunications equipment provided by other foreign companies is also capable of integrating with a PU. A tender from late 2013, shows that Kazakhtelecom was seeking repair services for a SIP Platform, a protocol facilitating VoIP and other communication service over IP. The tender shows that Kazakhtelecom is in possession of lawful interception software from Broadsoft, a US company, from which Kazakhtelecom purchased a license for Lawful Interception for up to 30,000 users. Included within the tender is a bid to provide capability for monitoring four E1 lines or 112 simultaneous connections. The SORM functionality appears to have been carried out by a Russian company that specializes in the sale of SORM equipment, MFI Soft. A tender for the software from 2013 explicitly asks for the ability to transfer data (statistical information, voice media streams) onwards to a PU.

Speech recognition software from Nuance, a NASDAQ listed US-based company, is used for the programme, enabling speech and speaker identification. The system allows for automatic response to speech over the phone, for example in a customer support centre. A tender for expanding the BroadWorks SIP platform in 2012 required the bidder to be certified to work on a SORM subsystem.

Uzbekistan

Similar to Kazakhstan, telecommunications equipment is required to comply with SORM. Numerous tenders for hardware, including switching equipment, ask that bidders comply with the SORM system. Contracts for SORM components in Uzbekistan are similarly subcontracted to small local companies. All telecoms operating in the country are obligated to subcontract such work to a local company, even if better rates can be obtained from foreign distributors.

SORM-related development work in Uzbekistan is overseen by a state-owned research centre. State Unitary Enterprise Scientific Engineering and Marketing Research Center (UNICON) is a state-sponsored research and development centre created in 1992 by decree of the Uzbek Ministry of Communication. The facility, located at the Uzbek National Communication and Technology University, has a SORM equipment certification, testing, and development centre. The centre also handles certification for telecom companies, ICT standardization, standard protocols development and information security facilities, plus marketing research and consultancy activities.

Between 2007 and 2010, according to UNICON's annual reports, the facility collaborated on all SORM projects in the country, which included consultancy work for SORM contracts with NSN, Huawei Tech, and Iskratel, as well as participating in the purchase and testing of SORM. In 2009 the certification of SORM-related equipment jumped 340 per cent in comparison to the previous year (2008). Unicon has signed SORM-related contracts with Nokia Siemens Networks, Iskratel (Slovenian-based equipment manufacturer), ZTE (China), Ericsson (Sweden) and Huawei Tech (China), while SORM integration testing and acceptance was carried out for the CSPs, Uzbektelecom and Coscom, which were then majority-owned by TeliaSonera.[123] Ericsson confirmed to Privacy International in writing that it had signed certification and approval contracts with UNICON during 2010-2012.

Chinese-French equipment manufacturer Alcatel Shanghai Bell has been a large provider of network equipment to Uzbekistan since 2005. In June 2005, Uzbektelecom and Alcatel Bell signed contracts for the supply of Alcatel S-12 switches, which were to be used for the modernisation and expansion of Tashkent's telecommunication network, valued at some US$4 million, which included SORM functionality. Separately, by 2009, Uzbektelekom had completed the expansion and reconstruction of an Alcatel S-12 switching system and implementation of the SORM function in the Karshy district of Uzbekistan, replacing analogue switching equipment with a modern digital device produced by Iskratel, another manufacturer of telecommunications equipment. Alcatel confirmed to Privacy International in writing that Alcatel Shanghai Bell had delivered SORM-compatible S12 equipment through Uzimpexaloka, an import-export body created in 1993 by the Uzbek Ministry of Communications.

123 "Годовой отчет", UNICON.UZ, available at http://unicon.uz/www/reports/unicon%20otchet.pdf

Surveillance equipment for law enforcement

There is now a substantial and growing market for electronic communications surveillance products designed and marketed for use by law enforcement and intelligence agencies. Such equipment can be integrated into the monitoring centres of specific agencies and used directly by law enforcement and intelligence agencies. The companies manufacturing these types of technologies regularly exhibit their products at surveillance and security trade shows. One of the largest trade shows, focused on North American and European providers, is Intelligence Support Systems World (ISS World). ISS World is a travelling trade show for surveillance companies that specialises in providing intelligence solutions for law enforcement and intelligence agencies, and training to vetted government and industry participants. In 2012, the KNB and a subsection – Kazakh Security Service – both attended ISS World,[124] as did the Turkmenistan National Security (the successor agency to the KGB in Turkmenistan) and the Government of Tajikistan.[125]

Offensive Malware

Offensive malware allows users to target and then effectively hijack a mobile phone or computer, thereby accessing all data on the device. Malware can even enable the user to remotely turn on and control the microphone and camera on the device. It is a particularly intrusive form of electronic surveillance given the personal information that can be obtained from such intimate access. Generally, available products on the market work by identifying and then targeting a specific user and then surreptitiously installing malware onto a device using forms of social engineering. They differ in their method of delivering the payload, with some methods requiring a user to download an executable programme while others rely on more covert methods. Such systems are typically marketed for their ability to avoid detection and to control various applications and functionalities on a device.

In late 2013, contractual documents were disseminated online showing that a UK-based surveillance company, Gamma, and a Swiss company, Dreamlab, had entered into a contract with the Turkmen government to install Gamma's mobile phone and computer targeting surveillance technology, FinFisher. FinFisher, which is only sold to government and law enforcement agencies, allows users to remotely install a trojan onto a computer or mobile device which subsequently allows for extraction of data and control of applications such as the webcam and microphone, while also allowing

124 "Surveillance Who's Who", Privacy International, available at https://www.privacyinternational.org/resources/surveillance-whos-who

125 "Program Schedule for Year 2013", TeleStrategies ISS World, 2013, hosted by Wikileaks at https://www.wikileaks.org/spyfiles/docs/ISS-2013-Sche2013-en.pdf

for access to applications such as Skype. Gamma also provides training, maintenance, and necessary upgrades to the products for customers. Dreamlab confirmed its relationship with Gamma, and expressed regret for entering into the contract, while refusing to confirm or deny whether the export to Turkmenistan took place. In 2013, The Citizen Lab, an interdisciplinary research institute in Canada, found evidence of a command and control server in Turkmenistan believed to be for tasking and receiving data from the FinFisher trojan. As of March 2013, 19 countries were identified as countries in which FinFisher servers were operating.[126]

The FinFisher trojan was also marketed to the Ministry of the Interior of Tajikistan in 2009 by the German-based surveillance company Trovicor. Documents show that in addition to providing a proposal to sell the government a monitoring centre, Trovicor provided price lists of the FinFisher system to the ministry.

In February 2014, The Citizen Lab also published forensic evidence indicating a trojan manufactured by the Italian company Hacking Team is currently or has previously been in use in Uzbekistan.[127] Similar to FinFisher, Hacking Team's Remote Control System can be used to hijack computer and mobile devices, whilst remaining undetectable to users, as it is designed to bypass common antivirus programmes and encryption. The analysis indicates that some 21 governments are suspected former or current users of the Remote Control System. Hacking Team received over €1.5 million in public financing from two venture capital funds originating from the Region of Lombardy in 2007. One of the funds, Finlombarda Gestioni SGR S.p.A (FGSGR) has only a single shareholder – Finlombarda S.pA, a public financial services agency whose only shareholder is the Region of Lombardy. FGSGR also lists its Head of Venture Capital as being a Board Member of Hacking Team.

126 The Citizen Lab, You Only Click Twice: FinFisher's Global Proliferation, 2013, https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

127 The Citizen Lab, Mapping Hacking Team's "Untraceable" Spyware, 2014, https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

Central Asia Legal Analysis

International Legal Frameworks

Kazakhstan, Uzbekistan, and Turkmenistan have each ratified the International Covenant on Civil and Political Rights ('the ICCPR'). This multilateral human rights treaty requires them to "respect and to ensure to all individuals within [their] territory" a range of human rights, including those most directly implicated by communications surveillance. Namely, the right to privacy (Article 17 ICCPR), and those rights that rely upon the protection of privacy for their realisation, such as, for instance, freedom of expression (Article 19 ICCPR), and freedom of association (Article 22 ICCPR).

It is well recognised under international law that respect for the right to privacy requires that states adopt domestic legislation that articulates clearly and in detail the circumstances under which surveillance can be conducted as well as the applicable safeguards. The UN Human Rights Committee (HRC), the expert body charged with interpretation of the ICCPR, has stipulated that surveillance must be carried out pursuant to legislation which "specifies in detail the precise circumstances in which such interferences may be permitted."[128] It has also held that any such authorised interference with rights must occur "only by the authority designated under the law, and on a case-by-case basis," and that broad-based surveillance, communications interception, wire-tapping etc, should be prohibited.[129] As has been recognised by the UN High Commissioner for Human Rights in 2014, the very existence of mass surveillance programmes interferes with the right to privacy.[130] Further, the UN Special Rapporteur on Freedom of Expression and Opinion has emphasised that all "communications surveillance should be regarded as a highly intrusive act" and that "legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority."[131]

As States parties to the ICCPR, therefore, Kazakhstan, Uzbekistan, and Turkmenistan are obliged, as a matter of international law, to refrain from broad surveillance programmes and to set out clearly in domestic legislation the conditions upon which limited interferences with citizens' privacy may be carried out, in exceptional cases.[132] Further, as member states of the Organization for Security and Co-Operation in

128 UN Human Rights Committee, General Comment 16, UN Doc. HRI/GEN/1/Rev.9(Vol 1), [8]

129 UN Human Rights Committee, General Comment 16, UN Doc. HRI/GEN/1/Rev.9(Vol 1), [8]

130 UN High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc. A/HRC/27/47, [20]

131 UN Special Rapporteur on Freedom of Expression, Report (17 April 2013), UN Doc. A/HRC/23/40, [81]

132 For further detail on the requirements of international human rights law with respect to State communications surveillance see the International Principles on the Application of Human Rights to Communications Surveillance, a soft law instrument supported by over 400 civil society organisations worldwide: https://necessaryandproportionate.org/.

Europe, Kazakhstan, Uzbekistan, and Turkmenistan have each committed themselves to respect international human rights and to give effect to the rule of law.[133]

Domestic Legal Frameworks

In purported fulfilment of their international legal obligations, Kazakhstan, Uzbekistan, and Turkmenistan each reflect the right to privacy in their national constitutions.[134] In each constitution, as is required at international law, the states provide that interferences with the right may only be in accordance with lawful authority and in limited circumstances. These constitutional protections are reinforced by domestic criminal laws prohibiting unauthorized surveillance and intrusion into certain private communications. Article 16 of the Kazakhstan Code of Criminal Procedure, for instance, which comes into force on 1 January 2015, provides for the privacy of "correspondence, telephone conversations, postal telegraph and other communications," and establishes that "[n]o one has the right to collect, keep, use or disseminate information regarding the private life of an individual without his consent, save in cases contemplated by law."[135]

Each State has legislation sanctioning interferences with the right to privacy in certain circumstances subject to lawful authorization. Kazakhstan, Uzbekistan, and Turkmenistan each provide, in their criminal codes, for covert surveillance and interception of the private communications of persons under criminal investigation.[136] Formally, authorization for such surveillance and interception typically requires the issuing of a warrant by a Procurator or a Court, although in certain circumstances the requirement of a warrant can be temporarily suspended. In Uzbekistan, for example, wire-taps can occur for limited periods without any warrant if the surveillance, in the opinion of the investigator "[does] not permi[t] delay."[137] In all three countries, warrants for targeted surveillance can only legally be issued as part of a formal investigation by a State investigator or examiner (an agent in a special type of accelerated criminal investigation common to post-Soviet states and inherited from Soviet practice). Our research suggests there is no provision in the laws of

133 See, for example, the commitments made in the OSCE Charter for European Security, Istanbul Document, 1999.

134 Constitution of the Republic of Kazakhstan, (30 August 1995), Article 18; Constitution of the Republic of Uzbekistan (8 December 1992), Article 27; and Constitution of Turkmenistan (18 May 1992) No 691-XII, Article 25

135 Code of Criminal Procedure of the Republic of Kazakhstan No 231-V (in force from 1 January 2015), Article 16(3)

136 See, for instance, Kazakhstan Code of Criminal Procedure, Articles 234, and 243-248; Uzbekistan Code of Criminal Procedure, Article 166-170; and Turkmenistan Code of Criminal Procedure, Article 282-284.

137 Uzbekistan Code of Criminal Procedure, Article 170.

of investigations of specific criminal activity. Further, in each jurisdiction, the State security services, while holding certain particular investigatory and detention powers, are required to comply with the same criminal procedure regime as the police and other law enforcement agencies.[138] Accordingly, while the investigators and agents of the State security services in Kazakhstan, Uzbekistan, and Turkmenistan are entitled to make requests for covert surveillance warrants, they require approval from a Procurator or Court prior to the carrying out of such surveillance.

Inadequacies in Legislation

While the legal frameworks governing surveillance by government bodies in Kazakhstan, Uzbekistan, and Turkmenistan appear, on their face, to reflect those States' international human rights law obligations, there are significant gaps in the legislative regulation of surveillance both within and outside of the formal sphere of criminal investigations. With respect to the former, the provisions described above do not circumscribe surveillance powers to a level necessary to protect against their being used arbitrarily. For example, there appears to be no reference in the relevant legislation to ex post oversight or scrutiny of warrant processes. There is no restriction on the duration of warrants or whether they can be renewed regularly or even indefinitely. There do not appear to be any provisions regulating the use or destruction of intercepted material or personal data after the surveillance has ceased. No provision is made in the legislation for dealing with confidential or privileged material. Further, there are no regulations governing or restricting the retention and storage of and access to intercepted material.

Outside of the surveillance powers pertaining to criminal investigation processes, there does not appear to be any legislation in Kazakhstan, Uzbekistan, or Turkmenistan permitting or regulating bulk collection of data pertaining to internet or digital communications, internet filtering or monitoring, or collection or interception of or access to communications data, which we know to be an increasingly common activity of security services worldwide. Likewise, there does not appear to be any legislation in Kazakhstan, Uzbekistan, or Turkmenistan permitting or regulating the use of Trojans or hacking techniques. Therefore, any surveillance being carried out by State security or law enforcement authorities outside the context of a targeted criminal investigation, will be entirely unfettered and unregulated, contrary to the provisions of these State's domestic constitutions and their obligations under international human rights law. Having regard to the legislative and other materials available to Privacy International, there does not seem to be any overarching oversight regime which would scrutinise the activities of the security services and law enforcement agencies, either within the context of the surveillance powers stipulated by legislation or outside of it.

138 Law of the Republic of Kazakhstan No 527-IV-Z on State Security (6 January 2012); Resolution of the Cabinet of Ministers under the President of the Republic of Uzbekistan No 276 on the National Security Service (2 November 1991); and Law of Turkmensitan No 283-IV on the Organs of National Security (31 March 2012)

This would suggest that security services in Kazakhstan, Uzbekistan, and Turkmenistan may be acting unconstrained by law or independent accountability mechanisms, which is plainly a matter of grave concern.

Further, there does not appear to be any publicly-available legislation regulating the conditions under which private companies operating in Kazakhstan, Uzbekistan, or Turkmenistan are or may be asked to monitor and intercept telephone, internet, and other communications or data, or to provide interception capability to government bodies. As documented in the Annex, before finalising this report, we wrote to a number of companies that we had identified as providing communication services in Central Asia. In none of the responses received from companies was there any detailed reference to the domestic legal framework that they were operating in nor how their operations complied with that domestic legislative framework, let alone with international human rights law more generally.

Vimpelcom provided one of the more detailed responses to Privacy International. They state that in relation to Kazakhstan, legislation imposes “certain obligations on... telecommunications providers through different legislative acts...” and that there is a “different regulatory approach depending on the type of data.” VimpelCom refers to “Kazakhstan legislation” requiring “CPSs to install certain data collecting/processing equipment on telecommunications networks and facilitate direct access for the national security agency to such equipment and data.” In so far as there is any legal framework governing corporate cooperation with State agencies in Kazakhstan, Uzbekistan and Turkmenistan with respect to the provisions of access to communications infrastructure, it is likely in the form of licence conditions or administrative orders made directly to companies, and notified only to those companies. If that is the legal arrangement for, for instance, CSPs like Vimpelcom installing certain data collecting/processing equipment on Kazakh telecommunications networks and facilitating direct access for Kazakh national security agencies, then that is clearly cause for concern, as it means that there is no possibility for public scrutiny of the relevant legal framework, nor is there the means to assess the state or companies’ compliance with the law.


"GARAŞSYZLYK TÜRKMEN

Conclusion

Global communications platforms and networks are critical to accelerating economic development, facilitating the enjoyment of human rights, particularly freedom of expression and communication, and the promotion of democratic ideals. In authoritarian systems of governance such as those in Central Asia, communications technologies and networks are essential to the effective work of journalists, human and labour rights activists, and political actors. Yet, as the surveillance capabilities of Central Asian governments expand, all of these actors are put at risk, as technologies that should advance social and economic progress are turned into tools of repression. The imperative for ensuring that actors for change in undemocratic societies are able to communicate privately and securely is clear, and demands urgent attention.

The role of the private sector in enabling unlawful and unrestrained communications surveillance in Central Asia cannot be underestimated. Interception and surveillance technologies, designed for use within strict legal frameworks and systems of oversight, have been exported to the region by companies in circumstances in which there has been a clear risk they would be abused by relevant governments in order to consolidate political control. CSPs and telecommunications equipment manufacturers have facilitated direct government access to their networks and to their subscribers' data, in exchange for permission to operate in the countries, despite the serious human rights concerns raised by bulk interception and surveillance practices and the complete absence of checks and balances.

The key policy challenge is how to enable communications services and networks to continue to operate effectively in Central Asia, while ensuring that those governments' desire to control and hijack services and networks for political control is checked. Confronting this challenge requires communications services providers and telecommunications equipment manufacturers to engage substantively in UN and industry-led business and human rights initiatives, including, for example, Corporate Social Responsibility and transparency measures, in conjunction with a broad range of other regulatory and soft law initiatives.

It also requires a strong regulatory approach towards the electronic surveillance industry. In Uzbekistan and Kazakhstan, two surveillance companies have enabled the principal intelligence agencies – widely implicated in human rights abuses – to have direct, unchecked access to the population's phone and internet activity through the establishment of monitoring centres. Sophisticated targeted surveillance technologies appear to have been exported to at least Uzbekistan and Turkmenistan. The role of these companies in facilitating unlawful or arbitrary surveillance is clear. The electronic surveillance industry develops products that are intrinsically open to abuse because of their mass application or invasive nature, and have supplied them in the knowledge that legal provisions are inadequate to effectively prevent their use in a manner than undermines human rights. Further, due to the very nature of the industry, surveillance technology companies tend to operate in the shadows, with few transparency initiatives or human rights commitments. Controls on the export of such technologies from the countries in which they are manufactured to repressive regimes like those in Central Asia must be prioritised. These types of technologies, specifically designed for surveillance and marketed for law enforcement purposes and end-users, will only continue to grow in number and sophistication. As perceived and real threats continue to be met by governments with increased censorship and surveillance, the industry will continue to offer states cheaper and more sophisticated and efficient options. Ensuring that these technologies no longer undermine human rights in Central Asia will require significant political will, and industry-led reform.

Annex

Kenneth Page
Privacy International
62 Britton Street
London, EC1M 5UY
United Kingdom

12 November 2014

Dear Kenneth Page,

Thank you for your letter dated 5 November 2014 regarding a request for information and clarification relating to past Alcatel telecommunications equipment deployment in Central Asia dating to 2005.

Attached to this letter you will find some clarification on the equipment deployment within the time constraints outlined in your letter.

I would like to highlight that in line with UN Ruggie Principles published in 2011, Alcatel-Lucent has taken a number of steps to address our international commitments relating to Human Rights Freedom of Expession and Privacy, including our involvement in the Telecommunications Industry Dialogue on Human Rights and implementation of Guiding Principles. We attach great importance to our corporate responsibility on a global scale relating to Human Rights.

More information on our commitment and activities is available on www.alcatel-lucent.com/sustainability and http://www.alcatel-lucent.com/sustainability/human-rights .

I remain available to meet with you to discuss any further questions you may have and look forward to a constructive dialogue.

Yours sincerely,

Christine Diamente
Head of Brand and Corporate Sustainability
christine.diamente@alcatel-lucent.com
mob+44 7590 447 002

Further Information on Privacy International Letter dated 5 November 2014:

In both Uzbekistan and Kazakhstan, by law, all networks connected to civil telecom networks must be compliant with the requirements of SORM. Therefore, any and all Alcatel-Lucent equipment supplied for connection to the telecom networks are, as they must be, compatible with local SORM requirements. However, in order to provide the national security services' respective access, the operators need to install additional SORM equipment. This equipment is typically subject to very stringent export control rules and regulations, which Alcatel-Lucent respects and is in compliance with.

Regarding the specific deployments by Alcatel Shanghai Bell (ASB) referred to in your letter we can confirm that:

- ASB contracted the referenced deal in the letter with Uzimpexaloka for end-customer Uztelecom, which included SORM compatible S12 delivery.

- ASB supplied S12 and SORM compatible S12 equipment in 2009 to Kazakhstan.

Given that these are dated contracts we have not been able to confirm in the very limited amount of time that you have given us, that ASB provided the additional SORM equipment that would have been necessary to conduct surveillance.

This information is based on the research we could find within your stated deadline of 12 November noon GMT.

Dear Kenneth and Edin,
On behalf of Elaine Weidman, please find Ericsson's reply to your request below.

Lawful intercept capabilities are an integral part of telecom standards and are intended for emergencies and fighting crime. Such capabilities are a requirement from most operators in the world, due to the legal requirements put upon them. Regarding the questions about Uzbekistan and Kazakhstan please see responses below.

Uzbekistan
UNICON is the Certification Body in Uzbekistan, they provide certification and type approval services but not any solutions or equipment. Certification of the network is a mandatory requirement in this market.

We have ordered certification/type approval services from them during the period of the time 2010-2012.

Kazakhstan
Since Ericsson's Lawful Interception Management System does not handle the SORM interface, we work together with a third party, Ronex, to meet that legal requirement in Kazakhstan.

Kindly note that Ericsson welcomes the multi-stakeholder dialogue around human rights challenges associated with unintended use of telecommunications systems and more specifically lawful interception functionality. Toward that end, we are in the process of completing a discussion paper on this topic together with the Institute of Human Rights and Business, where many of the dilemmas that Ericsson have faced are discussed in detail. The paper will be published in the coming days. We are also actively participating in the Wilton Park event next week, where we have noted that Privacy International will also be attending, and we could engage with you directly on this topic at that time, should you wish to discuss further.

Don't hesitate to contact me if you require any further information.
Kindly confirm receipt of this email.
Best, Heather

ERICSSON

HEATHER JOHNSON
Director, Communications and Stakeholder Engagement
Sustainability and Corporate Responsibility

As Privacy International already knows, Hacking Team does not disclose the names or locations of clients because our software is used in confidential law enforcement investigations. So any disclosure is up to the clients themselves should they choose to do so. Therefore, I cannot confirm or deny that Uzbekistan is or has been a client of Hacking Team. However, Citizen Lab in its own report, concedes that its effort to identify Hacking Team Clients is not conclusive but rather Citizen Lab repeatedly notes that the 21 governments it identifies are "suspected" government users of our system, RCS.

Eric

Eric Rabe

Hi Edin,

Below please find our response to your query.

Best wishes,

Erik

NICE Cyber and Intelligence Solutions help Law Enforcement Agencies (LEAs), intelligence organizations and SIGINT agencies to reduce crime, prevent terrorism and identify other security threats by providing solutions for lawful communication interception, collection, processing and analysis. NICE does not operate these systems, and has no access to the information gathered. Rather, that task is performed by the agencies themselves. NICE is not in a position to provide additional comment on its relationships with actual or possible customers.

ERIK SNIDER
Director of Corporate Communications

Jo Lunder
Chief Executive Officer

VimpelCom

VimpelCom Ltd.
Claude Debussylaan 88
1082 MD Amsterdam
The Netherlands

T +31 (0)20 797 72 00
F +31 (0)20 797 72 01
W www.vimpelcom.com

Trade reg. 34374835
VAT 821815568B01

To whom it may concern

Thank you for your letter dated 5 November 2014.

We understand that Privacy International is preparing a report on electronic surveillance in several Central Asian countries and the potential impact on human rights. In this regard, you have set out a number of points which you indicate are, "to your knowledge, true and correct."

We are pleased to be able to respond to your letter. However, our response is limited entirely to our experiences and should not be construed as confirmation of any of the statements you have made. In the short time allowed to respond to your letter we have liaised with our relevant business units to provide you with responses to your request. We have not, however, carried out a detailed analysis of your positions and this letter should not be construed as confirmation of any assertions in your letter.

Background

VimpelCom has businesses operating in four of the five countries mentioned in your letter: Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan. In these markets, and across other operations managed by VimpelCom, our primary aim is to provide high quality, reliable telecommunication services to our customers. This includes establishing controls over the security of customer data and VimpelCom complies with, and uses best efforts to exceed, the respective legal requirements established to regulate customer privacy in these jurisdictions.

The annex responds to your points regarding the surveillance position in the countries listed in your letter. Below, we respond to your more general points about policy options open to CSPs in relation to surveillance.

Requirements on CSPs

As a licensed CSP, we are of course obliged to act in accordance with our license, and broader regulation. If a legal request is made, or action is taken, by a government to access data, we have no legal basis or practical options, to prevent access. We place great importance on the privacy rights of our customers and in all cases, where a request is made, we carefully consider the request and where appropriate, seek clarification or confirmation from the governmental authorities to understand the request and to confirm the legal basis of the request. We would also note that, in many countries, including many western countries, it is actually illegal to provide information on the level and nature of government access to data.

Government access to certain telecommunications data is beneficial in certain important areas: it is important in tackling organized crime and terrorism, finding missing persons and in child protection. Governments in all parts of the world establish the legal framework through which they access this data and this is set out in both license (to operate) agreements established to regulate telecommunication operators, and other laws governing the topic. This legal framework can take several different forms, ranging from the presentation of a court order to the CSP which then facilitates access to the data covered by the court order, to situations where the legal framework permits certain government agencies to access networks and data through relevant technologies on the basis of legal approvals in which the CSP has no involvement and where it has no ability, legally or technically, to obstruct or challenge. Human rights concerns have arisen where governments are perceived to be 'abusing' this power for political, rather than public safety purposes.

We fully accept that the current situation is challenging and far from ideal and we are proponents of having clear and understandable legal frameworks that are not subject to abuse. We do feel that it is important for CSPs, including VimpelCom, to remain active and engaged in the markets you discuss in your letter. We provide important benefits and choice for the citizens of these countries and play a significant role in broader economic and social development. We believe that the line between the type of practices that you raise in your letter, and those operated in western countries is not black and white, as recent revelations have indicated, blurring any assessment of which countries are 'acceptable' to operate in and which are not.

We are very open to dialogue which targets realistic, practical steps to ensure that government access to, and use of, customer data is properly targeted, and not unnecessarily extensive.

Yours sincerely

Jo Lunder
Chief Executive Officer

Country Specific Comments

In relation to the specific points you raise in your letter, our response is as follows:

- Kazakhstan legislation imposes certain obligations on the telecommunication providers, through different legislative acts, which provide for a different regulatory approach depending on the type of data, the authorities requesting the information and the particular circumstances in which information is needed. Depending on those different factors our Business Unit may or may not have oversight and control the provision of information to the enforcing agencies in Kazakhstan. In particular, where authorities request information from our Business Unit, it applies precautionary measures and legality checks before disclosing personal and other types of protected data within the limits permitted by the law. However, in addition to the above, Kazakhstan legislation requires CSPs to install certain data collecting/processing equipment on telecommunication networks and facilitate direct access for the national security agency to such equipment and data, which leaves no room for the Business Unit to control or challenge such activities;

- In Kyrgyzstan, where subscriber data is requested directly from CSP, it is provided to law enforcement bodies only upon presentation of a court ruling that authorizes the respective law enforcement body to gather the requested information. Such ruling contains the description of the case and the range of the information that is being requested. No subscriber data is provided without such a court ruling;

- In addition, legislation of the Kyrgyz Republic provides that the authorized bodies obtaining information on subscriber connections from technical communication channels, computer systems and other hardware, as well as carrying out search operations on networks and telecommunication channels, is realized in the following order:

    - the authorized state body that carries out the investigative activity should receive and provide to the user (State Committee on National Security - GKNB) of SORM the judicial ruling with the application;

    - the request should contain a specific phone number and (or) IP address and the requested period of time for which the information should be provided;

    - the GKNB registers the receipt of such request and the provision of such information in separate documents;

    - fulfilled requests with accompanying judicial acts are stored by the GKNB;

    The GKNB is controlled by the Prosecutor's office and provides upon requests or complaints the information on specific measures that have been undertaken with the usage of SORM equipment. The CSPs, in accordance with the legislation, do not have access to the SORM equipment and cannot control the activities of the GKNB as the method and order of realization of investigative activities are maintained as confidential by the government;

- In Tajikistan, according to the current Tajik legislation, information on subscribers connections, accessing information from communication channels, computer systems and other hardware, as well as the holding of other search operations on telecommunication channels by the authorized investigative bodies, is realized on the basis of a court ruling. Our understanding is that the authorized investigative body provides the court ruling to the SORM user to enable the above-mentioned actions;

- In Russia, access to subscriber data is carried out on two legal grounds – Court Order and Legal competence granted to the authorized state body. In non-judicial procedures such access is provided exclusively for the state authorities. The state agencies that carry out the investigative activity have the right to use the Law Enforcement Monitoring Facility (SORM). In fact SORM allows the Federal Security Service direct access to the CSPs' networks. Other agencies directly request CSPs to render the subscriber's data if it is authorized by Law or on the basis of a Court decision. Supervision of the legality of any access to data subscribers within the framework of the investigation activity, including via SORM, is monitored by the Office of the Public Prosecutor.

Privacy International Request for Information

Nokia statement

Dear Sir,

Thank you for your e-mail dated November 5th inviting us to comment on the upcoming report.

Nokia provides products and services that expand opportunities to communicate and which directly contribute to the exercise of such fundamental rights as free expression and political participation, to the benefit of individuals and their societies. Nokia is committed to the Universal Declaration of Human Rights and the human rights principles of the United Nations' Global Compact and has embedded them in our Code of Conduct and in our Human Rights Policy.

As per your specific information request; According to national law, all telecommunications equipment must undergo certification in Uzbekistan by the equipment vendor, prior to delivery to customer. This certification is done to verify the system functionality according to international standards like the ETSI and 3GPP. Nokia has chosen to use UNICON for obtaining these certifications.

As a founding member of the Telecommunications Industry Dialogue in 2013, we remain committed to engaging in constructive dialogue with governments and NGOs around the complex and challenging issues of Internet censorship, privacy, and surveillance.

Please do not hesitate to contact me if you would like to discuss these issues further.

Sincerely,

Laura Okkonen
Corporate Responsibility

NOKIA

More information:

Nokia Code of Conduct: http://networks.nokia.com/ko/about-us/sustainability/our-approach/code-of-conduct

Nokia Human Rights Policy: http://networks.nokia.com/about-us/sustainability/ethics-and-human-rights

11 ноября 2014 года

Privacy international

62 Britton Street

London, EC1M 5UY

Great Britain

Заинтересованному лицу

Уважаемые господа! Вопрос защиты прав человека на неприкосновенность частной жизни, безусловно, очень важен для всего человечества.

Однако зачастую этот вопрос входит в противоречие с деятельность в области борьбы с терроризмом и преступностью.

Первичными в разрешении противоречия являются законы и другие нормативно-правовые акты, определяющие степень применения легальных средств доступа и контроля передаваемой информации.

В мире существуют десятки компаний, разрабатывающих технологическое оборудование для мониторинга телекоммуникационных сетей, но естественно, что не технологии являются определяющими в этой сфере.

Что касается деятельности нашей компании, как в России, так и за рубежом, то она базируется на основе законодательства и других нормативно-правовых актов, принятых в каждом из государств.

С уважением,
д-р А. А. Иванов,
президент

А. Иванов

ООО «МФИ Софт», Россия, 119146, г. Москва
Комсомольский проспект, д. 19 А
Тел.: +7 495 6427075, факс: +7 495 7896617
www.mfisoft.ru, e-mail: info@mfisoft.ru

Creator
Patrik Hiselius

Privacy International

Dear Mr Page,

Thank you for your e-mail dated November 5th inviting us to comment on your draft text.

TeliaSonera's Group Code of Ethics and Conduct states:

"TeliaSonera acknowledges the concerns following legislative, administrative, license or law enforcement requirements to which we must adhere but which may impact individual's privacy and freedom of expression. Our aim is to enable citizens to exchange ideas and provide tools for the development of more open societies. Freedom of expression and privacy are the core of our business."

TeliaSonera's has a firm position on unrestricted real time access: Governments should not have such access to our networks and systems. TeliaSonera should retain operational and technical control.

As to the text drafted by Privacy International, companies do not have oversight over how the systems work and how surveillance data is obtained and used. Also, we are not able to comment freely on issues directly related to national security.

The UN 'Protect, Respect, and Remedy' Framework for Business and Human Rights requires States to protect human rights, and companies to respect human rights. TeliaSonera takes this responsibility very seriously.

In March 2013, TeliaSonera together with several peers launched the 'Telecommunications Industry Dialogue on Freedom of Expression and Privacy'.

Based on the UN Guiding Principles, a TeliaSonera human rights impact assessment and the shared learning within the Industry Dialogue, TeliaSonera in December 2013 launched a Group Policy, the 'TeliaSonera Group Policy on Freedom of Expression in Telecommunications'. The Policy defines TeliaSonera's point of challenge in respect to government's demands with potentially serious impacts on freedom of expression of our customers and users. TeliaSonera's CEO has stated that TeliaSonera will advocate and argue for clear and transparent legislation, engaging in dialogue regarding regulations that affect our business and our customers. The first four principles of this policy define the basis of TeliaSonera's public policy. Principle 3 reads: "We advocate that governments should not have direct access to a company's networks and systems. The company should retain operational and technical control."

When TeliaSonera meets with authorities and governments throughout our operations, we raise our point of view based on our policy. At our latest Sustainability up-date to our investors, we informed about our public advocacy work to this regard that far, see slide number 21 here;
http://www.teliasonera.com/en/newsroom/news/2014/teliasonera-sustainability-update-shows-progress/

TeliaSonera encourages governments to be transparent about their use and scope of surveillance of communications, and we report transparently on our efforts in relation to surveillance of communications.

Our transparency report published in August 2014 includes a section on major events throughout our operations.

As a leading provider of telecommunication services, TeliaSonera is a vital part of the social and economic infrastructure in the markets where we operate. TeliaSonera provides tools and services that can significantly promote freedom of expression, even in countries where such freedoms are so far limited.

For further information on TeliaSonera's work on freedom of expression and privacy, including our work within the Industry Dialogue, please visit; http://www.teliasonera.com/en/sustainability/human-rights/

Our local companies Kcell and Ucell have published the Freedom of Expression Policy on their respective homepages.

Sincerely,
Patrik Hiselius
Senior Advisor, Digital Rights
TeliaSonera

Posted in trovicor.com Newsroom on February12th, 2014 – Rel. T02/2014

trovicor releases its new Cyber Security solution

Munich, Germany, February 12th, 2014 – trovicor, the German-based worldwide provider of turnkey intelligence solutions, has announced the release of its new Cyber Security solution for fighting the ever-growing threats of cyber crime.

The constantly evolving world of cyber space offers endless new opportunities for cyber criminals. Online thefts and frauds, espionage, security breaches, trojans, phishing and other advanced threats are among the thousands of cyber attacks that occur daily, causing disruption and damage on a vast scale. Ensuring cyber security has become a major challenge for the state, business and society both at national and international level.

trovicor's cyber security solution provides the tools needed to identify and respond to cyber attacks. And these tools are kept up to date - a team of trovicor cyber security experts regularly reviews its cyber security strategy, approach and solutions.

Based on trovicor's flagship product, the Intelligence Platform, the trovicor cyber security solution ensures recognition of the newest malware. As a result, millions of users can have trust that their transactions and generated data are protected.

The trovicor solution is designed for high-speed networks and the monitoring of large volumes of data traffic which can be accumulated from many different sources. Pattern and behaviour recognition software work in real time and can detect new threats, as well as those with known signatures.

The machine-learning algorithms can identify and separate malware from general traffic, and immediately send an alert when malware is detected. Information is displayed in the form of charts and graphics on a network dashboard. This visual approach assists the analysts in seeing new patterns or identifying non-standard activities.

The trovicor cyber security product can be developed and tailored to customers' particular needs. A multi-disciplinary team of trovicor experts provides consulting advice and helps scope the infrastructure required to secure large, high-risk networks.

About trovicor

trovicor is a worldwide leader in end-to-end communications and intelligence solutions, security services and consultancy support.

Headquartered in Munich, Germany, the company supplies systems based on own state-of-the art core developments for criminal investigation and national security to governmental customers around the globe.

Public authorities turn to trovicor for solutions to prevent crime and enhance safety and security in accordance with local laws and standards.

Leveraging our sophisticated knowledge of network technologies and operations, databases, call and IP data flows and ever-changing communication protocols and applications, our customers rely on our experience in the most sophisticated, advanced communication networks and environments.

www.trovicor.com

Posted in trovicor.com Newsroom on August 28th, 2014 – Rel. t03/2014

trovicor launches Environmental Monitoring Solution for Data Centre Security

Munich, Germany, August 28th, 2014 – trovicor, for many years a world leader in the provision of security solutions, is pleased to announce its new Environmental Monitoring Solution (EMS) for the protection of Data Centre operations.

Your company's data centre is critical to the success of your business. A data centre houses readily-accessible data and applications; it must be secure and resilient in order to keep your enterprise running at maximum productivity. But how secure is your data centre? Any outage or security breach could seriously damage your company's operations, productivity and profitability - not to mention your business reputation.

trovicor can help to secure data centres with an end-to-end security solution that continuously monitors all system components and operational aspects – hardware, software and environment. Here is how the trovicor EMS helps monitor and safeguard your data centre components:

- **Server** - Monitoring the availability and resource consumption of the server platform is the key to detecting hardware-based failures, as well as monitoring hardware-based performance criteria such as CPU and memory load.

- **Networks and active network components** - Stable network connection in combination with sufficient bandwidth is a prerequisite for any system. Tracking the network traffic and bandwidth usage between components helps with fault tracking as well as anticipating future needs.

- **External environment** - The environmental conditions are vital to ensuring sustainable operation for any technical system. The trovicor EMS offers a wide range of sensors (e.g. temperature, humidity, smoke detection) to monitor the physical environment of the technical room.

- **Applications** - Server hardware and the environment are just one side of the coin; the other is the monitoring of the availability of system applications as well as Operating System related issues. The EMS offers various possibilities for supervising application-specific criteria.

- **Alarms and error handling** - In the event of unusual conditions, alarms are sent out via SMS or e-mail, user-defined actions can be triggered (e.g. the execution of scripts) and applications/services can be restarted automatically. The EMS can also integrate alarm states sent by 3rd party applications (based on SNMP traps) which have been incorporated into the system.

- **Distributed and evolving systems** - The EMS supports the monitoring of distributed systems by using multiple appliances located at the different locations. In the case of a growing IT infrastructure in a location, it is further possible to scale the solution by subsequently adding additional appliances. With this concept, the EMS can be flexibly adjusted to support additional locations as well as growing IT infrastructure within one location.

The trovicor Environmental Monitoring Solution offers a rich reporting functionality, including for example reports on performance, hardware availability and outages, as well as system configuration maps.

In the words of trovicor's CEO: "We fill the gaps in traditional security by directly protecting high-value applications and data assets in physical and virtual data centres."

About trovicor

trovicor is a worldwide leader in end-to-end communications and intelligence solutions, security services and consultancy support.

The company supplies systems based on own state-of-the art core developments for criminal investigation and national security to governmental customers around the globe.

Public authorities turn to trovicor for solutions to prevent crime and enhance safety and security in accordance with local laws and standards.

Leveraging our sophisticated knowledge of network technologies and operations, databases, call and IP data flows and ever-changing communication protocols and applications, our customers rely on our experience in the most sophisticated, advanced communication networks and environments.

www.trovicor.com

Dear Kenneth,

you had sent us the following question:

In 2009, Trovicor GmbH provided the Ministry of the Interior of Tajikistan a proposal for the supply of a monitoring centre "for all cellular networks", in addition to a Lawful Interception Management System (LIMS). LIMS is manufactured and sold by Utimaco GmbH, which lists Trovicor as a partner.[1]

Utimaco can not confirm whether your statement is accurate. Trovicor GmbH is a long-term reseller of Utimaco solutions and with regards to their proposals, you will need to get confirmation from them directly.

We can however confirm the following:

1. There are no historic or current or planned sales, deliveries or installations of any Utimaco product, including Utimaco LIMS, in Tajikistan, neither with the entity you list in your question above – nor any other entity in that country.

2. Utimaco has not participated in any sales activities in Tajikistan up to now and it is not a country Utimaco is or plans to be active in the future.

3. **Utimaco does not sell directly to end customers, ie. telecom operators (with the exception of its home market Germany), but sells the LIMS system to network element vendors, who include the product as OEMs in their worldwide network offerings. All sales, deployment, training and support is done through these OEM partners and their respective local teams.**

4. **The LIMS product is subject to export control under the German and EU export regulations under categories 4 and 5 of the Wassenaar agreement. Within these export regulations general as well as individual embargo lists of the United Nations apply. The responsible export authority is the German "Bundesamt für Aussenwirtschaft (BAFA)". All OEM partners are mandated by law as well as by Utimaco to adhere to the German and EU export regulations and Utimaco holds the right to audit that this process is applied correctly.**

Should you have any further questions, don´t hesitate to contact us.

Best regards,

Malte Pollmann
CEO
Utimaco GmbH

АКЦИОНЕРНОЕ ОБЩЕСТВО «КАЗАХТЕЛЕКОМ»

«УТВЕРЖДАЮ»
Генеральный директор
Дирекции «Телеком Комплект»

_______________Е.М. Горбатовский

Приказ № 322– П «09» октября 2013г.

ТЕНДЕРНАЯ ДОКУМЕНТАЦИЯ
по электронному тендеру по закупке оборудования Пульта управления СОРМ с услугами монтажа и пуско-наладки "под ключ"
(далее – Тендерная документация)

г. Алматы 2013г.

ТЕНДЕРНАЯ ДОКУМЕНТАЦИЯ
по электронному тендеру по закупке оборудования Пульта управления СОРМ с услугами монтажа и пуско-наладки "под ключ"
(далее – Тендерная документация)

Закупки - Оборудование Пульта управления СОРМ с услугами монтажа и пуско-наладки

монтажа и пуско-наладки "под ключ"

(далее – Тендерная документация)

Закупки - Оборудование Пульта управления СОРМ с услугами монтажа и пуско-наладки "под ключ"

1. **Заказчик – АО «Казахтелеком».**
2. **Организатор закупок - Дирекция «Телеком Комплект» – филиал АО «Казахтелеком».**

Почтовый адрес Дирекции «Телеком Комплект» - филиала АО «Қазақтелеком»:
050031, г. Алматы, ул. Толе Би 291 Б.
Банковские реквизиты Дирекции «Телеком Комплект» - филиала АО «Қазақтелеком» (для резидентов):
Реквизиты в тенге: БИН 941240000193, ИИК KZ 079261802104233016, Кбе 16, в филиале АО «Казкоммерцбанк», БИК KZKOKZKX ***(указывать обязательно, что для Дирекции «Телеком Комплект»)***
В АФ АО "Казкоммерцбанк" г.Алматы, пр.Достык,107 РКО 18/29 БИК: KZKOKZKX
РНН банка 600400561686
Алматы, Республика Казахстан
БИН 941240000193
Банковские реквизиты АО «Қазақтелеком» (для нерезидентов):
Реквизиты в российских рублях:
Бенефициар:
АО "КАЗАХТЕЛЕКОМ" РНН 600700017446
Р/с: KZ559261802104233025 КБЕ-16
Банк бенефициара:
АФ АО "Казкоммерцбанк" БИК: KZKOKZKX
г. Алматы, Республика Казахстан, SWIFT: KZKOKZKX
К/с: 30111810400000000059
Банк-корресп.банка Бенеф:
Сберегательный банк РФ, Москва, Россия (СБЕРБАНК РОССИИ)
ИНН 7707083893
К/с: 30101810400000000225 в РКЦ ГУЦБ РФ
БИК: 044525225
SWIFT: SABRRUMM012
Реквизиты в долларах США:
JSC "Kazakhtelecom"
Astana, Kazakhstan
ACC.# KZ249261802104233001
JSC "Kazkommertsbank"
Almaty, Kazakhstan
SWIFT: KZKOKZKX
CORR/ACC.# 890-0223-057
'BANK OF NEW YORK'
NY, USA
SWIFT: IRVTUS3NCHIPS: 0001
Реквизиты в EUR:
JSC "Kazakhtelecom"
Astana, Kazakhstan
ACC. # KZ679261802104233003
JSC "Kazkommertsbank"
Almaty, Kazakhstan
SWIFT: KZKOKZKX
CORR/ACC.# 400/8866048/01EUR
Commerzbank AG
GERMANY, FRANKFURT
SWIFT: COBADEFF
Электронный адрес интернет-ресурса, на котором размещена информация о проводимых закупках: http://www.telecom.kz, www.samruk-kazyna.kz.
Адрес электронной почты и номер телефона для обращения потенциальных поставщиков в случае нарушения их прав в связи с проводимыми закупками: zakupDTK@telecom.kz, +7 (727) 226 82 61.

3. **Фонд** – АО «Самрук-Казына»;
4. **Холдинг –** совокупность Фонда и юридических лиц, пятьдесят и более процентов голосующих акций (долей участия) которых прямо или косвенно принадлежат Фонду на праве собственности или доверительного управления. Косвенная принадлежность – принадлежность каждому последующему юридическому лицу пятидесяти и более

4. **Холдинг** – совокупность Фонда и юридических лиц, пятьдесят и более процентов голосующих акций (долей участия) которых прямо или косвенно принадлежат Фонду на праве собственности или доверительного управления. Косвенная принадлежность – принадлежность каждому последующему юридическому лицу пятидесяти и более процентов голосующих акций (долей участия) иного юридического лица на праве собственности или доверительного управления;
5. **Правила** – Правила закупок товаров, и услуг акционерным обществом «Фонд национального благосостояния «Самрук-Қазына» и организациями, пятьдесят и более процентов голосующих акций (долей участия) которых прямо или косвенно принадлежат АО «Самрук-Қазына» на праве собственности или доверительного управления, утвержденных решением Совета директоров Фонда (протокол № 93 от 07 июня 2013 года).
6. **Инструкция** – Инструкция по организации и осуществлению электронных закупок товаров, работ, услуг акционерного общества «Самрук-Қазына» и организациями пятьдесят и более процентов голосующих акций (долей участия) которых прямо или косвенно принадлежат АО «Самрук-Қазына» на праве собственности или доверительного управления, утвержденная решением Правления АО «Самрук-Қазына» от 5 июля 2012 года № 29/12.

7. **Участник –** Заказчик, потенциальный поставщик, прошедший регистрацию в Системе.
8. **Система –** информационная система электронных закупок Фонда (www.tender.sk.kz);
9. **электронный документ –** документ, в котором информация предоставлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи;
10. **электронная копия -** электронный эквивалент документа, полученный путем преобразования в цифровую (электронную) форму, полностью воспроизводящий содержание исходного документа;
11. **ЭЦП –** электронно-цифровая подпись, набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания.
12. **Сумма, выделенная для закупки без учета НДС:** 200 000 000,00 (двести миллионов) тенге 00 тиын.

Лот	Название Лота	Сумма, тенге без учёта НДС
1	Оборудование Пульта управления СОРМ с услугами монтажа и пуско-наладки "под ключ"	200 000 000,00

13. **Базовые условия платежа:**

-15% предоплата от общей стоимости оборудования и услуг оплачивается в течение 20 (двадцать) рабочих дней с момента подписания договора и внесения обеспечения возврата аванса (предоплаты);

-85% от стоимости оборудования оплачивается в течение 20 (двадцать) рабочих дней с момента подписания Акта приема-передачи оборудования;

-85% от стоимости услуг оплачивается в течение 20 (двадцать) рабочих дней после оказания услуг. Датой оказания услуг считается дата подписания Акта приемки оказанных услуг.

14. **Размер обеспечения заявки на участие в тендере** составляет 1 % (один процент) от суммы, указанной для закупки данного товара и услуг, в настоящей тендерной документации. При этом течение срока действия обеспечения заявки на участие в тендере начинается со дня вскрытия конвертов с заявками на участие в тендере.

При осуществлении электронных закупок обеспечение заявки на участие в тендере может представляться в виде электронной банковской гарантии в соответствии с Инструкцией по проведению электронных закупок.

Оригинал обеспечения заявки на участие в электронном тендере в виде банковской гарантии предоставляется по адресу: г. Алматы, ул. Толе Би 291 Б, Дирекция «Телеком-Комплект» - филиал АО «Казахтелеком», 4 этаж тендерный отдел.

Обеспечение заявки на участие в тендере не вносится:

1) организациями инвалидов (физическими лицами - инвалидами, осуществляющими предпринимательскую деятельность), состоящими в Реестре организаций инвалидов (физических лиц - инвалидов, осуществляющих предпринимательскую деятельность) Холдинга;

2) отечественными товаропроизводителями закупаемого товара;

3) организациями, входящими в Холдинг;

4) участниками СЭЗ «Парк инновационных технологий» (при участии в тендере на поставку товаров, оказание услуг, относящихся к приоритетным видам деятельности, соответствующим

2) отечественными товаропроизводителями закупаемого товара;

3) организациями, входящими в Холдинг;

4) участниками СЭЗ «Парк инновационных технологий» (при участии в тендере на поставку товаров, оказание услуг, относящихся к приоритетным видам деятельности, соответствующим целям СЭЗ «Парк инновационных технологий» и предмету закупок).

Положения настоящего пункта не распространяются на консорциумы.

15. **Заявки на участие в тендере предоставляются потенциальными поставщиками путем регистрации в Системе.**

Срок начала представления заявок 13:30 часов «10» октября 2013 года.

Окончательный срок представления заявок 11:00 часов «28» октября 2013 года.

16. **Срок действия заявки на участие в тендере должен быть не менее 70 (семьдесят) календарных дней с даты вскрытия конвертов с тендерными заявками;**
17. **Размер обеспечения возврата аванса (предоплаты)** составляет 15 % (пятнадцать процентов) от общей суммы договора о закупках.

Требование о представлении Заказчику/Организатору закупок обеспечения возврата аванса (предоплаты), не распространяется на:

- организации, входящие в Холдинг;
- отечественных товаропроизводителей закупаемого товара;
- организации инвалидов (физические лица – инвалиды, осуществляющие предпринимательскую деятельность), производящие закупаемый товар, состоящие в Реестре организаций инвалидов (физических лиц - инвалидов, осуществляющих предпринимательскую деятельность) Холдинга.

1 . Требования к потенциальным поставщикам

18. Для участия в тендере потенциальный поставщик должен обладать правоспособностью (для юридических лиц) и дееспособностью (для физических лиц).

2. Оформление и представление заявки

19. Заявка потенциального поставщика на участие в тендере (далее – Заявка) является выражением согласия потенциального поставщика на поставку оборудования Пульта управления СОРМ с услугами монтажа и пуско-наладки "под ключ" в соответствии с требованиями и условиями, предусмотренными Тендерной документацией.
20. Заявка должна быть закреплена ЭЦП потенциального поставщика и должна содержать электронные копии и электронные документы в соответствии с требованиями пункта 33 Тендерной документации.
21. Заявки на участие в тендере, поданные потенциальными поставщиками, автоматически регистрируются в Системе.
22. В качестве подтверждения приема или отказа в приеме заявки на участие в электронных закупках способом тендера потенциальному поставщику, подавшему заявку на участие в электронных закупках способом тендера автоматически направляется Системой соответствующее уведомление.
23. Система помещает поступившие заявки в недоступное извне защищенное хранилище до наступления даты и времени вскрытия заявок, указанных в объявлении.
24. В Заявке не должно быть никаких вставок между строками, подтирок или приписок, за исключением тех случаев, когда потенциальному поставщику необходимо исправить грамматические или арифметические ошибки.
25. Заявка составляется на языке в соответствии с законодательством Республики Казахстан. При этом Заявка может содержать документы, составленные на другом языке при условии, что к ним будет прилагаться точный перевод на язык Тендерной документации и в этом случае преимущество будет иметь перевод.

3. Обеспечение Заявки

26. Потенциальный поставщик вносит обеспечение Заявки в размере, указанном в пункте 14 Тендерной документации, в качестве гарантии того, что он:
    1) не отзовет либо не изменит свою Заявку после истечения окончательного срока предоставления Заявок;
    2) в случае определения его победителем тендера заключит договор с Заказчиком/ Организатором закупок в сроки, установленные протоколом об итогах тендера и

предоставления Заявок;

2) в случае определения его победителем тендера заключит договор с Заказчиком/ Организатором закупок в сроки, установленные протоколом об итогах тендера и внесет обеспечение возврата аванса (предоплаты).

27. Потенциальный поставщик вправе выбрать один из следующих видов обеспечения Заявки:

1) банковскую гарантию - по форме приложения 5 к настоящей Тендерной документации;

2) гарантийный денежный взнос, который вносится на банковский счет Заказчика/ Организатора закупок;

При этом срок действия банковской гарантии должен быть не менее срока действия тендерной заявки.

28. В случае внесения потенциальным поставщиком обеспечения заявки на участие в электронном тендере в виде банковской гарантии, ее оригинал представляется Заказчику до окончательного срока представления заявок на участие в электронном тендере.

29. Расчет соответствия суммы внесенного обеспечения заявки на участие в тендере требованиям тендерной документации определяется согласно курса Национального Банка Республики Казахстан, установленного на дату перечисления платежа, выдачи банковской гарантии или иного обеспечения, определенного Заказчиком/Организатором закупок.

30. Все Заявки, не содержащие подтверждения внесения обеспечения Заявки, отклоняются тендерной комиссией как не отвечающие требованиям Тендерной документации. В случае внесения обеспечения Заявки на участие путем перечисления гарантийного денежного взноса на банковский счет Заказчика/Организатора закупок в подтверждающем документе должны быть указаны название тендера либо иные данные, позволяющие установить, что обеспечение представлено в рамках проводимой закупки, сумма обеспечения, наименования Заказчика/Организатора закупок и потенциального поставщика.

31. Обеспечение Заявки не возвращается Заказчиком/Организатором закупок при наступлении одного из следующих случаев:

1) потенциальный поставщик отозвал Заявку после истечения окончательного срока представления Заявок;

2) потенциальный поставщик, определенный победителем тендера, уклонился от заключения договора о закупках;

3) победитель тендера, заключив договор о закупках, не исполнил либо несвоевременно исполнил требования, установленные Тендерной документацией о внесении обеспечения возврата аванса (предоплаты);

4) потенциальный поставщик, занявший по итогам сопоставления и оценки второе место, определенный в случае, предусмотренном пунктом 81 настоящей Тендерной документации, уклонился от заключения договора о закупках или, заключив договор о закупках, не исполнил либо несвоевременно исполнил требование, установленное Тендерной документацией, о внесении обеспечения возврата аванса (предоплаты);

5) несоответствия нотариально засвидетельствованных копий документов, предоставленных в соответствии с пунктом 33 Тендерной документации, электронным документам.

Требование, установленное настоящим подпунктом Тендерной документации, не распространяется на случаи, когда в период с момента подачи заявки до момента заключения договора, в документы, содержащиеся в заявке, были внесены изменения в соответствии с требованиями законодательства.

32. Заказчик/Организатора закупок возвращает потенциальному поставщику внесенное им обеспечение Заявки в течение 10 (десять) рабочих дней со дня наступления одного из следующих случаев:

1) отзыва данным потенциальным поставщиком своей Заявки до истечения окончательного срока представления Заявок;

2) подписания протокола об итогах тендера. Указанный случай не распространяется на участника тендера, определенного победителем и потенциального поставщика, занявшего по итогам сопоставления и оценки второе место;

3) вступления в силу договора о закупках и внесения победителем тендера обеспечения возврата аванса (предоплаты), предусмотренного Тендерной документации;

4) вступления в силу договора о закупках и внесения потенциальным поставщиком, занявшим по итогам сопоставления и оценки второе место, определенным в случае, предусмотренном пунктом 81 настоящей Тендерной документации, обеспечения возврата аванса (предоплаты), предусмотренного тендерной документацией.

4. Содержание Заявки

33. З

4. Содержание Заявки

33. Заявка должна содержать следующие документы:

1) электронную форму Заявки согласно приложениям 3, 4 к настоящей Тендерной документации;
2) нотариально засвидетельствованную копию лицензии либо заявление потенциального поставщика, содержащее ссылку на официальный интернет-источник (веб-сайт) государственного органа, выдавшего лицензию, использующего электронную систему лицензирования (на деятельность, которая подлежит обязательному лицензированию);
3) техническую спецификацию (техническое задание) потенциального поставщика потенциального поставщика, которая должна соответствовать требованиям, установленным тендерной документацией;
4) перечень соисполнителей при оказании услуг, объем и виды передаваемых на соисполнение услуг, который не должен превышать определенного в пункте 39 тендерной документации предельного объема услуг.
5) нотариально засвидетельствованные копии лицензий либо заявление потенциального поставщика, содержащее ссылку на официальный интернет источник (веб-сайт) государственного органа, выдавшего лицензию, использующего электронную систему лицензирования оказываемые соисполнителем услуги в случае, если потенциальный поставщик привлекает субподрядчиков (соисполнителей) на тендер, которым предполагается деятельность, подлежащая обязательному лицензированию;
6) оригинал документа, подтверждающего внесение обеспечения заявки на участие в открытом тендере, соответствующего условиям внесения, содержанию и виду, изложенному в тендерной документации, при этом сумма обеспечения заявки на участие в открытом тендере не должна быть ниже размера, установленного тендерной документацией

Срок действия обеспечения заявки на участие в тендере должен быть не менее срока действия заявки на участие в тендере.

7) оригинал или нотариально засвидетельствованную копию документа о назначении (избрании) первого руководителя потенциального поставщика (в случае участия консорциума представляется оригинал или нотариально засвидетельствованная копия документа о назначении (избрании) первого руководителя каждого юридического лица, входящего в консорциум, а также оригинал или нотариально засвидетельствованная копия документа, подтверждающего право подписания соглашения о консорциуме уполномоченным лицом каждого юридического лица, входящего в консорциум);
8) документы, подтверждающие применимость к заявке критериев оценки и сопоставления, указанных в пункте 55 настоящей тендерной документации

При этом непредставление документов, подтверждающих критерии, влияющие на условное понижение цены, не является основанием для отклонения такой заявки;

9) ценовое предложение заполняется в Системе;
10) нотариально засвидетельствованную копию свидетельства о государственной регистрации (перерегистрации) юридического лица или справки о государственной регистрации юридического лица либо заявление потенциального поставщика, содержащее ссылку на официальный интернет источник (www.e.gov.kz) государственного органа, выдавшего справку, использующего электронную систему регистрации, для физического лица – нотариально засвидетельствованную копию документа о регистрации в качестве субъекта предпринимательства, для временного объединения юридических лиц (консорциум) - нотариально засвидетельствованную копию соглашения о консорциуме и нотариально засвидетельствованные копии свидетельств о государственной регистрации (перерегистрации) участников консорциума;
11) документ, содержащий сведения об учредителях: нотариально засвидетельствованную копию устава, утвержденного в установленном законодательством порядке; для юридических лиц, зарегистрированных на основании типового устава – копию заявления установленной формы о регистрации юридического лица; в случае участия консорциума представляется нотариально засвидетельствованная копия устава каждого юридического лица, входящего в консорциум; нотариально засвидетельствованную копию выписки из реестра держателей акций, выданную не более чем за 30 (тридцать) календарных дней до даты вскрытия заявок;
12) сведения об ознакомлении потенциального поставщика с условиями внесения потенциального поставщика в Перечень ненадежных потенциальных поставщиков

реестра держателей акций, выданную не более чем за 30 (тридцать) календарных дней до даты вскрытия заявок;

12) сведения об ознакомлении потенциального поставщика с условиями внесения потенциального поставщика в Перечень ненадежных потенциальных поставщиков (поставщиков) Холдинга;

13) оригинал или нотариально засвидетельствованную копию доверенности, выданную лицу (лицам), представляющему интересы потенциального поставщика, на право подписания заявки и документов, содержащихся в заявке на участие в тендере, за исключением первого руководителя потенциального поставщика, имеющего право выступать от имени потенциального поставщика без доверенности, в соответствии с уставом потенциального поставщика.

Заявка на участие в электронном тендере должна соответствовать требованию к языку составления и представления заявок на участие в тендере, изложенного в тендерной документации, а также срок действия заявки на участие в открытом тендере должен соответствовать или быть не менее срока, установленного тендерной документацией.

При осуществлении электронных закупок документы, предусмотренные данным пунктом, представляются в порядке, предусмотренном Инструкцией по проведению электронных закупок.

34. Потенциальный поставщик, не являющийся резидентом Республики Казахстан, представляет те же документы, что и резиденты Республики Казахстан, в соответствии с пунктом 33 настоящей Тендерной документации, либо оригиналы или нотариально засвидетельствованные копии документов, содержащих аналогичные сведения о потенциальном поставщике-нерезиденте Республики Казахстан с нотариально засвидетельствованным переводом на язык Тендерной документации.

35. В случае, если потенциальным поставщиком представляются документы, исходящие от компетентных органов и организаций иностранных государств, они принимаются при наличии консульской легализации, если иное не предусмотрено законодательством Республики Казахстан или международным договором, участниками которого являются Республика Казахстан и государство, от органов и организаций которого исходит представляемый документ.

36. Техническая спецификация Заявки на участие в тендере должна содержать:

1) документы, подтверждающие соответствие предлагаемого товара, услуги Технической спецификации, указанной в Приложении № 2.

37. Ценовое предложение участника тендера, являющегося резидентом Республики Казахстан, должно быть выражено в тенге. Ценовое предложение участника тендера, не являющегося резидентом Республики Казахстан, может быть выражено в иной валюте.

38. Ценовое предложение должно содержать цену за единицу, а также общую/итоговую цену товаров, и услуг без учета НДС, с включенными в нее расходами на их транспортировку и страхование, оплату таможенных пошлин, других налогов, сборов, а также иных расходов, предусмотренных условиями поставки товаров, оказания услуг.

39. Не допускается передача потенциальным поставщиком соисполнителям на соисполнение в совокупности более двух третей объема услуг.

5. Изменение Заявок и их отзыв

40. Потенциальный поставщик с применением ЭЦП вправе изменить или отозвать свою заявку на участие в электронном тендере в любое время до истечения окончательного срока представления Заявок, не утрачивая права на возврат внесенного им обеспечения заявки на участие в электронном тендере.

41. Не допускается внесение изменеий в Заявки на участие в электронном тендере, после истечения окончательного срока их представления.

42. Потенциальный поставщик несет все расходы, связанные с его участием в тендере. Заказчик/Организатор закупок, тендерная комиссия, экспертная группа, эксперт не несут обязательств по возмещению этих расходов независимо от итогов электронного тендера.

6. Вскрытие и рассмотрение Заявок на участие в электронном тендере

43. После наступления даты и времени вскрытия заявок, указанных в объявлении заявки автоматически вскрываются Системой и предоставляется доступ для их просмотра, как тендерной комиссии, так и потенциальным поставщикам, принявшим участие в данном электронном тендере.

44. Заявка на участие в электронном тендере поступившая в Систему после истечения окончательного срока приема заявок на участие в электронном тендере подлежит автоматическому отклонению Системой.

44. Заявка на участие в электронном тендере поступившая в Систему после истечения окончательного срока приема заявок на участие в электронном тендере подлежит автоматическому отклонению Системой.

45. В случае отсутствия представленных потенциальными поставщиками заявок по истечении окончательного срока представления заявок Системой автоматически формируется объявление об итогах.

46. Протокол вскрытия открытого электронного тендера оформляется в Системе и заверяется тендерной комиссией посредством ЭЦП.

47. Протокол вскрытия конвертов с Заявками на участие в открытом тендере должен содержать следующие сведения:

1) день, время и место вскрытия заявок;
2) состав тендерной комиссии;
3) полное наименование, фактический адрес потенциальных поставщиков, предоставивших Заявки в установленные сроки, с указанием даты и времени предоставления Заявок;
4) информацию о содержании Заявок, в том числе документов, подтверждающих применимость к заявке критериев оценки и сопоставления, влияющих на условное понижение цены, указанных в пункте 55 настоящей Тендерной документации, ценах и скидках, заявленных потенциальными поставщиками в ценовых предложениях на понижение цены (в случае их наличия);

48. Заявки рассматриваются тендерной комиссией на предмет соответствия Заявок требованиям пункта 33 настоящей Тендерной документации. Не отклоненные по основаниям, указанным в пункте 50 настоящей Тендерной документации, Заявки сопоставляются и оцениваются тендерной комиссией в целях выбора победителя электронного тендера, предложившего наилучшие условия поставки (выполнения, оказания) закупаемых товаров, услуг.

49. Заявки на участие в электронном тендере рассматриваются тендерной комиссией в срок не более 10 (десяти) рабочих дней со дня вскрытия Системой заявок на участие в электронном тендере. При проведении закупок товаров, услуг, имеющих сложные технические характеристики и спецификации, заявки рассматриваются тендерной комиссией с привлечением эксперта (экспертной комиссии) в срок не более 20 (двадцати) рабочих дней со дня вскрытия Системой заявок.

В случае проведения закупок товаров, по которым часть лотов или один лот требуют дополнительного рассмотрения, связанного с испытанием продукции, в связи с предложением потенциальным поставщиком альтернативных технических характеристик и (или) технологических решений при ее производстве, срок рассмотрения заявок по данному лоту (лотам) дополнительно продлевается до получения результатов испытаний, но не более чем на 20 (двадцать) рабочих дней. При этом по оставшимся лотам, не требующим дополнительного рассмотрения, заявки тендерной комиссией рассматриваются в сроки, установленные абзацем первым настоящего пункта.

50. При рассмотрении Заявок тендерная комиссия вправе:

1) запросить в Системе у потенциальных поставщиков материалы и разъяснения, необходимые для рассмотрения, оценки и сопоставления заявок (за исключением предложенной цены (скидок), технической спецификации и документов, подтверждающих критерии, влияющие на условное понижение цены, предусмотренные пунктом 55 настоящей Тендерной документации);

2) с целью уточнения сведений, содержащихся в Заявках, запросить необходимую информацию у соответствующих государственных органов, физических и юридических лиц.

При этом не допускаются запросы и иные действия тендерной комиссии, связанные с приведением Заявки на участие в тендере в соответствие с требованиями пункта 33 настоящей Тендерной документации, заключающиеся в дополнении Заявки недостающими документами, замене документов, приведении в соответствие ненадлежащим образом оформленных документов.

51. Тендерная комиссия отклоняет Заявку в случае:

1) признания заявки на участие в тендере несоответствующей требованиям, предусмотренным пунктом 33 настоящей Тендерной документации, за исключением случаев, несоответствия технической спецификации, когда потенциальный поставщик предлагает лучшие условия поставки товара, оказания услуг, а также лучшие характеристики закупаемых товаров, услуг;
1) если потенциальный поставщик является аффилированным лицом другого потенциального поставщика, подавшего Заявку на участие в данном тендере (лоте);
2) если ценовое предложение потенциального поставщика превышает сумму, выделенную для закупки;
2) потенциальный поставщик либо его субподрядчик (соисполнитель), либо юридическое лицо, входящее в консорциум, состоит в Перечне ненадежных потенциальных поставщиков (поставщиков) Холдинга и (или) в Реестре недобросовестных участников

2) потенциальный поставщик либо его субподрядчик (соисполнитель), либо юридическое лицо, входящее в консорциум, состоит в Перечне ненадежных потенциальных поставщиков (поставщиков) Холдинга и (или) в Реестре недобросовестных участников государственных закупок;

52. Не допускается отклонение заявки на участие в открытом тендере по формальным основаниям.

Формальными основаниями являются случаи, не указанные в пункте 50 настоящей Тендерной документации.

53. Неотклоненные заявки оцениваются и сопоставляются тендерной комиссией согласно критериям, содержащимся в тендерной документации. При этом оценке подлежит общая/итоговая цена ценового предложения потенциального поставщика.

Победитель тендера определяется на основе наименьшей условной цены, рассчитываемой с учётом применения критериев, содержащихся в тендерной документации.

54. Потенциальный поставщик, занявший по итогам оценки и сопоставления второе место, определяется на основе цены, следующей после наименьшей условной цены, рассчитываемой с учётом применения критериев, содержащихся в тендерной документации.

При равенстве условных цен тендерных ценовых предложений победителем (или потенциальным поставщиком, занявшим по итогам оценки и сопоставления второе место) признается отечественный товаропроизводитель закупаемого товара.

При равенстве условных цен тендерных ценовых предложений отечественных товаропроизводителей победителем (или потенциальным поставщиком, занявшим по итогам оценки и сопоставления второе место) признается отечественный товаропроизводитель, имеющий больший опыт работы производства закупаемых товаров.

При равенстве условных цен тендерных ценовых предложений, в случае отсутствия отечественного товаропроизводителя победителем (или потенциальным поставщиком, занявшим по итогам оценки и сопоставления второе место) признается потенциальный поставщик, имеющий больший опыт работы на рынке закупаемых товаров, являющихся предметом открытого тендера.

При равенстве условных цен тендерных ценовых предложений и равном опыте работы на рынке закупаемых товаров (или в случае невозможности определения опыта работы на основании представленных потенциальными поставщиками документов) победителем (или потенциальным поставщиком, занявшим по итогам оценки и сопоставления второе место) признается потенциальный поставщик, ранее предоставивший заявку на участие в тендере.

55. Неотклоненные Заявки оцениваются и сопоставляются тендерной комиссией согласно критериям, содержащимся в тендерной документации. При этом оценке подлежит общая/итоговая цена ценового предложения потенциального поставщика. Победитель тендера определяется на основе наименьшей условной цены, рассчитанной с учетом применения следующих обязательных критериев:

№	Критерий	Условное понижение/увеличение цены
1	Потенциальный поставщик является отечественным товаропроизводителем закупаемого товара в соответствии с представленным оригиналом или нотариально заверенной копией сертификата происхождения товара (формы CT KZ) либо копией, заверенной государственным или иным уполномоченным органом, выдавшим сертификат и состоит в Реестре отечественных товаропроизводителей.	- 5%
2	Потенциальный поставщик является добросовестным поставщиком в соответствии с Перечнем добросовестных поставщиков Холдинга	- 1%
3	Потенциальный поставщик является организацией инвалидов (физическим лицом - инвалидом, осуществляющим предпринимательскую деятельность), производящей закупаемый товар в соответствии с представленным оригиналом или нотариально заверенной копией сертификата происхождения товара (формы CT KZ) либо копией, заверенной государственным или иным уполномоченным органом, выдавшим сертификат и состоит в Реестре организаций инвалидов (физических лиц - инвалидов, осуществляющих предпринимательскую деятельность) Холдинга	-5%
4	Наличие у потенциального поставщика опыта работы на однородном рынке закупаемых товаров, услуг, в течение	- 1,5% за 3 года опыта работы и - 0,5% за

	Холдинга	
4	Наличие у потенциального поставщика опыта работы на однородном рынке закупаемых товаров, услуг, в течение последних 5 лет, подтвержденного соответствующими оригиналами или нотариально засвидетельствованными копиями накладных, соответствующих актов, подтверждающих прием-передачу поставленных товаров, оказанных услуг.	- 1,5% за 3 года опыта работы и - 0,5% за каждый последующий 1 год работы, но не более 2,5%
5	Наличие у потенциального поставщика сертифицированной системы (сертифицированных систем) менеджмента в соответствии с требованиями государственных стандартов Республики Казахстан, соответствующей предмету проводимых закупок, подтвержденной нотариально засвидетельствованной копией сертификата системы менеджмента или копией, заверенной организацией, выдавшей сертификат	- 1%
6	Местное содержание в товаре потенциального поставщика, являющегося предметом проводимых закупок, которое определяется на основании оригинала или нотариально заверенной копии сертификата происхождения товара (формы СТ KZ) либо копии, заверенной государственным уполномоченным органом, выдавшим сертификат;	- 0,15% за каждый 1% местного содержания
7	Заявление (декларацию), подписанную первым руководителем потенциального поставщика или уполномоченным им лицом, с указанием наименования закупаемого товара, производство которого потенциальный поставщик обязуется организовать на территории Республики Казахстан до полного исполнения договора и доли местного содержания в процентном выражении в товаре. При этом потенциальный поставщик должен быть отечественным товаропроизводителем товаров, однородных с закупаемым в соответствии с представленным оригиналом или нотариально заверенной копией сертификата происхождения товара (формы СТ KZ) либо копией, заверенной государственным или иным уполномоченным органом, выдавшим сертификат. В случае применения к заявке потенциального поставщика на участие в тендере критерия, определенного настоящим подпунктом, критерии предусмотренные подпунктами 1) и 6) настоящего пункта к заявке на участие в тендере данного потенциального поставщика не применяются.	- 0,15% за каждый 1% от указанного в заявлении (декларации) процентного значения местного содержания
8	Потенциальный поставщик является участником специальной экономической зоны (СЭЗ) «Парк инновационных технологий» и поставляет товары, оказывает услуги, относящиеся к приоритетным видам деятельности, соответствующим целям СЭЗ «Парк инновационных технологий» и предмету закупок в соответствии с представленной нотариально засвидетельствованной копией договора об осуществлении деятельности в качестве участника СЭЗ «Парк инновационных технологий», заключенного между управляющей компанией и участником. В случае применения к заявке потенциального поставщика на участие в тендере критерия, определенного настоящим подпунктом, критерии, предусмотренные подпунктами 1) и 3) настоящего пункта к заявке на участие в тендере данного потенциального поставщика не применяются.	- 5 %

Потенциальному поставщику также необходимо заполнить Приложение 8 к Тендерной документации, для учета вышеуказанных критериев.

56. В случае непредставления потенциальным поставщиком документов, подтверждающих критерии, влияющие на условное понижение цены, тендерная комиссия не применяет к такому потенциальному поставщику условную скидку, при этом непредставление документов, подтверждающих критерии, влияющие на условное понижение цены, не является основанием для отклонения такой заявки.

такому потенциальному поставщику условную скидку, при этом непредставление документов, подтверждающих критерии, влияющие на условное понижение цены, не является основанием для отклонения такой заявки.

57. В случае участия в тендере консорциума обязательные критерии оценки и сопоставления заявок потенциальных поставщиков на участие в электронном тендере, влияющие на условное понижение цены тендерной комиссией, применяются только к головному участнику консорциума, определенному консорциальным соглашением его участников.

58. Под отечественным товаропроизводителем понимаются потенциальные поставщики – производящие на территории Республики Казахстан:

товары, полностью произведенные в Республике Казахстан, перечисленные в пункте 5 Правил по определению страны происхождения товара, составлению и выдаче акта экспертизы о происхождении товара и оформлению, удостоверению и выдаче сертификата о происхождении товара, утвержденных постановлением Правительства Республики Казахстан от 22 октября 2009 года № 1647.

товары, подвергнутые достаточной переработке в Республике Казахстан в соответствии с критериями достаточной переработки, установленными пунктом 7 Правил по определению страны происхождения товара, составлению и выдаче акта экспертизы о происхождении товара и оформлению, удостоверению и выдаче сертификата о происхождении товара, утвержденных постановлением Правительства Республики Казахстан от 22 октября 2009 года № 1647.

Под местным содержанием понимается процентное содержание стоимости оплаты труда граждан Республики Казахстан, задействованных в исполнении договора о закупках от общего фонда оплаты труда по данному договору и (или) стоимости доли (долей) местного происхождения, установленной в товаре (товарах) в соответствии с критериями достаточной переработки или полного производства резидентами Республики Казахстан от общей стоимости товара (товаров) по договору о закупках.

Для определения местного содержания в товаре потенциальный поставщик должен предоставить оригинал или нотариально заверенную копию сертификата происхождения товара (формы CT KZ) либо копии, заверенную (-ые) государственным уполномоченным органом, выдавшим сертификат, или заявление–декларацию, выданное соответствующим уполномоченным органом при выпуске единичного, нестандартного, несерийного товара или товара, выпускаемого под заказ.

59. Если ценовые предложения участников тендера выражены в различных валютах, то для их оценки и сопоставления они переводятся в валюту Республики Казахстан - тенге - по официальному курсу национальной валюты Республики Казахстан к иностранным валютам, установленному Национальным банком Республики Казахстан на день вскрытия конвертов с Заявками.

7. Подведение итогов тендера

60. Протокол итогов электронного тендера оформляется в Системе, заверяется тендерной комиссией посредством ЭЦП.

61. Заказчик/организатор закупок не позднее 3 (трех) рабочих дней со дня заверения тендерной комиссией посредством ЭЦП протокола об итогах открытого тендера направляет победителю уведомление.

62. В случае признания заявки потенциального поставщика победившей, потенциальный поставщик в срок не более 5 (пяти) рабочих дней с момента получения уведомления, направляет Заказчику нотариально засвидетельствованные копии документов указанные в пункте 33 Тендерной документации.

В протоколе об итогах тендера должна содержаться информация:

- о месте и времени подведения итогов;
- о поступивших Заявках потенциальных поставщиков на участие в тендере;
- о сумме, выделенной для закупки, предусмотренной годовым планом закупок без учета НДС;
- об отклоненных Заявках с указанием детализированных оснований отклонения и неприменения критериев влияющих на условное понижение цены;
- о потенциальных поставщиках, чьи заявки на участие в тендере не отклонены;
- о результатах применения критериев оценки и сопоставления;
- об итогах тендера;
- о сумме и сроках заключения договора о закупках в случае, если тендер состоялся;
- о потенциальном поставщике, занявшем второе место;
- сведения о направлении в соответствии с пунктом 50 настоящей Тендерной документации запросов потенциальным поставщикам, соответствующим государственным органам, физическим и юридическим лицам;
- иная информация по усмотрению тендерной комиссии.

запросов потенциальным поставщикам, соответствующим государственным органам, физическим и юридическим лицам;

- иная информация по усмотрению тендерной комиссии.

63. Тендер признаётся тендерной комиссией несостоявшимся в случае:

1) представления заявок на участие в тендере менее двух потенциальных поставщиков;

2) если после отклонения тендерной комиссией по основаниям, предусмотренным пунктом 51 настоящей Тендерной документации, осталось менее двух Заявок на участие в тендере потенциальных поставщиков;

3) уклонения победителя тендера и потенциального поставщика, занявшего второе место, от заключения договора;

4) непредставления победителем тендера и потенциальным поставщиком, занявшим второе место, обеспечения возврата аванса (предоплаты) в соответствии с пунктами 75 и 83 настоящей Тендерной документации.

64. Заказчик/Организатор закупок до даты вскрытия заявок на участие в тендере вправе отказаться от осуществления закупок в случаях сокращения расходов на приобретение товаров, услуг, предусмотренных в плане(нах) закупок, обоснованного уменьшения потребности или обоснованной нецелесообразности приобретения товаров, услуг. Отказ от закупок осуществляется путем внесения соответствующих изменений в план(ы) закупок.

При этом в случае, предусмотренном в абзаце первом настоящего пункта внесение изменений и дополнений в план закупок, свидетельствующих о последующем увеличении расходов на приобретение, увеличении потребности или возникновении целесообразности приобретения таких товаров, услуг в текущем году не допускается.

В этом случае Заказчик/ Организатор закупок обязан:

1) в течение 3 (трех) рабочих дней со дня принятия решения об отказе от осуществления закупок известить об этом лиц, участвующих в проводимых закупках; Уведомление об отказе от осуществления электронного тендера автоматически рассылается Системой всем участникам электронных закупок.

2) в течение 5 (пяти) рабочих дней со дня принятия решения об отказе от осуществления закупок возвратить внесенные обеспечения заявок.

65. В случае обнаружения нарушений, влияющих на итоги электронного тендера (лота), в проводимом/проведенном тендере (лоте) Заказчик/Организатор закупок и (или) тендерная комиссия до момента заключения договора обязана отменить тендер (лот) или его итоги. При этом, тендер (лот) должен быть пересмотрен (в том же составе тендерной комиссии с теми же потенциальными поставщиками, участвовавшими в тендере (лоте) или проведен повторно.

Заказчик/Организатор закупок в течение 2 (двух) рабочих дней со дня принятия решения об отмене электронного тендера (лота) или его итогов обязан известить об этом лиц, участвовавших в проводимых закупках. Уведомление об отмене тендера автоматически рассылается системой всем участникам электронных закупок. В случае обнаружения нарушений в тендерной документации по тендеру (лоту) до даты вскрытия конвертов с заявками потенциальных поставщиков Заказчик/ организатор закупки обязан отменить тендер (лот), привести в соответствие тендерную документацию и заново объявить тендер (лот).

8. Заключение договора о закупках по итогам электронного тендера

66. Заказчик до заключения договора о закупках с победителем электронного тендера производит сопоставление электронных документов потенциального поставщика с нотариально засвидетельствованными копиями документов, в случае несоответствия нотариально засвидетельствованных копий документов электронным документам, Заказчиком удерживается внесенное потенциальным поставщиком обеспечение заявки и тендерная комиссия определяет победителем электронного тендера потенциального поставщика, занявшего по итогам сопоставления и оценки второе место.

67. Сведения о поставщике, чьи нотариально засвидетельствованные копии документов не будут соответствовать электронным документам, направляются Заказчиком в Уполномоченный орган по вопросам закупок в лице дочерней организации, определенной Правлением Фонда для внесения сведений о таком поставщике в Перечень ненадёжных потенциальных поставщиков (поставщиков) Холдинга.

Требования, установленные настоящим пунктом тендерной документации, не распространяются на случаи, когда в период с момента подачи заявки до момента заключения договора, в документы, содержащиеся в заявке были внесены изменения в соответствии с требованиями законодательства.

68. Договор о закупках заключается в соответствии с содержащимся в Тендерной документации договора, в документы, содержащиеся в заявке были внесены изменения в соответствии с требованиями законодательства.

68. Договор о закупках заключается в соответствии с содержащимся в Тендерной документации проектом договора Приложение 7.

В случае заключения договора о закупках с нерезидентом Республики Казахстан допускается оформление договора о закупках в предлагаемой им форме с учетом требований законодательства Республики Казахстан.

69. Заказчик/ Организатор закупок не менее чем за 10 (десять) календарных дней до окончательного срока подписания договора согласно протокола об итогах тендера направляет победителю тендера подписанный со стороны Заказчика/ Организатора закупок проект договора о закупках. Победитель тендера должен подписать проект договора о закупках в течение 5 (пяти) календарных дней с даты получения проекта договора о закупках, подписанного со стороны Заказчика/Организатора закупок. Договор о закупках заключается в сроки, указанные в протоколе об итогах тендера, но не ранее чем через 5 (пять) календарных дней с даты заверения посредством ЭЦП протокола об итогах и не более 20 (двадцати) календарных дней с даты заверения протокола об итогах.

В случае, если договор о закупках заключается с нерезидентами Республики Казахстан данный срок может быть дополнительно продлен на 10 (десять) календарных дней.

Тендерной документацией допускается установление возможности доработки проекта договора, прилагаемого к Тендерной документации, с учётом предложений победителя тендера. При этом вносимые изменения в проект договора о закупках не должны затрагивать условия договора, касающиеся наименования товара, услуги, цены и другие условия, явившиеся основой для выбора поставщика.

70. Договор о закупках должен содержать цену, предложенную победителем тендера, с начислением к ней НДС, за исключением случаев, когда победитель тендера не является плательщиком НДС или поставляемый товар, оказываемая услуга не облагается НДС в соответствии с законодательством Республики Казахстан.

71. Договор о закупках товаров и услуг должен содержать указанную поставщиком в заявке на участие в тендере долю местного содержания в товарах, или услугах согласно сертификату происхождения товара формы CT-KZ, гарантийному обязательству и условие о его ответственности за неисполнение обязательств по доле местного содержания в виде штрафа в размере 5%, а также 0,15% за каждый 1% невыполненного местного содержания, от общей стоимости договора, но не более 15% от общей стоимости договора. Также договор о закупках должен содержать ответственность поставщика в виде штрафа за несвоевременное предоставление отчетности по местному содержанию и предоставление недостоверной отчетности.

72. Договор о закупках должен предусматривать право Заказчика/ Организатора закупок в одностороннем порядке отказаться от исполнения договора и требовать возмещения убытков в случае представления потенциальным поставщиком/поставщиком недостоверной информации по доле местного содержания в товарах, услугах.

73. Договор о закупках должен содержать обязательство поставщика по организации производства закупаемого товара на территории Республики Казахстан до полного исполнения договора о закупках и доле местного содержания в процентном выражении в товаре, представленной им в заявке на участие в тендере в виде заявления (декларации). Подтверждением исполнения обязательства поставщика по организации производства закупаемого товара на территории Республики Казахстан и доле местного содержания в процентном выражении является предоставление поставщиком до даты подписания сторонами соответствующего (окончательного) акта, подтверждающего прием – передачу закупленного товара, сертификата формы CT-KZ (оригинал, нотариально засвидетельствованная копия, либо копия, заверенная печатью уполномоченного органа по выдаче сертификата о происхождении товара для внутреннего обращения) на закупаемый товар.

В случае непредставления поставщиком в указанные сроки сертификата формы CT-KZ, поставщик несет ответственность за неисполнение обязательств по организации производства закупаемого товара в виде штрафа в размере 15% от общей стоимости договора о закупках, который должен быть оплачен поставщиком или может быть удержан Заказчиком/Организатором закупок до подписания сторонами соответствующего (окончательного) акта, подтверждающего прием – передачу закупленного товара. При этом сведения о таком поставщике Заказчиком/ Организатором закупок в установленном порядке направляются в Уполномоченный орган по вопросам закупок в лице дочерней организации, определенной Правлением Фонда для внесения в Перечень ненадежных потенциальных поставщиков (поставщиков) Холдинга.

В случае неисполнения поставщиком обязательства по доле местного содержания в процентном выражении в товаре, указанной в заявлении (декларации), поставщик несет вопросам закупок в лице дочерней организации, определенной Правлением Фонда для внесения в Перечень ненадежных потенциальных поставщиков (поставщиков) Холдинга.

В случае неисполнения поставщиком обязательства по доле местного содержания в процентном выражении в товаре, указанной в заявлении (декларации), поставщик несет ответственность в виде штрафа в размере 5%, а также 0,15% за каждый 1% невыполненного процентного значения местного содержания, указанного в заявлении (декларации), но не более 15% от общей стоимости договора, который должен быть оплачен поставщиком или может быть удержан Заказчиком/ Организатором закупок до подписания сторонами соответствующего (окончательного) акта, подтверждающего прием – передачу закупленного товара.

74. Если договор заключается с организацией инвалидов (физическим лицом - инвалидом, осуществляющим предпринимательскую деятельность), состоящей в Реестре организаций инвалидов (физических лиц - инвалидов, осуществляющих предпринимательскую деятельность) Холдинга, отечественным товаропроизводителем закупаемого товара или участником СЭЗ «Парк инновационных технологий» (при закупке товаров, услуг, относящихся к приоритетным видам деятельности, соответствующим целям СЭЗ «Парк инновационных технологий» и предмету закупок), условиями договора должна предусматриваться предоплата в размере не менее 30% от суммы договора, которая должна выплачиваться не позднее 30 (тридцати) календарных дней с даты заключения договора.

75. В случае, если договором о закупках предусматривается выплата аванса (предоплаты), то победитель тендера должен в течение 20 (двадцати) рабочих дней со дня заключения договора о закупках представить обеспечение возврата аванса (предоплаты) в размере, указанном в пункте 17 настоящей Тендерной документации, путём перечисления гарантийного денежного взноса на банковский счет Заказчика/ Организатора закупок, или предоставления банковской гарантии по форме согласно приложению 6 к Тендерной документации, или в иной не противоречащей законодательству РК форме.

Не допускается совершение поставщиком действий, приводящих к возникновению у третьих лиц права требования в целом либо в части на внесенный гарантийный денежный взнос до полного исполнения обязательств по договору о закупках.

76. В качестве иного обеспечения возврата аванса (предоплаты) Поставщик может предоставить страховой договор на всю сумму выплаченного аванса (предоплаты).

При этом, страховой договор должен быть выдан страховой организацией, являющейся платежеспособной и финансово-устойчивой. Подтверждением платежеспособности и финансовой устойчивости принимается соблюдение страховой организацией пруденциальных нормативов в течение 12 (двенадцати) месяцев, предшествующих первому числу месяца, в котором выдан страховой договор.

Страховой договор должен быть подписан на условиях нулевой условной франшизы.

77. Источником информации являются ежемесячные данные, публикуемые на сайте уполномоченного органа по контролю и надзору финансовых рынков и финансовых организаций Национального банка Республики Казахстан.

78. В случае, если обеспечение возврата аванса (предоплаты) не будут предоставлены в указанные сроки, то Заказчиком/Организатором закупок в одностороннем порядке расторгается заключенный договор о закупках, удерживается внесенное потенциальным поставщиком обеспечение заявки и тендерная комиссия определяет победителем тендера потенциального поставщика, занявшего по итогам оценки и сопоставления второе место.

79. Заказчик/Организатор закупок при выплате аванса (предоплаты) участнику СЭЗ «Парк инновационных технологий» (при определении участника СЭЗ «Парк инновационных технологий» победителем тендера на поставку товаров, оказание услуг, относящихся к приоритетным видам деятельности, соответствующим целям СЭЗ «Парк инновационных технологий» и предмету закупок) вправе исключить требование о предоставлении обеспечения возврата аванса (предоплаты).

80. Заказчик/Организатор закупок возвращает внесенное обеспечение возврата аванса (предоплаты) в течение 10 (десяти) рабочих дней с даты поставки товара, услуг на сумму, превышающую сумму оплаченного аванса (предоплаты) по договору о закупках.

81. В случае, если победитель тендера в сроки, установленные протоколом об итогах тендера не представил Заказчику/Организатору закупок подписанный договор о закупках, то Заказчиком/Организатором закупок удерживается внесенное потенциальным поставщиком обеспечение заявки и тендерная комиссия в течение 3 (трех) рабочих дней со дня истечения срока установленного для подписания договора о закупках, победителем, или со дня письменного отказа от подписания договора о закупках победителем, определяет победителем тендера потенциального поставщика, занявшего по итогам оценки и сопоставления второе место по цене и на условиях, предложенных им в заявке на участие в тендере.

Уведомление о подписании договора о закупках поставщику, занявшему по итогам оценки и сопоставления второе место Заказчик/Организатор закупок обязан направить в течение 3 (трех) сопоставления второе место по цене и на условиях, предложенных им в заявке на участие в тендере.

Уведомление о подписании договора о закупках поставщику, занявшему по итогам оценки и сопоставления второе место Заказчик/Организатор закупок обязан направить в течение 3 (трех) рабочих дней со дня подписания решения тендерной комиссии о признании победителем поставщика, занявшего по итогам оценки и сопоставления второе место. Поставщик, занявший по итогам оценки и сопоставления второе место договор о закупках должен подписать в течение не более 5 (пяти) календарных дней с даты получения уведомления от Заказчика/Организатора закупок.

82. Если на этапе исполнения договора договор о закупках был расторгнут по вине поставщика, Заказчик/Организатор закупок должен направить потенциальному поставщику, занявшему по итогам оценки и сопоставления второе место уведомление о намерении заключения с ним договора о закупках, по цене, не превышающей предложенную им цену в заявке на участие в тендере, с учетом стоимости обязательств исполненных поставщиком и оплаченных Заказчиком/Организатором закупок. В случае, если потенциальным поставщиком, занявшим по итогам оценки и сопоставления второе место не будет представлен ответ на уведомление, то Заказчик/Организатор закупок по истечении 10 (десяти) рабочих дней с даты направления уведомления вправе осуществить закупки в соответствии с Правилами.

83. В случае, если договором о закупках предусматривается выплата аванса (предоплаты), победитель тендера, определенный в соответствии настоящей Тендерной документации должен в течение не более 20 (двадцати) рабочих дней с даты заключения договора о закупках представить обеспечение возврата аванса (предоплаты).

84. Сведения о поставщике, не внесшем обеспечение возврата аванса (предоплаты), Заказчиком/Организатором закупок направляются в установленном порядке в Уполномоченный орган по вопросам закупок в лице дочерней организации, определенной Правлением Фонда для внесения сведений о таком поставщике в Перечень ненадежных потенциальных поставщиков (поставщиков) Холдинга, за исключением случая, когда Заказчиком/Организатором закупок изменены условия оплаты по договору в связи с отказом потенциального поставщика от аванса (предоплаты) по договору, определенного Заказчиком/Организатором закупок.

При проведении электронных закупок, сведения о победителе тендера, не представившем оригиналы и/или нотариально засвидетельствованные копии документов, представленных им в составе заявки на участие в открытом тендере, а также в случае выявления несоответствия оригиналов и/или нотариально засвидетельствованных копий документов, представленных им в составе заявки на участие в открытом тендере, направляются Заказчиком в установленном порядке в Уполномоченный орган по вопросам закупок в лице дочерней организации, определенной Правлением Фонда для внесения сведений о таком поставщике в Перечень ненадежных потенциальных поставщиков (поставщиков) Холдинга.

85. Внесение изменений и дополнений в проект договора о закупках допускается по взаимному согласию сторон:

1) в части уменьшения суммы проекта договора о закупках при условии неизменности качества и других условий, явившихся основой для выбора поставщика;

2) в случае принятия Заказчиком/Организатором закупок альтернативных условий потенциального поставщика;

3) в случае отказа либо изменения условий выплаты аванса (предоплаты);

4) в части продления сроков выполнения обязательств поставщика по поставке товаров, оказанию услуг, в случаях его заключения в соответствии с пунктами 81 и 82 Тендерной документации с потенциальным поставщиком, занявшим по итогам оценки и сопоставления второе место, при этом договор о закупках заключается по цене, не превышающей предложенную им цену в заявке на участие в тендере. В таком случае учитывается произведенная Заказчиком/Организатором закупок оплата стоимости обязательств исполненных победителем тендера.

В случае применения пункта 81 Тендерной документации срок продлевается на количество дней, исчисляемые со дня подписания протокола об итогах тендера до даты истечения срока, установленного для подписания договора о закупках, победителем, или со дня письменного отказа от подписания договора о закупках победителем (за исключением случая, когда победитель тендера отказался от подписания договора в пределах срока, установленного для подписания договора). В случае применения пункта 82 Тендерной документации срок продлевается на количество дней, исчисляемые со дня заключения договора с победителем тендера до даты расторжения договора с победителем тендера.

86. Внесение изменений в заключенный договор о закупках допускаются по взаимному согласию сторон в следующих случаях:

1) в части уменьшения цены на товары, услуги и соответственно суммы договора о закупках, если в процессе исполнения договора о закупках цены на аналогичные закупаемые товары, услуги

согласию сторон в следующих случаях:

1) в части уменьшения цены на товары, услуги и соответственно суммы договора о закупках, если в процессе исполнения договора о закупках цены на аналогичные закупаемые товары, услуги изменились в сторону уменьшения;

2) в части уменьшения либо увеличения суммы договора о закупках на сумму и объем, не превышающие первоначально запланированные в плане закупок, связанной с уменьшением либо обоснованным увеличением потребности в объеме приобретаемых товаров, услуг, а также в части соответствующего изменения сроков исполнения договора, при условии неизменности цены за единицу товара, услуги, указанных в заключенном договоре о закупках. Такое изменение заключенного договора о закупках товаров, услуг допускается в пределах сумм и объемов, предусмотренных для приобретения данных товаров, услуг в плане закупок на год, определенных для осуществления закупки;

3) в случае, если поставщик в процессе исполнения заключенного с ним договора о закупках товаров, услуг предложил при условии неизменности цены за единицу более лучшие качественные и (или) технические характеристики, либо сроки и (или) условия поставки товаров, оказания услуг являющихся предметом заключенного с ним договора о закупках товаров, услуг;

4) в части уменьшения или увеличения суммы договора о закупках, связанной с изменением цен, тарифов, сборов и платежей, установленных законодательством Республики Казахстан. Такое изменение заключенного договора о закупках товаров, работ, услуг допускается в пределах сумм, предусмотренных для приобретения данных товаров, услуг в плане закупок;

5) в части изменения цены за единицу товара, на который устанавливается государственное регулирование цен в пределах цены, установленной государственным органом, осуществляющим руководство в сферах естественных монополий и на регулируемых рынках.

87. Изменения и дополнения, вносимые в договор о закупках, оформляются в виде дополнительного письменного соглашения к договору, являющегося неотъемлемой частью договора.

88. Не допускается вносить в проект либо заключенный договор о закупках изменения, которые могут изменить содержание условий проводимых (проведенных) закупок и (или) предложения, явившихся основой для выбора поставщика, по иным основаниям, не предусмотренным пунктами 85 и 86 настоящей Тендерной документации.

89. Потенциальные поставщики (поставщики) вправе обжаловать действия и решения, принимаемые в процессе закупок руководителями и членами органов Заказчика/Организатора закупок, а также иных лиц, включая членов тендерной, экспертной комиссий, эксперта.

90. Жалобы могут быть направлены для рассмотрения Организатору закупок: zakupDTK@telecom.kz, +7 (727) 226 82 61, в Фонд АО «Самрук-Қазына».

9. Разъяснение положений Тендерной документации

91. При проведении тендера Заказчик/Организатор закупок вправе организовать встречу с потенциальными поставщиками, получившими Тендерную документацию, для разъяснения положений Тендерной документации.

По итогам встречи с участниками тендера секретарь тендерной комиссии оформляет протокол, который должен содержать:

1) наименование, юридический адрес, контактные телефоны потенциальных поставщиков и их уполномоченных представителей с указанием фамилий, имен, отчеств присутствовавших на встрече, на основании документов, подтверждающих право представителя потенциального поставщика участвовать во встрече;
2) информацию о работниках Заказчика/Организатора закупок с указанием должности и фамилий, имен, отчеств участвовавших во встрече;
3) затронутые вопросы и ответы на них в рамках Тендерной документации;
4) сведения о необходимости внесения изменений и/или дополнений в Тендерную документацию.

Протокол подписывается работниками Заказчика/Организатора закупок, присутствовавшими на встрече и в течение 2 (двух) рабочих дней со дня проведения встречи направляется всем потенциальным поставщикам, участвовавшим во встрече, а также размещается на веб-сайте Заказчика/Организатора закупок и на веб-сайте Фонда.

92. Потенциальный поставщик, получивший Тендерную документацию, вправе обратиться с запросом в Системе о разъяснении положений Тендерной документации в срок не позднее 7 (семи) календарных дней до истечения окончательного срока приема Заявок.

Заказчик/Организатор закупок обязан не позднее 3 (трех) рабочих дней с момента поступления запроса ответить на него и разместить в Системе. Уведомление об ответе на запрос потенциального поставщика автоматически рассылается системой всем участникам электронных

Заказчик/Организатор закупок обязан не позднее 3 (трех) рабочих дней с момента поступления запроса ответить на него и разместить в Системе. Уведомление об ответе на запрос потенциального поставщика автоматически рассылается системой всем участникам электронных закупок

10. Изменение Тендерной документации

93. Изменения и дополнения в Тендерную документацию вносятся Заказчиком/Организатором закупок в установленном порядке в срок не позднее 5 (пяти) календарных дней до истечения окончательного срока представления Заявок. При этом окончательный срок представления Заявок продлевается не менее чем на 10 (десять) календарных дней. Об изменениях и дополнениях Тендерной документации и изменённом сроке представления Заявок Заказчик/ Организатор закупок уведомляет всех потенциальных поставщиков, получивших Тендерную документацию, в течение 2 (двух) рабочих дней со дня утверждения изменений и дополнений в Тендерную документацию посредством размещения соответствующей информации и Тендерной документации с внесенными изменениями на веб-сайте Заказчика/ Организатора закупок и на веб-сайте Фонда.

Приложения:

1. Перечень закупаемого товара и услуг (Приложение 1);
2. Техническая спецификация (техническое задание) закупаемого товара и услуг (Приложение 2);.
3. Форма Заявки потенциального поставщика для юридических лиц (Приложение 3);
4. Форма Заявки потенциального поставщика для физических лиц (Приложение 4);
5. Форма банковской гарантии в обеспечение заявки (Приложение 5);
6. Форма банковской гарантии в обеспечение возврата аванса (предоплаты) (Приложение 6);
7. Проект договора закупаемого товара и услуг (Приложение 7);
8. Критерии для расчета минимальной условной цены (Приложение 8).

Приложение 1
к Тендерной документации по электронному тендеру по закупке оборудования Пульта управления СОРМ с услугами монтажа и пуско-наладки "под ключ"

Перечень закупаемых товаров и услуг

№/№ лотов	Наименование товаров, услуг (по лотам)	Краткая характе-ристика (описание) товаров, услуг*	Ед. изм.	Коли-чество (объем потреб ности)	Срок поставки товаров, оказания услуг	Место поставки товаров, оказания услуг
№1	Оборудование Пульта управления СОРМ с услугами монтажа и пуско-наладки "под	См. Техническую спецификацию	Комп лект	1	Поставка оборудования в течение 90 (девяносто) календарных дней с момента подписания договора	DDP г. Алматы

№1	управления СОРМ с услугами монтажа и пуско-наладки "под ключ"	См. Техническую спецификацию (Приложение № 2)	Комплект	1	календарных дней с момента подписания договора. Оказание услуг в течение 180 (сто восемьдесят) календарных дней с момента подписания договора	DDP г. Алматы

*Полное описание и характеристика товаров и услуг, указаны в технической спецификации (Приложение 2).

Генеральный директор

Дирекции «Телеком Комплект» **Горбатовский Е. М.**

М.П

Приложение 2
к Тендерной документации по электронному тендеру по закупке оборудования Пульта управления СОРМ с услугами монтажа и пуско-наладки "под ключ"

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ
К ОБОРУДОВАНИЮ ПУЛЬТА УПРАВЛЕНИЯ СОРМ
(Интерфейс доступа)

1. Введение

Настоящие технические требования распространяются на комплекс оборудования Пульт Управления СОРМ для исполнение требований СТ РК 2267-2012 (Средства телекоммуникационного оборудования для обеспечения проведения оперативно-розыскных мероприятии).

Текст СТ РК 2267-2012 является неотъемлемой частью данного ТЗ. В случае разночтения требовании настоящего документа с техническими требованиями СТ РК 2267-2012, главенствующую силу имеет СТ РК 2267-2012

Настоящий документ определяет технические и функциональные требования к программному комплексу для обеспечения оперативно-розыскных мероприятий в телекоммуникационной сети фиксированной телефонной связи АО «Казахтелеком».

Программный комплекс ОРМ состоит из нескольких основных компонент:

- Система Управления Перехватом (СУП)
- Система Сбора и Мониторинга или Система Мониторинга (ССМ/СМ)

СУП используется для управления процессом работы персонала с перехватами и предоставляет технические инструменты для исполнения перехватов в телекоммуникационной сети. СУП является центральным инструментом для хранения и управления перехватами, обеспечивает пользовательскую политику доступа к программе и управляет системой сбора информации.

ССМ/СМ обеспечивает сбор, хранение и подготовку информации в формате предписанным обеспечивает пользовательскую политику доступа к программе и управляет системой сбора информации.

ССМ/СМ обеспечивает сбор, хранение и подготовку информации в формате предписанным стандартом для использования уполномоченными органами в делопроизводстве о произведенных разговорах или их содержании. ССМ/СМ также предоставляет систему управления хранилищем и обеспечивает масштабирование системы до уровня предписанного стандартом для одновременного сбора и сохранения информации и последующей ее обработки и анализа.

2. Определение системы управления перехватом (СУП)

2.1. СУП (Система Управления Перехватом) служит в качестве централизованного устройства управления подключенными к ней коммутаторов телекоммуникационной сети и сети передачи данных с активированными интерфейсами перехвата LI ETSI.

2.2. СУП должна поддерживать работу как минимум с интерфейсами и протоколами перехвата следующих основных производителей коммуникационного и коммутационного оборудования: Alcatel Lucent, Nortel/Genband, Cisco, Ericsson, Nokia-Siemens, Huawei, Broadsoft, Juniper, Cisco.

2.3. СУП должен предоставлять механизмы и инструменты для расширения поддержки интерфейсов других производителей телекоммуникационного оборудования.

2.4. СУП служит в качестве централизованного сервера для инициализации и управления перехватами. Пользовательский интерфейс должен поддерживать центральную базу данных всех выданных заданий на перехват. После ввода задания в систему управления, СУП должна провести инициализацию перехвата через систему преобразования в соответствующей промежуточной системе перехвата или напрямую.

2.5. Централизованная СУП обеспечивает единую точку инициализации, администрирования, аудита, контроля безопасности и отчетности для поддержки нескольких вспомогательных подсистем перехвата.

3. Определение системы мониторинга (СМ)

3.1. СМ (Система Мониторинга) – система работающая в телекоммуникационной сети и сети передачи данных и используемая правоохранительными органами для перехвата содержания сообщений с помощью электронных средств связи. Содержание перехваченного сообщения как правило, попадает в одну из двух категорий: Звуковая коммуникация (такие, как звуковой сигнал телефонных разговоров), Незвуковая коммуникация (такие как текстовые сообщениями или содержание передачи по факсу и т.п.), передача данных по Интернет протоколу (электронные сообщения, просмотр ресурсов в интернете и т.д.)

СМ должна обеспечивать следующие основные функции:

3.1.2. Возможность архивирования всех перехваченных сообщений в форме подходящей для обработки и анализа;

3.1.3. Возможность воспроизведения и просмотра по необходимости для анализа, создания стенограммы или перевода, повторного рассмотрения перехваченной коммуникации в установленном промежутке времени;

3.2. Кроме того, СМ должна соответствовать нормам и законам регулирующим юридические процедуры применения перехвата. Со временем, изменения в законодательстве может потребовать изменения и адаптации продукта.

4. Обзор системы управления перехватом (СУП)

СУП работает в телекоммуникационной сети ОА «Казахтелеком» и совместно с Системой Мониторинга (СМ) интегрируется с решениями перехвата различных производителей коммутаторов.

4.1. СУП включает в себя как минимум следующие функции доступные на системе управления:

4.1.2. Пользователь должен иметь механизм, который проверяет символы в поле ввода

4.1. СУП включает в себя как минимум следующие функции доступные на системе управления:

4.1.2. Пользователь должен иметь механизм, который проверяет символы в поле ввода, чтобы обеспечить достоверность информации перед отправкой данных на интерфейс перехвата производителя коммутатора. Это позволит обеспечить введение правильных данных задания на перехват и обеспечит корректную работу интерфейса перехвата. Должен быть предусмотрен механизм автоматического блокирования отправки некорректных идентификаторов абонента.

4.1.3. Пользователь должен иметь функцию управления синхронизацией со всеми подключенными интерфейсами перехвата для каждого типа телекоммуникационного оборудования вовлеченного в процесс перехвата.

4.1.4. Пользователь должен иметь индикатор уведомления о состоянии выполнения каждого конкретного задания на перехват. Индикатор состояния должен отображать информацию о правильности выбранной цели или статус соединения с коммутатором.

4.1.5. Все перехваты должны проходить непрерывную проверку на соответствие статусу в период действия перехвата, в частности включая санкционирование выполнения перехвата и его положительную инициализацию в телекоммуникационной сети.

4.1.6. Пользователь должен иметь возможность проверки отдельного перехвата и вручную инициировать повторную инициализацию или изменение деталей перехвата в случае появления ошибки инициализации. Все модификации перехвата должны быть просматриваемыми и должны фиксироваться в журнале изменений под соответствующим идентификатором пользователя.

4.1.7. Во время проверки целостности, пользователь должен иметь возможность автоматического исправления ошибки. Факт о данной ошибке должен фиксироваться в журнале и ясно отображаться в интерфейсе приложения.

4.1.8. Все активные, а в некоторых случаях и неактивные задания на перехват, должны быть доступны для просмотра в отчете. Если максимальное количество записей превышено, то информация должна быть архив доступный с экрана инициализации перехватов. Индикатор должен информировать пользователя, если 90% и более свободного пространства для хранения перехватов занято.

4.1.9. Пользователь должен иметь конфигурируемый механизм повтора инициализации перехвата.

4.1.10. Пользователь должен иметь постоянную информацию о количестве интерфейсов перехвата подключенных к СУП.

4.2. СУП обеспечивает настройки и расширения интерфейса, используемого для неограниченного представления отчетности, начиная с отчетов о перехватах и заканчивая отчетами аудита. Кроме того, доступ к отчетам должен ограничиваться привилегиями пользователя и, если необходимо, может быть интегрирован с любым сторонним продуктом.

4.3. СУП должна вести журнал о производительности системы, операциях и активности обмена информацией. Отчет или соответствующий опрос данных должен быть доступен администратору в любое время.

4.4. СУП должна иметь механизм поддерживающий работоспособность системы без вмешательства человека, другими словами, автоматический механизм восстановления рабочего состояния. Данная система должна проверять работоспособность системы и предоставлять механизм уведомления администратора о любых ошибках. Серьезность ошибки и способ уведомления должны настраиваться соответственно требованиям администратора.

4.5. Постоянно обновляемый статус задания на перехват должен передаваться на систему мониторинга статуса перехвата. Т.е., не только оповещение о произошедшей ошибке при обработке перехвата, а постоянное обновление статуса (активный, ошибка, неполадка, неактивный, …) перехвата в промежутке времени действия самого перехвата в системе.

обработке перехвата, а постоянное обновление статуса (активный, ошибка, неполадка, неактивный, …) перехвата в промежутке времени действия самого перехвата в системе.

4.6. СУП обеспечивает единую архитектуру для сетей с классической и пакетной коммутацией. Сторонние элементы сети должны иметь возможность интеграции с системой управления.

4.7. СУП должна вести журнал о всех действиях и уведомлениях вовлеченных сетевых элементов в период действия перехвата - обновление программного обеспечения, перезапуск системы, любые преднамеренные или случайные помехи связанные с активным перехватом и др.

4.8. СУП должна иметь возможность расширения функциональности как, например, добавление промежуточных систем или увеличение масштаба и скорости работы системы, сохранять свою работоспособность при изменениях или росте коммуникационной сети.

4.9. СУП должна контролировать состояние подключения каждой промежуточной системы оператора связи и при необходимости, контролировать состояние мобильных коммутаторов или других элементов сети.

4.10. СУП должна иметь, как минимум, следующие дополнительные возможности:

4.10.1. Механизм обеспечения запуска и остановки перехвата должен работать только в течении периода действия задания на перехват, действие данного периода должно автоматически обрабатываться системой. Любые изменения или действия по инициализации перехвата должны легко просматриваться в журнале активности или отчете по истории данного перехвата.

4.10.2. В целях обеспечения целостности перехвата в любое время в течение периода его действия, система должна иметь механизм постоянного контроля срока действия перехвата. Данный активный механизм должен работать в автоматическом или ручном режиме.

4.10.3. В некоторых случаях на коммутаторах телефонной сети придется инициализировать перехват лишь с датой начала перехвата и без даты его окончания. Данная опция должна поддерживаться системой инициализации.

4.11. Интерфейс пользователя СУП должен быть приложением, которое может работать в обычном интернет-браузере (т.е. иметь web-интерфейс).

4.12. Архитектура приложения СУП должна разделять бизнес- и презентационную логику. Бизнес-логика должна выполняться на сервере, а презентационная логика отображаться в тонком клиенте, таком как интернет-браузер.

4.13. СУП должна иметь механизм для периодической проверки целостности сетевых элементов и по необходимости корректировать ошибки.

4.14. СУП должна поддерживать, как минимум, следующие механизмы распределения и регистрации перехвата на коммутаторах:

4.14.1. Параллельное – перехват распределяется между коммутаторами параллельно;

4.14.2. Последовательное – перехват распределяется между коммутаторами в определенной последовательности.

4.15. Приложение СУП должно предоставлять обзорную страницу статуса всех коммутаторов, маршрутизаторов и перехватов в телекоммуникационной сети.

4.16. Дизайн приложения должен поддерживать «Мастера настройки», при котором ввод большого количества данных разбивается на отдельные диалоги.

4.17. СУП должна поддерживать механизм синхронизации между базой данных приложения и выбранным коммутатором/маршрутизатором. Синхронизации подлежат данные о коммутаторе/маршрутизаторе, его конфигурации и всех перехватов, зарегистрированных на данном коммутаторе или маршрутизаторе.

4.18. СУП должна предоставлять возможность работы с шаблонами для различных типов на данном коммутаторе или маршрутизаторе.

4.18. СУП должна предоставлять возможность работы с шаблонами для различных типов перехвата, определяя в шаблоне, как минимум следующие детали: описание и определение полей, ограничение полей, менеджер перехвата, исключаемые коммутаторы или маршрутизаторы.

4.19. СУП должна предоставлять возможность работы с шаблонами для различных типов выдаваемой информации, определяющей, как минимум следующие поля: описание и определение полей выдачи.

4.20. СУП должна вести журнал активности с возможностью аудита действий всех пользователей приложения. Записи должны индексироваться в журнале аудита (с функцией поиска по журналу).

4.21. СУП должна поддерживать расширенную функциональность по удаленному оповещению администратора, используя электронную почту. Настройка оповещения должна поддерживаться для всех типов записей в журнале аудита.

4.22. СУП должна поддерживать работу с шаблонами для создания различных типов отчетов.

4.23. СУП должна поддерживать архивирование данных о перехвате, журналов аудита, конфигурационных файлов и шаблонов. Архив должен предоставлять возможность поиска по архиву и функцию восстановления информации из архива.

4.24. СУП должна поддерживать автоматическое архивирование данных о перехвате из внутреннего архива на внешние носители после определенного периода времени.

5. Обзор системы мониторинга (СМ)

5.1. Установленная система должна соответствовать определению системы (см. подраздел 3).

5.2. СМ должна быть выстроена вокруг централизованного ядра, на котором должны собираться, сохраняться и обрабатываться все факты. Все данные, содержание и результаты обработки собранных данных в сети должны храниться и быть доступными в централизованном месте.

5.3. Система должна быть спроектирована для постоянной работы без перерыва, в течении 24 часов в сутки, 365 дней в году. Система должна быть построена гибко, с возможностью достаточного резервирования для поддержания рабочего режима в течение срока работы системы.

5.4. Воспроизведение, стенограмма, перевод, просмотр, формирование отчетов и анализ должны выполняться на рабочих станциях по обработке звуковой и пакетной информации. Все отдельные функции должны быть полностью исполняемыми в любой момент времени для любой цели независимо от того, в какой части телекоммуникационной сети производился мониторинг объекта.

5.5. СМ собирает и декодирует звуковую информацию, пакетную информацию и другую сигнальную информацию и предоставляет автоматизированный, постоянно работающий механизм записи любого перехваченного звукового и пакетного контента. Разработчик должен обеспечить возможность дальнейшего расширения системы расшифровки, анализа и обработки стандартных протоколов для аудио, не-аудио и пакетных потоков данных.

5.6. СМ должна поддерживать конфигурацию для достаточного дублирования и автоматического резервирования каждой критической компоненты с целью предотвращения или сведения к минимуму времени простоя из-за отказов. Архивирование должно дублироваться с несколькими контроллерами. Аудио и данные должны находиться в нескольких локациях до архивирования и до удаления из системы после завершения работы по анализу перехвата. Система должна иметь возможность быстрого восстановления после неисправности. Все данные должны дублироваться на постоянной основе на внешние устройства хранения данных, такие как NAS, съемные жесткие диски или в сети хранения данных (SAN) и т.д.

5.7. СМ должна обладать гарантиями защиты собранных данных и результатов их обработки постоянной основе на внешние устройства хранения данных, такие как NAS, съемные жесткие диски или в сети хранения данных (SAN) и т.д.

5.7. СМ должна обладать гарантиями защиты собранных данных и результатов их обработки от потери во время событий, таких, как например, перебои в подаче электроэнергии.

5.8. СМ предусматривает поддержку всех форм фиксированной телефонной связи и должна обеспечивать прием всех видов телефонной связи и форматов передачи, включая аналоговые, ISDN PRI, ISDN BRI, SS7 ISUP. Передача данных предусматривает поддержку Интернет Протокола (IP).

5.9. Система сбора и мониторинга должна обеспечивать пользователя возможностью быстрого получения ранее собранного содержания перехвата для проверки, возможной подготовки стенограммы или перевода, и сохранения результата обработки.

5.10. Система должна обеспечивать пользователя различными инструментами для управления, выбора и просмотра собранной информации. Для обработки записанной сессии система должна предоставлять возможность выбирать скорость и направление проигрывания записи или ее частей.

5.11. Система должна обеспечивать возможность выбора аудио-фрагмента для проигрывания его циклически, в “петле”.

5.12. Система должна обеспечивать пользователя функцией перемотки “вперед/назад” и перехода к началу или концу звуковой дорожки.

5.13. При воспроизведении “стерео”-записи, пользователь должен иметь возможность заглушать выбранную дорожку.

5.14. Система должна быть оснащена как минимум функциями графического эквалайзера, возможностью удаления шума и смены тона без изменения темпа записи.

5.15. Во время работы в режиме воспроизведения, система должна предоставлять пользователю возможность присвоения сопровождающей отметки аудио-контенту. Система должна также предоставлять возможность удалять отметки. Система должна иметь возможность присваивать метки только части аудио-контента.

5.16. Как минимум, система должна обеспечивать обработчиков следующими возможностями в нахождении одной или нескольких сессий:

5.16.1. Система должна позволять обработчикам выполнять поиск по дате/датам и времени.

5.16.2. Система должна позволять обработчикам выполнять поиск по полям классификации, маркировки, статуса и другим атрибутам сессии.

5.17. Система должна обеспечивать обработчиков окном для автоматического вывода перечня самых последних сессий за период времени задаваемый пользователем.

5.18. Система должна иметь поле для статуса каждой индивидуальной сессии, которое заполняется системой автоматически.

5.19. Система должна иметь возможность открытия несколько сессий для одновременного воспроизведения. При этом пользователь должен иметь возможность заглушать выбранные сессии.

5.20. В режиме воспроизведения на экране должно отображаться визуальное представление звуковой дорожки ранее перехваченной системой.

5.21. В режиме воспроизведения система должна позволять пользователям делать индивидуальные настройки.

6. Система безопасности и шифрование

6.1. Система Мониторинга (СМ) и Система Управления Перехватом (СУП) должны иметь расширенные возможности для защиты и сохранения целостности собранных данных и результатов их обработки.

6.2. Обе системы должны быть оборудованы защитными механизмами для разрешения результатов их обработки.

6.2. Обе системы должны быть оборудованы защитными механизмами для разрешения доступа к системе только авторизированным пользователям и защищать системы и собранные данные от попыток внешних атак на систему.

6.3. Пользователи обеих систем независимо от роли (например обработчики, надзорщики администраторы, системные администраторы) должны получать доступ к системе только при наличии уникального пользовательского имени и связанного с ним пароля, чтобы предотвратить несанкционированный доступ. Учетные записи пользователей должны иметь минимальную длину пароля согласно установленным правилам политики безопасности. Программное обеспечение не должно интерактивно запрашивать авторизацию для старта программы, т.е. приложение должно пройти авторизацию через операционную систему с использованием системы единого входа с установленным сервисом LDAP или похожим.

6.4. Система должна предоставлять для каждой учетной записи пользователя расширенный выбор прав входа, доступа к функционалу и данным, хранимым в приложении. Система должна по умолчанию отказывать в доступе к системным ресурсам приложениям, данным, подсистемам, аналитике и пользовательским данным при отсутствии соответствующих прав у пользователя.

6.5. Если необходимы авторизационные коды для работы любой функции в рамках системы, производитель должен предоставить таковые владельцу системы.

6.6. Система должна поддерживать учетные записи пользователей, групп и политики безопасности. Пользователи объединяются в группы, а группам присваиваются определенные политики безопасности, состоящие из правил доступа к ресурсам системы.

7. Масштабируемость и конфигурация систем СУП и СМ

7.1. В целях последующего расширения работоспособности Системы Мониторинга, система должна быть надежной и масштабируемой, чтобы иметь возможность быстрого расширения общего количества перехватов. На момент первоначальной покупки и установки, система мониторинга должна быть в состоянии поддерживать, как минимум, сто (100) одновременных перехватов.

7.2. Для целей последующего расширения работоспособности СУП, система должна быть надежной и масштабируемой, чтобы иметь возможность расширить быстрого расширения общего количества перехватов. На момент первоначальной покупки и установки, система перехвата должна быть в состоянии поддерживать, как минимум, сто (100) перехватов одновременно.

8. Отчеты

8.1. Система должна предоставлять широкий спектр возможностей для составления, конфигурации, адаптации и изменения отчетов. Система должна поддерживать экспорт данных отчетов в статистические и аналитические программы.

8.2. При разработке статистических и аналитических отчетов, все поля баз данных должны быть доступными для выбора, поиска, сортировки, и также других общих функций составления отчетности.

8.3. Построение отчетов должно поддерживаться на каждом удаленном узле системы.

8.4. Система должна быть оборудована общим хранилищем отчетов для хранения часто используемых отчетов и для быстрого доступа пользователей системы.

8.5. Формат и содержание отчета должны настраиваться системным администратором.

8.6. Система должна обеспечивать сохранение отчетов на широком спектре средств хранения, например CD-R, CD-RW, DVD-R, DVD-RW, BD-R, BD-RE и устройствах, подключенных к системе через USB.

8.7. Пользователи системы должны иметь возможность сохранения адаптированных версий доклада для своих нужд.

подключенных к системе через USB.

8.7. Пользователи системы должны иметь возможность сохранения адаптированных версий доклада для своих нужд.

8.8. Система должна поддерживать шаблоны для генерируемых отчетов.

8.9. Система должна учитывать права пользователей и групп при показе, составлении или сохранении отчетов.

8.10. Как минимум следующие отчеты должны предоставляться системой: список активных перехватов, количество перехватов различных подразделений, количество перехватов за определенный период времени, ошибки в сети за определенный период работы системы, синхронизация и целостность элементов сети.

9. Системное администрирование

9.1. Система должна предоставлять различные инструменты системного администрирования для помощи в управлении системой.

9.2. Система должна обеспечивать системных администраторов простыми средствами управления для проверки журналов ошибок, статуса активных перехватов, статуса пользователей, сроков действия заданий на перехват и другой информации, необходимой для организации нормальной работы системы. Система должна обеспечивать системных администраторов средствами для простой проверки состояния всех компонент системы: подсистем, сетевых ресурсов, аппаратных средств и т.д. Сообщения о неполадках направляются непосредственно к системному администратору по электронной почте.

9.3. Система должна обеспечивать системных администраторов средствами создания учетных записей пользователей для администраторов, операторов, надзорщиков и других системных администраторов, и установления степени доступа и привилегий по возможности детально.

9.4. Система должна обеспечивать системных администраторов средствами для настройки перехвата заданного абонента и обеспечивать автоматическое закрытие задания по дате и времени.

9.5. Системные администраторы должны получать немедленное уведомление или подтверждение от системы при изменении статуса перехвата заданного абонента или потере соединения.

9.6. Системные администраторы должны получать немедленное уведомление или подтверждение от системы при изменении статуса сетевого соединения основных компонентов системы или при потере связи.

9.7. Система должна обеспечивать системных администраторов средствами проверки состояние емкости хранилища системы. Кроме того, система должна периодически отправлять автоматические уведомления системным администраторам при достижении хранилищем порога доступной емкости настраиваемой системным администратором.

9.8. Система должна обеспечивать системных администраторов автоматическим оповещением о каких-либо перерывах в нормальной работе процесса архивирования.

9.9. Система должна обеспечивать системных администраторов инструментами удаленного администрирования систем после входа в саму систему. Системный администратор должен иметь возможность администрирования и мониторинга всех удаленных объектов.

9.10. Система должна предоставлять диалоги типа "Мастера настройки" для облегчения выполнения повторяющихся процессов, таких как создание и удаление пользовательских учетных записей, удаление домашней папки, пользовательского профиля, создания и удаление задания на перехват, обновление или расширение задания, проверке правильной работы архивирования, доработке и экспорта данных, обеспечения процесса обслуживания и т.д.

9.11. Системным администраторам должен быть обеспечен полным доступом ко всей системе с единственным исключением доступа к местам, которые должны быть полностью обеспечения процесса обслуживания и т.д.

9.11. Системным администраторам должен быть обеспечен полным доступом ко всей системе с единственным исключением доступа к местам, которые должны быть полностью защищены, например записям для целей аудита.

10. Аудит системы мониторинга

10.1. Система мониторинга должна быть оснащена широким спектром гарантий безопасности, чтобы обеспечить широкие возможности аудита деятельности пользователей.

10.2. Система должна иметь надежный механизм аудита и отслеживания входа в систему для всех учетных записей простых и административных пользователей. Детали аудита должны представлять подробную информацию о деятельности пользователя в системе, сделанных им изменениях и данных которые были просмотрены. Система аудита должна отслеживать инициированные пользователем события, которые должны включать, как минимум: создание, экспорт, сохранение или удаление любого документа или файла, просмотр любого документа или файла; воспроизведение сессии, вход в систему (время / дата), выход из системы (время / дата), изменение в классификации и статуса сессий.

10.3. Системный журнал должен предоставлять механизм поиска, обеспечивая фильтрацию результатов поиска, как минимум, по имени учетной записи пользователя и просмотренных или измененных данных за определенный период времени, (т.е., что делал пользователь А в системе в определенный период времени, или кто из пользователей инициировал определенное событие в системе за определенный период времени и т.д.)

10.4. Система должна быть способна экспортировать данные аудита в доступных форматах на носители информации для целей архивирования.

10.5. Журнал событий должен оставаться неизменным и обнаруживать любые попытки его изменения или фальсификации. Проверка попыток изменения журнала должна проверяться только специально уполномоченным персоналом.

11. Стороннее программное обеспечение

11.1. Подрядчик принимает на себя полную ответственность за совместимость, функциональность, производительность и обновление программного обеспечения сторонних производителей, включенных в его систему.

11.2. Система мониторинга и система управления перехватом должны работать на операционных системах, которые в данный момент поддерживаются производителем данных систем.

11.3. Подрядчик должен предложить любые возможности функционального расширения системы, такие как распознавание голоса, распознавание речи и другие функции для будущего расширения.

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К СИСТЕМЕ ТЕХНИЧЕСКОЙ ЭКСПЛУАТАЦИИ ПУ СОРМ (по части АО «Казахтелеком»)

1. ОБЩЕЕ ОПИСАНИЕ ТЕХНИЧЕСКОГО ТРЕБОВАНИЯ

Настоящее техническое задание распространяются на комплекс оборудования, предназначенного для обеспечения проведения оперативно-розыскных мероприятии (далее ОРМ) на сети АО «Казахтелеком» и получения информации уполномоченными органами по проведению ОРМ в отношении абонентов коммутационных систем и систем ПД подключаемых к данному комплексу.

1.1. Общие технические требования

1.1.2. Технические параметры, не упомянутые в технических требованиях и в данном техническом задании, должны соответствовать рекомендациям ITU-T, ETSI, ОГСТФС, а

1.1. Общие технические требования

1.1.2. Технические параметры, не упомянутые в технических требованиях и в данном техническом задании, должны соответствовать рекомендациям ITU-T, ETSI, ОГСТФС, а также должны быть адаптированы к существующей национальной сети телекоммуникаций Республики Казахстан;

1.1.3. Предлагаемое решение должно иметь распределенную архитектуру с централизованным управлением;

1.1.4. В предложениях должны быть указаны отдельные расценки по оборудованию (включая все виды плат и элементы соединений), монтажу и инженерным работам;

1.1.5. Должна быть обеспечена возможность модульного наращивания емкости и производительности оборудования без остановки системы;

1.1.6. Все поставляемое оборудование должно быть произведено в соответствии с международным сертификатом качества ISO 9001;

1.1.7. Участник конкурса должен представить информацию о наличии Сертификатов соответствия на все поставляемое оборудование, зарегистрированных в реестре государственной системы сертификации Республики Казахстан. В случае отсутствия Сертификатов фирма-победитель должна представить их до подписания акта окончательной приемки оборудования в эксплуатацию. Все расходы по сертификации поставщики берут на себя;

1.1.8. Оборудование поставщика должно быть адаптировано для взаимодействия с оборудованием коммутационных систем АО «Казахтелеком»;

1.1.9. Поставщик при дальнейшей эксплуатации должен гарантировать достижение полной совместимости всех видов поставляемого оборудования с оборудованием других поставщиков, при условии использования открытых протоколов и интерфейсов взаимодействия.

1.1.10. Система легального перехвата должна обеспечивать централизованную форму работы и обеспечивать активную форму перехвата в телекоммуникационной сети АО «Казахтелеком», подключаясь напрямую к телекоммуникационным станциям (предпочтительно) или через конверторы управляя функциями перехвата через интерфейсные карты правомерного перехвата производителей телекоммуникационного оборудования.

1.1.11. Оборудование ПУ СОРМ, должен принимать интерфейсы от коммутационных систем с возможными небольшими вариациями со следующими стандартизованными интерфейсами взаимодействия:

1.1.11.1. **ETSI TS 201 671 v3.1.1.**

1.1.11.2. **CALEA-STD-025B**

1.1.11.3. **Казахстанский интерфейс СОРМ в соответствии с ТУ 640 РК 00032098 ДКНБ-001-2006**

1.1.11.4. **Российский интерфейс СОРМ в соответствии Приказу № 70 от 20.04.99г. Госкомсвязи России**

1.1.11.5. **ETSI TS 102 232 (все версии)**

1.1. Требования по надежности

1.1.2. Коэффициент готовности оборудования должен быть не менее 0,9999954;

1.1.3. Все основные узлы оборудования должны быть зарезервированы по схеме 1+1 либо N+1;

1.1.4. Изменение конфигурации и любых настроек системы должно производиться без прерывания сервисов;

1.2. Должна быть реализована возможность возврата к предыдущей конфигурации программного обеспечения

1.3. Требования по масштабируемости

1.3.1. Оборудование должно иметь модульную архитектуру. Расширение системы должно производиться при помощи простого подключения дополнительных модулей для увеличения производительности только той функциональной части системы, которая подлежит расширению;

производиться при помощи простого подключения дополнительных модулей для увеличения производительности только той функциональной части системы, которая подлежит расширению;

1.3.2 Модульная архитектура не должна накладывать ограничений на дальнейшее расширение оборудования в будущем;

1.4. Требования к резервированию и восстановлению системы

Оборудование должно обеспечивать:

1.4.1 Резервирование всех плат, влияющих на прохождение трафика в каждом отдельно взятом устройстве. Переключение на резервную плату должно производиться без прерывания существующего трафика;

1.4.2 «Горячую» замену плат без снятия питающего напряжения и без прерывания существующего трафика;

1.4.3 Резервирование всех интерфейсных соединений с СТОП и с пакетной сетью в каждом отдельно взятом устройстве. Переключение на резервный интерфейс должно производиться без прерывания существующего трафика;

1.4.4 Подключение к двум независимым питающим сетям. Переключение на резервный источник питания должно производиться без прерывания существующего трафика;

1.4.5 Обновление, модификацию и перезагрузку программного обеспечения для каждого отдельно взятого устройства и для всей системы в целом, без прерывания существующего трафика.

1.5. Требования к системе технической эксплуатации Центра мониторинга (ЦМ) (сторона операторов АО «Казахтелеком»)

1.5.1 система технической эксплуатации должна обеспечивать интеграцию с существующей в АО "Казахтелеком" Системой Управления Сетями Телекоммуникаций посредством передачи потоков аварийных и информационных сообщений с использованием одного из интерфейсов: SNMP, RS-232 / SSH;

1.5.2 Система экплуатации должна обеспечивать интеграцию с существующей в АО "Казахтелеком" Системой ASAP с использованием одного из интерфейсов: SNMP, WebAPI и.т.д.

1.6.3.1. Все принимаемые сообщения должны содержать:

a) Физический и/или логический адрес оборудования, на котором произошла неисправность;

b) Идентификатор или внутренний номер репортажа;

c) Тип репортажа (проблема/разрешение/информация);

d) Категория срочности устранения неисправности (critical/minor/major, и т.п.);

e) Дата и время возникновения неисправности;

f) Другая дополнительная информация, которую технический персонал может использовать для локализации и устранения неисправности оборудования.

1.6.3.2. Эксплуатационная документация на поставляемое оборудование должна содержать перечни аварийных и информационных сообщений, включающие в себя описание формата сообщений, идентификаторы (уникальные ключевые слова) сообщений, и их описание на английском и русском языках.

1.5.3 Требования к интерфейсу SNMP***:***

1.6.4.1. Сообщения должны передаваться в следующих форматах:

a) SNMP V1 traps, V2c traps, and V3 traps;

b) SNMP V2c and V3 informs.

1.6.4.2. Эксплуатационная документация на поставляемое оборудование должна содержать:

a) Версию используемого протокола;

b) Набор всех необходимых MIB файлов, соответствующий оборудованию, включая все вышестоящие MIB;

c) Описание Trap’ов и Inform’ов;

d) Описание и формат значений передаваемых OID’ов.

1.5.4 Требования к интерфейсу RS-232 / Telnet/SSH***:***

d) Описание и формат значений передаваемых OID’ов.

1.5.4. Требования к интерфейсу RS-232 / Telnet/SSH***:***

1.6.5.1. Сообщения должны передаваться в формате ASCII или CP1251;

1.6.5.2. Выводить сообщения без запроса (без выполнения команд);

1.6.5.3. Сообщение должно заканчиваться фиксированным символом или их набором информируя о логическом завершении сообщения.

1.5.5. Интеграцию с различными системами BSS \ OSS посредством web-сервисов и прочих решений концепции сервис ориентированной архитектуры (SOA).

1.5.6. Синхронизацию и автоматическую загрузку следующих данных о конфигурации во внешние системы инвентаризации ресурсов сети:

1.6.7.1. данных об объектах сети (наименование, тип, инвентарный номер, серийный номер…);

1.6.7.2. данных о местонахождении оборудования;

1.6.7.3. данных о конфигурации портов;

1.6.7.4. данных о физическом соединении устройств, о логических каналах;

1.6.7.5. данных об услугах и т.д.

1.5.7. Для осуществления контроля качества (QOS) на вновь вводимых сегментах Сети Передачи Данных все активное сетевое оборудование, которое будет участвовать в определений границ доверия на сети (маршрутизаторы, коммутаторы Метро сетей и оборудования Магистральных сетей IP/MPLS ДКП), должно быть дополнительно укомплектовано маршрутизатором, содержащим компонент Service Assurance Agent (SAAsr с типом интерфейса Fast Ethernet), для проведения измерений.

1.5.8. Система эксплуатации должна:

1.5.8.1 Представлять собой программное обеспечение, способное управлять всем комплексом оборудования, на единой аппаратной платформе, через единый интерфейс технической эксплуатации (ИТЭ, ИЭ);;
1.5.8.2 Предоставлять графическую систему конфигурации, управления и мониторинга;
1.5.8.3 Предоставлять возможность доступа для нескольких операторов;
1.5.8.4 Обеспечивать защиту от несанкционированного доступа;

1.5.9 Должно быть обеспечено выполнение следующих функций:

1.5.9.1 Управление доступом к системе;
1.5.9.2 Управление авариями;
1.5.9.3 Управление конфигурацией;
1.5.9.4 Другие необходимые функции управления и мониторинга.

1.5.10 ИЭ должен в графическом виде отображать весь комплекс оборудования ЦМ и каналы связи как внутри ЦМ, так и каналы связи подключения ЦМ к оборудованию сети связи. При этом на данной схеме должен отображаться актуальный статус указанного оборудования и каналов связи; ИЭ должен иметь средства настройки, конфигурирования и тестирования оборудования ЦМ, средства отладки и устранения неисправностей.

1.5.11 Все действия по конфигурированию, наладке, устранению неисправностей, обновления ПО должны осуществляться только через ИЭ.

1.5.12 Функции эксплуатации и технического обслуживания оборудования должны выполняться как в автоматическом режиме, так и по запросу оператора;

1.5.13 Система технической эксплуатации должна предоставлять возможность определить разные уровни доступа для разных операторов;

1.5.14 Все действия оператора через ИЭ должны сохраняться в эксплуатационном журнале, защищенном от редактирования.

1.5.15 ИЭ должен предоставлять оператору, имеющему соответствующий допуск (права), механизм просмотра эксплуатационного журнала.

1.5.16 Система эксплуатации должна обеспечивать защиту от несанкционированного доступа, как на программном, так и на аппаратном уровне. Поставщик должен описать механизм применяемой защиты;

1.5.10 Система эксплуатации должна обеспечивать защиту от несанкционированного доступа, как на программном, так и на аппаратном уровне. Поставщик должен описать механизм применяемой защиты;

1.6. Требования по безопасности

Требования по доступу к системе технической эксплуатации:

1.6.1 Доступ к системе должен быть защищен паролями;

1.6.2 Через интерфейс эксплуатации должен быть исключен доступ к функционалу перехвата.

1.6.3 Администратор должен иметь интуитивно понятный механизм настройки системы безопасности;

1.6.4 Несколько неудачных попыток доступа должны приводить к завершению сессии и немедленному сообщению об угрозе в системе безопасности;

1.6.5 Система управления должна завершить текущий сеанс по истечении заранее определенного Администратором периода неактивности оператора.

Требования по безопасности сетевых приложений:

1.6.6 Неиспользуемые порты протоколов должны быть закрыты;

Требования по безопасности протоколов и соединений:

1.6.7 Должна быть обеспечена безопасная система доступа для санкционированных пользователей и безопасная регистрация элементов сети;

Требования по безопасности систем управления и техобслуживания:

1.6.8 Доступ к системам управления и техобслуживания должны иметь только зарегистрированные пользователи, обладающие разными уровнями административного управления и соответствующими ограничениями;

1.6.9 Все попытки несанкционированного доступа должны блокироваться и протоколироваться;

1.6.10 Для безопасного доступа к системе управления необходимо использовать протокол IPSec.

1.7. Требования к монтажу

1.7.1 Оборудование системы может быть установлено внутри помещения в стандартной стойке или в закрытом напольном шкафу;

1.8. Требования к оборудованию цифровых кроссов

1.8.1 Стойки DDF должны быть обеспечены необходимым материалом для укладки и крепления как для 2Мб/с кабелей, так и для соединительных кабелей между рамками;

1.8.2 Должны быть поставлены кроссовые кабели из расчета необходимого количества рамок кросса. Длина кабелей, предполагаемых к задействованию в последующем, должна позволять осуществлять соединение между двумя наиболее удаленными рамками кросса;

1.8.3 Аппаратура должна быть укомплектована ответными частями разъемов для подключения внешних кабелей к портам;

1.8.4 DDF должен обеспечивать удобное параллельное подключение кроссировок на отдельных разъемах без нарушения основных соединений для подключения систем мониторинга и другого оборудования.

1.9. Требования к системе энергоснабжения

1.9.1 Номинальное напряжение питания оборудования должно составлять - 48В. Допустимые пределы питания должны составлять - 38В ÷ - 72В;

1.9.2 Каждый статив оборудования должен быть снабжен индивидуальными устройствами защиты для каждого комплекта оборудования, устанавливаемой на шкафу, а также общестоечными клеммами рабочего и защитного заземления;

1.9.3 Для оборудования, требующего безобрывного переменного напряжения 220 В, должны быть поставлены конверторы DC/AC 48/220 В соответствующей мощности, с учётом резерва не менее N+1, а также комплекты розеток для подключения оборудования;

1.10 Аварийная сигнализация

1.10.1 Оборудование должно иметь устройства технического обслуживания, измерения, контроля и индикации состояния системы во время работы и при поиске неисправностей и обеспечивать взаимодействие с сетевой системой обслуживания и местным терминалом;

1.10.1 Оборудование должно иметь устройства технического обслуживания, измерения, контроля и индикации состояния системы во время работы и при поиске неисправностей и обеспечивать взаимодействие с сетевой системой обслуживания и местным терминалом;

1.10.2 Должны быть обеспечены при выводе на устройства оптической и звуковой сигнализации следующие виды аварийных сигналов:

- 1.10.2.1 Срочный;
- 1.10.2.2 Несрочный.

1.10.3 Аварийная сигнализация должна быть на блоках и комплектах аппаратуры. Должна иметься возможность трансляции аварийных сигналов в стойку;

1.11 Требования к условиям окружающей среды

1.11.1 Диапазон рабочей температуры - от +5°C до +50°C;
1.11.2 Температура хранения: -40°C до +70°C;
1.11.3 Относительная влажность не более 80%;
1.11.4 Удар и вибрация - согласно ETS 300 019-2-4;
1.11.5 Транспортировка - согласно ETS 300 019-2-2 Класс 2.2;
1.11.6 Электробезопасность должна соответствовать стандарту ETS 300 386-1;
1.11.7 Безопасность должна соответствовать стандартам 69050 (IEC 950);
1.11.8 Участник конкурса должен приложить спецификацию заземления.

1.12 Техническая поддержка и ремонт

1.12.1 Поставщик должен обеспечивать поставку ЗИП после окончания гарантийного срока не менее 10 лет. Цены на ЗИП не должны повышаться не менее 7 лет после заключения договора;

1.12.2 Поставщик должен предоставить АО «Казахтелеком» услуги по технической поддержке на весь период эксплуатации оборудования. Необходимо предложить различные варианты услуг по технической поддержке, которые будут предоставляться по отдельному сервисному контракту;

1.12.3 Техническая поддержка должна включать в себя поставку и ремонт оборудования, сопровождение программного обеспечения (устранение ошибок, загрузка новых версий ПО и др.), устранение аварий;

1.12.4 Услуги по технической поддержке классифицированы в зависимости от их степени:

- 1.12.4.1 Полная или частичная потеря функции перехвата (ПРОБЛЕМА ПЕРВОЙ СТЕПЕНИ);
- 1.12.4.2 Опасность потери функции перехвата (ПРОБЛЕМА ВТОРОЙ СТЕПЕНИ);
- 1.12.4.3 Проблемы, не влияющие на функции перехвата (ПРОБЛЕМА ТРЕТЬЕЙ СТЕПЕНИ).

1.12.5 Нормативное время на устранение проблем:

- 1.12.5.1 Проблема первой степени – 4 часа;
- 1.12.5.2 Проблема второй степени – 48 часов;
- 1.12.5.3 Проблема третьей степени – 1 месяц.

1.12.6 Неисправное оборудование должно быть восстановлено и возвращено поставщиком в течение 45 (рабочих) дней со дня отправки на ремонт.

1.12.7 Стоимость ремонта неисправного оборудования не должна превышать 30% от стоимости данного оборудования указанную спицификациях к поставке.

1.12.8 ЗИП должен обеспечивать бесперебойную работу оборудования (исключение ПРОБЛЕМ ПЕРВОЙ И ВТОРОЙ степеней);

1.12.9 При превышении сроков ремонта оборудования Поставщик уплачивает Покупателю пеню в размере 0,1 % от суммы ремонта данного оборудования за каждый день просрочки, но не более 5% от суммы неисполненных обязательств;

1.12.10 В случае если в договоре затраты по ремонту входят в стоимость технической поддержки, то Поставщикь при превышении сроков ремонта оборудования уплачивает Заказчику пеню в размере 0,05 % от суммы неисполненного обязательства за каждый день просрочки, но не более 5% от договорной стоимости услуг по филиалу (филиалам).

1.13 ГАРАНТИЙНЫЙ ПЕРИОД

1.13.1 Гарантийный период на все оборудование, включая оборудование других производителей,

1.13 ГАРАНТИЙНЫЙ ПЕРИОД

1.13.1 Гарантийный период на все оборудование, включая оборудование других производителей, поставляемое в комплекте должен составлять не менее 12 месяцев;

1.13.2 Гарантийный период начинается с момента подписания Акта окончательной приемки оборудования;

1.13.3 Услуги по технической поддержке в гарантийный период должны входить в стоимость контракта. Поставщик в течение гарантийного периода должен обеспечить ремонт оборудования, сопровождение программного обеспечения (устранение ошибок, загрузка новых версий ПО и др.), устранение аварий.

1.13.4 В случае замены вышедшего из строя блока во время гарантийного периода, срок гарантийного периода на данный блок продлевается с момента получения блока на склад покупателя;

1.13.5 Техническая поддержка в гарантийный период должна включать в себя поставку и ремонт оборудования, сопровождение программного обеспечения (устранение ошибок, загрузка новых версий ПО и др.), устранение аварий;

1.13.6 Услуги по технической поддержке в гарантийный период должны быть классифицированы в зависимости от их степени:

- 1.13.6.1 Полная или частичная потеря трафика (ПРОБЛЕМА ПЕРВОЙ СТЕПЕНИ);
- 1.13.6.2 Опасность потери трафика (ПРОБЛЕМА ВТОРОЙ СТЕПЕНИ);
- 1.13.6.3 Проблемы, не влияющие на трафик (ПРОБЛЕМА ТРЕТЬЕЙ СТЕПЕНИ).

1.13.7 Нормативное время на устранение проблем в гарантийный период:

- 1.13.7.1 Проблема первой степени – 4 часа;
- 1.13.7.2 Проблема второй степени – 48 часов;
- 1.13.7.3 Проблема третьей степени – 1 месяц.

1.13.8 Неисправное оборудование должно быть восстановлено и возвращено Поставщиком в течение 45 рабочих дней со дня отправки на ремонт или заменено на аналогичное;

- 1.13.8.1 При превышение сроков ремонта оборудования в гарантийный период Исполнитель уплачивает Заказчику пеню в размере 0,1 % от стоимости ремонтируемого блока за каждый день просрочки, но не более 5% от стоимости ремонтируемого блока.

1.14 Требования к услугам по проектированию, монтажу и пусконаладке

Оказываемые услуги и проводимые работы должны включать в себя:

1.14.1 Разработку Требований к Местам установки Оборудования;

1.14.2 Изыскания на объектах Покупателя;

1.14.3 Разработку Технического документа;

1.14.4 Разработку Программы и методики испытаний;

1.14.5 Сборку, наладку, конфигурирование и тестирование комплектов оборудования на производственных площадках АО «Казахтелеком»;

1.14.6 Проведение приемочных испытаний.

1.15 Требования к документации

1.15.1 Вся документация должна соответствовать принятым стандартам. По возможности должны быть использованы стандартизированные символы и термины, рекомендованные ITU-T, ETSI, IETF;

1.15.2 Технический документ

- 1.15.2.1 Технический документ должен быть выполнен на русском или английском языке;
- 1.15.2.2 Технический документ должен быть выполнен поставщиком, представлен в бумажном виде и утвержден АО «Казахтелеком».

Технический документация ПУ СОРМ должен включать:

- 1.15.2.3 Структура проектируемого оборудования;
- 1.15.2.4 Детальная схема проектируемого оборудования;
- 1.15.2.5 Логические схемы всех подсистем оборудования;
- 1.15.2.6 Схемы и таблицы внутриузловых и межузловых соединений;
- 1.15.2.7 Монтажные схемы узлов сети;
- 1.15.2.8 Зарисовки фасадов стоек с оборудованием на узлах сети;
- 1.15.2.9 Схемы подключения к кроссам;
- 1.15.2.10 Схемы распределения питания на устройства сети;
- 1.15.2.11 Система IP адресации;
- 1.15.2.12 Система организации маршрутизации и используемые транспортные протоколы;
- 1.15.2.13 Детальная схема подключения пользователей и организации услуг;
- 1.15.2.14 Схема организации качества обслуживания на сети;

1.15.2.11. Система IP адресации;

1.15.2.12. Система организации маршрутизации и используемые транспортные протоколы;

1.15.2.13. Детальная схема подключения пользователей и организации услуг;

1.15.2.14. Схема организации качества обслуживания на сети;

1.15.2.15. Схема организации и механизмы обеспечения информационной безопасности;

1.15.2.16. Схема организации связи с внешними сетями;

1.15.2.17. Описание системы управления комплексом оборудования;

1.15.2.18. Описание настроек типовых сервисов сети;

1.15.3. Эксплуатационная документация

1.15.3.1. Основная эксплуатационная документация, необходимая для повседневной работы обслуживающего персонала должна быть представлена в бумажном или электронном виде на русском или английском языке.

1.15.3.2. Эксплуатационная документация, не связанная с повседневной работой обслуживающего персонала, а так же подверженная частым корректировкам при смене версий программного обеспечения может быть представлена в электронном виде на английском языке.

Эксплуатационная документация для обеспечения эффективной технической эксплуатации ПУ СОРМ должна включать руководства оператора:

1.15.3.3. Общее описание оборудования, включающее основные характеристики, производительность, описание оборудования, программного обеспечения, принципы технической эксплуатации оборудования;

1.15.3.4. Функциональное описание системы;

1.15.3.5. Описания подсистем и функциональных блоков;

1.15.3.6. Описание программного обеспечения, включающее технические описания программ (обработки вызовов, технической эксплуатации и др.);

1.15.3.7. Описания функционирования плат (назначение платы, подробное описание работы по электрической схеме, сопряжение платы с остальным оборудованием);

1.15.3.8. Инструкция по техобслуживанию с перечнем операций по обслуживанию и управлению неисправностями, а также с перечнем директив, связанных с ними;

1.15.3.9. Руководство по аварийным ситуациям и процедурам восстановления и замене аппаратных средств;

1.15.3.10. Инструкция по вхождению оборудования в нормальный режим работы при аварийных ситуациях (включая дуплексные остановки, т.е. загрузку с backup);

1.15.3.11. Справочник по аварийной сигнализации, содержащий информацию о выводимых на принтер (дисплей) сообщениях об аварийном состоянии с точностью до съемной платы или об ошибках файлов программного обеспечения;

1.15.3.12. Справочник по директивам, содержащий описание директив в соответствии с пунктами Инструкции по эксплуатации;

11.4. Справочник по кодам разъединений (ошибок в установлении соединений) и их анализу;

Спецификация по подключаемым телекоммуникационным объектам
для расчета ПУ СОРМ

К оборудованию ПУ СОРМ устанавливаемому в г.Алматы и г.Актобе, в первом этапе подключаются оборудования указанные в таблице №1 и таблице №2. Впоследствии к ПУ СОРМ г.Алматы будут подключены коммутационные системы Алматинской области, Жамбылской области, Кызылординской области, Южно-Казахстанской области. К ПУ СОРМ г.Актобе впоследствии будут подключены коммутационные системы Мангистауской области, Атырауской области, Западно-Казахстанской области. Разрешается давать ценовое предложение на одну точку организации ПУ СОРМ (г.Алматы) с организацией точек съема в областных центрах и с передачей в центр снятой информации по IP среде (в данном случае в г.Актобе будет только центр съема трафика).

В случае когда оборудование ПУ СОРМ поставщика не может от коммутационной системы принять интерфейс СОРМ (например ETSI, CALEA, российский и.т.д.), что в свою очередь требует установки конвертора, для АО «Казахтелеком» конвертор является частью оборудования ПУ СОРМ и поставщик должен предложить ценовое предложение на каждое подключение.

В составе поставляемого оборудования должна быть рассмотрена аппаратная и программная возможность тестового подключения двух интерфейсов от маршрутизаторов Cisco и Juniper по стандарту **LI ETSI TS 102 232 (все версии)**

Таблица №1. г.Алматы.

Название	Тип	Кол-во	Версия ПО	Станционный	Наличие конвертора

Juniper по стандарту **LI ETSI TS 102 232 (все версии)**

Таблица №1. г.Алматы.

Название коммутационной системы	Тип системы	Кол-во абонентов	Версия ПО	Станционный интерфейс СОРМ	Наличие конвертора СОРМ
SSW Almaty	CS2000 Nortel	172877	CVM12	ETSI	Установлен конвертор Mera. Преобразование на казахстанский интерфейс
SSW GEO Almaty	CS2000 Nortel	184963	CVM14	ETSI	Установлен конвертор Mera. Преобразование на казахстанский интерфейс
ОПТС-3	5ESS	61056	5EE16(1)	CALEA	Установлен конвертор Ронекс. Преобразование на казахстанский интерфейс
ОПТС-6-2	5ESS	31867	5EE16(1)	CALEA	Установлен конвертор Ронекс. Преобразование на казахстанский интерфейс
ОПС-73	5ESS	22286	5EE16(1)	CALEA	Установлен конвертор Ронекс. Преобразование на казахстанский интерфейс
ОС-2512	C&C08	2128	Version 6.10(R002)	ETSI	нет
ОПТС-4	S-12	36103	WR1	ETSI	
ОПТС-6	S-12	38220	WR1	ETSI	
ОПС-51	S-12	19965	EC7.1	ETSI	Конвертора нет. Установлен A8619, который преобразовывает на российский стандарт
ОПС-521	S-12	12000	EC7.1	ETSI	Конвертора нет. Установлен A8619, который преобразовывает на российский стандарт
Концетратор СОРМ Искрател				Казахстанский интерфейс	Казахстанский интерфейс
SoftX3000 Востоктелеком	SoftX3000	120 000	PVMV100R013C03B032SP034	ETSI	XPTU -> российский -> Протех -> казахстанский

Таблица №2. Г.Актобе .

Название коммутационной системы	Тип системы	Кол-во абонентов	Версия ПО	Станционный интерфейс СОРМ	Наличие конвертора СОРМ
SSW CDMA	SoftX3000	76793	V300R601	ETSI	XPTU -> российский -> Протех -> казахстанский
АТС-21/22	DMS-100	26875	ISN07	ETSI	Нет. Нет подключения

					> Протех -> казахстанский
АТС-21/22	DMS-100	26875	ISN07	ETSI	Нет. Нет подключения к ПУ
АТС-54/56	DMS-100	46610	ISN07	ETSI	Установлен конвертор Ронекс. Преобразование на казахстанский интерфейс
SSW NGN	CS2000 Nortel	28912	CVM11	ETSI	Установлен конвертор Mera. Преобразование на казахстанский интерфейс
Концетратор СОРМ Искрател				Казахстанский интерфейс	Казахстанский интерфейс

Приложение 3
к Тендерной документации по электронному тендеру по закупке оборудования Пульта управления СОРМ с услугами монтажа и пуско-наладки "под ключ"

Форма заявки на участие в электронных закупках способом тендера
(для юридических лиц)

Кому: ____

(указывается наименование заказчика)

От кого ____

(указывается наименование потенциального поставщика)

1. Сведения о юридическом лице, претендующем на участие в тендере (потенциальном поставщике):

Полное наименование юридического лица - потенциального поставщика (в соответствии со свидетельством о государственной регистрации)	
Номер и дата свидетельства о государственной регистрации юридического лица	
Регистрационный номер налогоплательщика (РНН)	
Бизнес-идентификационный номер (БИН)	
Юридический, почтовый адрес и адрес электронной почты, контактные телефоны, потенциального поставщика	
Банковские реквизиты юридического лица (включая полное наименование банка или его филиала)	
Ф.И.О. первого руководителя юридического лица	

2. ___________________ (указывается полное наименование юридического лица) настоящей заявкой на участие в электронных закупках способом тендера (далее - Заявка) выражает желание принять участие в электронных закупках способом тендера ___________________________ (наименование закупки) в качестве потенциального поставщика и выражает согласие оказать услуги, поставить товары в соответствии с требованиями и условиями, предусмотренными настоящей Тендерной документацией.

3. Потенциальный поставщик подтверждает, что он ознакомлен с Тендерной документацией и осведомлен об ответственности за предоставление Заказчику и Тендерной комиссии

предусмотренными настоящей Тендерной документацией.

3. Потенциальный поставщик подтверждает, что он ознакомлен с Тендерной документацией и осведомлен об ответственности за предоставление Заказчику и Тендерной комиссии недостоверных сведений о своей правомочности, квалификации, качественных и иных характеристиках поставки товаров, оказания услуг, соблюдении им авторских и смежных прав, а так же иных ограничений, предусмотренных действующим законодательством Республики Казахстан.

Потенциальный поставщик принимает на себя полную ответственность за представление в данной заявке на участие в электронных закупках способом тендера и прилагаемых к ней документах таких недостоверных сведений.

4. Перечень документов подтверждающих применимость к заявке критериев оценки, влияющих на условное понижение цены потенциального поставщика указанных в пункте 39 Правил закупок Холдинга (в случае, если потенциальный поставщик претендует на применение критериев, влияющих на условное понижение цены).

№ п/п	Критерии оценки	Условное понижение цены	Подтверждающий документ
1.			
2.			

5. Перечень прилагаемых документов.

№ п\п	Наименование документа	Количество листов
1.		
2.		

6. Настоящая заявка действует в течение ___ дней.

7. До момента заключения договора о закупках настоящая заявка вместе с Вашим уведомлением о признании ее выигравшей будет выполнять роль обязательного договора между нами.

Дата заполнения ____________________

Приложение 4
к Тендерной документации по электронному тендеру по закупке оборудования Пульта управления СОРМ с услугами монтажа и пуско-наладки "под ключ"

Форма заявки на участие в электронных закупках способом тендера

Форма заявки на участие в электронных закупках способом тендера
(для физического лица)

Кому: ____

(указывается наименование Заказчика)

От кого: ____

(Ф.И.О. потенциального поставщика)

1. Сведения о физическом лице, претендующем на участие в тендере (потенциальном поставщике):

Ф.И.О. физического лица - потенциального поставщика, в соответствии с документом, удостоверяющим личность	
Данные документа удостоверяющего личность физического лица – потенциального поставщика	
Адрес регистрации физического лица - потенциального поставщика	
Фактический адрес проживания физического лица - потенциального поставщика	
Регистрационный номер налогоплательщика (РНН)	
Индивидуальный идентификационный номер (ИИН)	
Номер свидетельства о регистрации либо иного документа дающего право на занятие, соответствующее предмету закупки, предпринимательской деятельностью в соответствии с законодательством Республики Казахстан	
Банковские реквизиты физического лица - потенциального поставщика (включая полное наименование банка или его филиала)	
Контактные телефоны, почтовый адрес и адрес электронной почты (при его наличии) физического лица - потенциального поставщика	

2. ___________________ (указывается Ф.И.О. физического лица) настоящей заявкой на участие в электронных закупках способом тендера (далее - Заявка) выражает желание принять участие в электронных закупках способом тендера ___________________________ (наименование закупки) в качестве потенциального поставщика и выражает согласие оказать услуги, поставить товары, в соответствии с требованиями и условиями, предусмотренными настоящей Тендерной документацией.

3. Потенциальный поставщик подтверждает, что он ознакомлен с Тендерной документацией и осведомлен об ответственности за предоставление Заказчику и Тендерной комиссии недостоверных сведений о своей правомочности, квалификации, качественных и иных характеристиках поставки товаров, оказания услуг, соблюдении им авторских и смежных прав, а так же иных ограничений, предусмотренных действующим законодательством Республики Казахстан.

Потенциальный поставщик принимает на себя полную ответственность за представление в данной заявке на участие в электронных закупках способом тендера и прилагаемых к ней документах таких недостоверных сведений.

4. Перечень документов подтверждающих применимость к заявке критериев оценки, влияющих на

данной заявке на участие в электронных закупках способом тендера и прилагаемых к ней документах таких недостоверных сведений.

4. Перечень документов подтверждающих применимость к заявке критериев оценки, влияющих на условное понижение цены потенциального поставщика указанных в пункте 39 Правил закупок Холдинга (в случае, если потенциальный поставщик претендует на применение критериев, влияющих на условное понижение цены).

№ п/п	**Критерии оценки**	**Условное понижение цены**	**Подтверждающий документ**
1.			
2.			

5. Перечень прилагаемых документов.

№ п\п	**Наименование документа**	**Количество листов**
1.		
2.		

6. Настоящая заявка действует в течение ___ дней.

7. До момента заключения договора о закупках настоящая заявка вместе с Вашим уведомлением о признании ее выигравшей будет выполнять роль обязательного договора между нами.

____

__________________________/ _________________/

(Ф.И.О. физического лица - потенциального поставщика и его подпись)

Дата заполнения __________________

Приложение 5
к Тендерной документации по электронному тендеру по закупке оборудования Пульта управления СОРМ с услугами монтажа и пуско-наладки "под ключ"

Банковская гарантия
(форма обеспечения тендерной заявки)

Наименование банка____
(наименование и реквизиты банка)

Кому____
(наименование и реквизиты Заказчика/Организатора закупок)

Гарантийное обязательство №_______

__________________ «___»_________ ______________г.
(местонахождение)

Мы были проинформированы, что ____,
(наименование потенциального поставщика)
в дальнейшем «Поставщик», принимает участие в тендере по закупке
____,
организованном ____,
(наименование Заказчика/Организатора закупок)
и готов осуществить поставку (оказать услугу) ____________________
_________________________________ на общую сумму ________________________ тенге.
(наименование и объем товаров , услуг) (прописью)

(наименование Заказчика/Организатора закупок)

и готов осуществить поставку (оказать услугу) ___________________

________________________________ на общую сумму ______________________ тенге.

(наименование и объем товаров, услуг) *(прописью)*

Тендерной документацией от «___»__________ _____ г. по проведению вышеназванных закупок предусмотрено внесение потенциальными поставщиками обеспечения тендерной заявки в виде банковской гарантии.

В связи с этим мы ______________________________________ настоящим берем на себя

(наименование банка)

безотзывное обязательство выплатить Вам по Вашему требованию сумму, равную

____,

(сумма в цифрах и прописью)

по получении Вашего письменного требования на оплату, а также письменного подтверждения того, что Поставщик:

- отозвал или изменил тендерную заявку после истечения окончательного срока представления тендерных заявок;
- не подписал в установленные сроки договор о закупках;
- не внес обеспечения возврата аванса (предоплаты) после подписания договора о закупках в форме, объеме и на условиях, предусмотренных в тендерной документации.

Данное гарантийное обязательство вступает в силу со дня вскрытия конвертов с тендерными заявками

Данное гарантийное обязательство действует до окончательного срока действия тендерной заявки Поставщика на участие в тендере и истекает полностью и автоматически, независимо от того, будет ли нам возвращен этот документ или нет, если Ваше письменное требование не будет получено нами к концу _____________. Если срок действия тендерной заявки продлен, то данное гарантийное обязательство продлевается на такой же срок.

Подпись и печать гаранта Дата и адрес

Все права и обязанности, возникающие в связи с настоящим гарантийным обязательством, регулируются законодательством Республики Казахстан.

Приложение 6
к Тендерной документации по электронному тендеру по закупке оборудования Пульта управления СОРМ с услугами монтажа и пуско-наладки "под ключ"

Банковская гарантия

(форма обеспечения возврата аванса (предоплаты))

Наименование банка:

____

(наименование и реквизиты банка)

Кому: ____

(наименование и реквизиты заказчика/Организатора закупок)

Гарантийное обязательство № ___

__________________ «___»___________ _____ г.

(местонахождение)

Принимая во внимание, что ___________________________________,

(наименование поставщика)

«Поставщик», заключил (-ит)* договор о закупках №__ от ______ г. (далее - Договор) на поставку (выполнение, оказание)

____

______________,и Вами было ____

(описание товаров, услуг)

предусмотрено в Договоре, что Поставщик внесет обеспечение возврата аванса (предоплаты)) в виде банковской гарантии на общую сумму

_________ тенге, настоящим ____

(наименование банка)

подтверждаем, что являемся гарантом по вышеуказанному Договору и берем на себя безотзывное обязательство выплатить Вам по Вашему требованию сумму, равную

____,

(сумма в цифрах и прописью)

по получении Вашего письменного требования на оплату, а также письменного подтверждения того, что Поставщик не исполнил или исполнил ненадлежащим образом свои обязательства по

(сумма в цифрах и прописью)

по получении Вашего письменного требования на оплату, а также письменного подтверждения того, что Поставщик не исполнил или исполнил ненадлежащим образом свои обязательства по Договору.

Данное гарантийное обязательство вступает в силу с момента его подписания и действует до момента исполнения поставщиком обязательств на сумму, превышающую сумму оплаченного аванса (предоплаты)/полного исполнения Поставщиком своих обязательств по Договору. *(нужное подчеркнуть)*.

Все права и обязанности, возникающие в связи с настоящим гарантийным обязательством, регулируются законодательством Республики Казахстан.

Подпись и печать гарантов Дата и адрес

Приложение 7
к Тендерной документации по электронному тендеру по закупке оборудования
Пульта управления СОРМ с услугами монтажа и пуско-наладки "под ключ"

Проект Договора о закупках товаров и услуг

г. Алматы **«__»_________2013г.**

АО «КАЗАХТЕЛЕКОМ», именуемое в дальнейшем Покупатель, в лице ______________________, действующего на основании ________________, с одной стороны и _______________________, именуемое в дальнейшем Поставщик, в лице _________________________, действующего на основании _____________________, с другой стороны, именуемые в дальнейшем Стороны, а по отдельности Сторона, на основании Правил закупок товаров, работ и услуг Акционерным Обществом «Фонд национального благосостояния «Самрук-Казына» и организациями пятьдесят и более процентов голосующих акций (долей участия) которых прямо или косвенно принадлежат АО «Самрук-Казына» на праве собственности или доверительного управления, утвержденных решением Совета Директоров АО «Самрук-Казына» (протокол № 93 от 07 июня 2013 года.) и Протокола об итогах открытого тендера по закупке оборудования Пульт управления СОРМ с услугами монтажа и пуско-наладки «под ключ» № _____ от «____» 2013 года заключили настоящий договор (далее - Договор) и пришли к соглашению о нижеследующем.

Организатор тендера, Дирекция «Телеком Комплект» объявил открытый тендер по закупке оборудования Пульт управления СОРМ с услугами монтажа и пуско-наладки «под ключ» и принял тендерную заявку Поставщика на сумму в размере ____ без учета НДС.

1. Предмет Договора

1.1. Поставщик обязуется поставить оборудование Пульт управления СОРМ (далее – Оборудование) на условиях DDP г. Алматы (далее - место назначения) и оказать услуги по монтажу и пусконаладке «под ключ» (далее – Услуги) в соответствии со Спецификацией, указанной в Приложении №1 Договора, а Покупатель обязуется принять Оборудование и оказанные Услуги и оплатить стоимость поставленного Оборудования и оказанных Услуг на условиях Договора.

1.2. Перечисленные ниже Приложения и условия, оговоренные в них, входят в состав данного Договора и являются его неотъемлемой частью, а именно:

1) Приложение №1 – «Спецификация Оборудования и Услуг»,
2) Приложение №2 – «Техническое задание»,
3) Приложение №3 – «Форма акта приема-передачи Оборудования»,
4) Приложение №4 – «Форма акта приемки-сдачи оказанных услуг»
5) Приложение №5 – «Форма акта предварительной приемки оборудования в эксплуатацию».
6) Приложение №6 – «Форма акта окончательной приемки оборудования в эксплуатацию».

3) Приложение №3 – «Форма акта приема-передачи Оборудования»,
4) Приложение №4 – «Форма акта приемки-сдачи оказанных услуг»
5) Приложение №5 – «Форма акта предварительной приемки оборудования в эксплуатацию».
6) Приложение №6 – «Форма акта окончательной приемки оборудования в эксплуатацию».

2. Обязательства Сторон

2.1. Поставщик обязуется:

2.1.1. Внести обеспечение возврата аванса (предоплаты) в размере 15 % (пятнадцать процентов) от цены Договора в течение 20 (двадцать) рабочих дней со дня подписания Договора;
2.1.2. Поставить Оборудование до мест назначений, указанных в пункте 5.1. Договора;
2.1.3. Предоставить сертификат соответствия Республики Казахстан, выданный юридическим лицом, аккредитованным Госстандартом Республики Казахстан, к моменту ввода оборудования в эксплуатацию. Все расходы по сертификации Поставщик берет на себя;
2.1.4. За свой счет произвести осмотр/обследование всех станций, чтобы точно определить, какой инсталляционный материал требуется и обследовать любые потенциальные проблемы;
2.1.5. Оказать Услуги на условиях Договора, представить счета-фактуры на монтажные и пусконаладочные работы;
2.1.6. Сдать объекты в эксплуатацию в соответствии с техническими требованиями;
2.1.7. Осуществлять гарантийное техническое обслуживание Оборудования в соответствии с условиями Договора;
2.1.8. За 3 (три) календарных дня поставить в известность Покупателя о времени и сроках поставки Оборудования;
2.1.9. Обеспечить долю местного содержания в Оборудовании и Услугах в размере ___ % и предоставлять достоверную отчетность по местному содержанию по запросу Покупателя и по форме, предоставленной Покупателем *(в случае наличия местного содержания)*.

2.2. **Покупатель обязуется:**

2.2.1. Принять поставляемое Оборудование в месте и в сроки, указанные в разделе 5 Договора;
2.2.2. Оплатить стоимость поставленного Оборудования и оказанных Услуг в порядке и на условиях Договора;
2.2.3. Возвратить Поставщику внесенное обеспечение возврата аванса (предоплаты) в течение 10 (десять) рабочих дней с даты поставки Оборудования и оказания Услуг на сумму, превышающую 15 % (пятнадцать процентов) стоимости Оборудования и оказываемых Услуг.

3. Цена и общая сумма Договора

3.1. Стоимость Оборудования, поставляемого по Договору, включая транспортировку до Места назначения, составляет ________________________.

3.2. Стоимость Услуг, оказываемых по Договору (далее – Стоимость услуг) составляет ______________________.

3.3. Цена Договора составляет ______________________________, плюс НДС в размере 12 % в сумме ____________________. Общая сумма Договора составляет ______________________, включая НДС.

3.4. Цена Услуг по Договору, указанная в Спецификации Приложения №1 к Договору, включает все расходы по командированию специалистов Поставщика, включая их проживание в Республике Казахстан, а также зарплату, страхование, и другие расходы, связанные с выполнением их обязательств и все остальные расходы, понесенные в период исполнения обязательств по Договору.

4. Условия платежа

4.1. Оплата по Договору за поставляемое Оборудование и оказанные Услуги будет осуществляться следующим образом:

- 15% предоплата от стоимости Оборудования и Услуг оплачивается в течение 20 (двадцать) рабочих дней с момента подписания договора и внесения обеспечения возврата аванса;
- 85% от стоимости Оборудования оплачивается в течение 20 (двадцать) рабочих дней с момента подписания Акта приема-передачи оборудования;
- 85% от стоимости Услуг оплачивается в течение 20 (двадцать) рабочих дней после оказания услуг. Датой оказания услуг считается дата подписания Акта сдачи-приемки оказанных услуг.

4.2. Все расчеты между Покупателем и Поставщиком по Договору производятся в

- 85% от стоимости Услуг оплачивается в течение 20 (двадцать) рабочих дней после оказания услуг. Датой оказания услуг считается дата подписания Акта сдачи-приемки оказанных услуг.

4.2. Все расчеты между Покупателем и Поставщиком по Договору производятся в ____________*(указать валюту).*

4.3. Оплата будет производиться на банковский (расчетный) счет Поставщика указанный в разделе 19. Договора. Датой осуществления платежа считается дата списания средств со счета Покупателя.

Для резидентов Республики Казахстан:

4.4. НДС оплачивается по мере возникновения налогового обязательства и предоставления счет-фактуры Поставщиком

Для нерезидентов Республики Казахстан:

4.5. Сумма выплат по Договору уменьшается на сумму налогов, подлежащих удержанию с доходов нерезидентов, согласно законодательству РК. При этом Поставщик вправе получить от Покупателя документ, подтверждающий удержание налога по законодательству РК. При наличии конвенции об избежании двойного налогообложения Поставщик вправе обратиться в соответствующие государственные органы страны Покупателя с заявлением о возврате или уменьшении подоходного налога с юридических лиц нерезидентов РК.

4.6. Оплата таможенных сборов и иных расходов, связанных с таможенной очисткой Оборудования в связи с импортом Оборудования на территорию Республики Казахстан, производится Поставщиком. Налоги, таможенные пошлины, подлежащие уплате на территории Республики Казахстан и все налоговые обложения, таможенные пошлины и другие расходы, связанные с поставкой Оборудования, за пределами страны Покупателя, оплачивает Поставщик.

4.7. Банковские расходы, возникающие при исполнении Договора и других сопутствующих документов, на территории страны Покупателя оплачиваются Покупателем, вне территории страны Покупателя - получателем платежа.

4.8. В случае заключения трехстороннего Соглашения по передаче прав и обязательств Поставщика в части оказания Услуг, предусмотренных Договором, какому-либо третьему лицу, стоимость, условия и сроки оплаты таких Услуг должны остаться такими, как это предусмотрено в пунктах 3.2 и 4.1. Договора *(в случае необходимости, если предусмотрено тендерной заявкой поставщика).*

5. Сроки и условия поставки Оборудования и оказания Услуг.

5.1.Поставка Оборудования должна быть осуществлена в течение 90 (девяносто) календарных дней, оказание Услуг услуг в течение 180 (сто восемьдесят) календарных дней с момента подписания Договора

Оборудование поставляется Поставщиком Покупателю на условиях DDP (ИНКОТЕРМС 2010), Республика Казахстан, по следующему адресу: *Грузополучатель:* Республика Казахстан, 050016, Алматы, ул. 2-я Гончарная, 145А, Дирекция «Телеком-Комплект». Код получателя: 5454, ОКПО 304154830073, РНН: 600500060008, тел./факс: (727) 294-26-68 (далее - Место назначения). Получатель: ГЦУСТ - филиал АО «Казахтелеком».

5.2. Датой поставки Оборудования считается дата поступления Оборудования на склад Покупателя в Месте назначения согласно расходной накладной, подписанной уполномоченным представителем Покупателя.

Датой оказания Услуг считается дата подписания Акта приемки оказанных Услуг по форме, указанной в Приложении 4 к Договору.

5.3. Досрочная поставка Оборудования и поставка партиями допускается. Определение вида транспорта, которым осуществляется транспортировка и склада временного хранения, осуществляется дополнительно по согласованию Поставщика и Покупателя в письменном виде до начала осуществления поставки Оборудования / каждой партии Оборудования.

5.4. Отгруженное Оборудование/каждая партия Оборудования должно иметь следующие сопроводительные документы:

Для резидентов РК:

- счет-фактура, 1 оригинал и 2 копии;
- накладная, 1 оригинал и 3 копии;
- техническое описание Оборудования на русском языке.

Один экземпляр расходной накладной, подписанной уполномоченным представителем Покупателя, должен быть возвращен Поставщику с оригиналом доверенности на получение товара

- техническое описание Оборудования на русском языке.

Один экземпляр расходной накладной, подписанной уполномоченным представителем Покупателя, должен быть возвращен Поставщику с оригиналом доверенности на получение товара по указанной расходной накладной.

Для нерезидентов РК:

- инвойс - 1 оригинал и 2 копии;
- транспортная накладная - 1 оригинал и 3 копии;
- экспортная декларация – 1 копия;
- упаковочный лист (с указанием серийных номеров оборудования и запасных деталей) - 3 оригинала;
- сертификат происхождения - 1 оригинал и 1 копия;
- техническое описание Оборудования на русском языке.

5.5. Поставщик, не позднее чем за 3 (три) календарных дней до даты поставки Оборудования на склад/передачи Оборудования (партии) грузоотправителю, должен согласовать с Покупателем отгрузочные документы (счет-фактуру / инвойс) на поставляемое Оборудование.

5.6. Поставщик несет ответственность за недостоверность информации, содержащейся в сопроводительных документах, указанных в пункте 5.4. Договора и возмещает все причинённые убытки.

5.7. Оборудование должно быть поставлено в комплектации, количестве и на условиях, определенных в Приложении № 1 к Договору.

5.8. По письменному запросу Поставщика Покупатель до начала монтажных работ должен получить и предоставить все разрешения, которые могут требоваться в связи с выполнением монтажных работ, такие как, но не ограничиваясь перечисленным: специальные разрешения, необходимые для перевозки, проезда к месту монтажа Оборудования, пропуски для прохода в здания и монтажные площадки, где будут вестись работы. При необходимости проведения обследования, согласно подпункту 2.1.4. Договора, такие пропуски и разрешения должны быть предоставлены Покупателем не позднее, чем за 3 (три) календарных дня до запланированной даты начала проведения обследования, при условии направления Поставщиком письменного запроса не менее чем за 15 (пятнадцать) календарных дней до начала проведения обследования.

5.9. По запросу Покупателя Поставщик своевременно предоставит ему необходимую информацию, которая может потребоваться Покупателю для оформления такого рода разрешений. Все документально подтвержденные расходы и затраты, непосредственно связанные с любого рода задержками, возникающими по причине неполучения Покупателем каких-либо требуемых разрешений, должны быть отнесены на счет и риск Покупателя.

6. Упаковка и маркировка

6.1. Оборудование должно быть упаковано в надлежащую упаковку. Упаковка должна обеспечить сохранность Оборудования во время транспортировки соответствующим видом транспорта с завода - изготовителя до конечного пункта и во время хранения в складских помещениях. Упаковка должна соответствовать государственным стандартам, техническим условиям, другой нормативно-технической документации. Упаковка должна обеспечивать возможность ручной и механической погрузки (грузоподъемником).

6.2. Упаковка (тара) маркируется водостойкой краской на английском и русском языках несмываемой краской. Маркировка должна быть четкой и включать следующие сведения:

- Покупатель
- Грузополучатель
- Договор №
- Изготовитель Оборудования;
- Количество Оборудования;
- Товарный знак;
- Условное обозначение Оборудования;
- Номер места (ящика, контейнера);
- Вес нетто, вес брутто;
- Размеры тары в см. (длина, высота, ширина).

Маркировка может иметь также другие обозначения, наличие которых предполагается специфическим характером оборудования или станции, где оно будет установлено.

6.3. Поставщик несет ответственность за все потери и/или неисправности, связанные с ненадежной упаковкой и неправильной маркировкой.

6.4. Поставщик обеспечивает передачу Оборудования (любых и всех составляющих

6.3. Поставщик несет ответственность за все потери и/или неисправности, связанные с ненадежной упаковкой и неправильной маркировкой.

6.4. Поставщик обеспечивает передачу Оборудования (любых и всех составляющих (комплектующих) частей оборудования) в усиленной упаковке производителя, соответствующей стандартам экспортной упаковки, безопасной транспортировки любым видом транспорта и хранению Оборудования подобного рода.

6.5. Покупатель должен обеспечить соответствующие условия хранения на основании технических и климатических требований по хранению.

7. Уведомления, переписка

7.1. Любые уведомления или другая информация, которые должны быть переданы одной из сторон другой стороне, будут считаться действительно переданными, когда они будут направлены по почте (предварительно оплаченным заказным письмом), или по факсу, или с курьером по следующим адресам:

Покупатель:	**Поставщик:**
АО «Казахтелеком» 050059, г. Алматы, ул. Фурманова, 240 б Департамент сопровождения контрактов, тел. +7 (727) 2587344, факс +7 (727) 2587446	

8. Приемка Оборудования

8.1 Поставщик, согласно подпункту 2.1.8. Договора, не менее чем за 3 (три) календарных дня до начала отправки, информирует Покупателя о готовности Оборудования к отправке.

8.2. Приемка Оборудования по количеству мест осуществляется филиалом – получателем в Месте назначения. При приемке филиалом - получателем составляются и подписываются документы в соответствии с внутренними нормативными актами Покупателя.

8.3. В случае отсутствия замечаний к поставленному Оборудованию по количеству и комплектности Сторонами в течение 7 (семь) рабочих дней со дня прибытия Оборудования на склад Покупателя в Место назначения подписывается Акт приема-передачи Оборудования по форме, указанной в Приложении № 3 к Договору. Вскрытие упаковки и проверка поступившего Оборудования на соответствие его Спецификациям осуществляется на месте монтажа.

8.4. В течение 14 (четырнадцати) календарных дней с Даты поставки Оборудования Покупатель обязан сообщить об обнаружении каких-либо дефектов или недостатков, в том числе, недопоставки, некомплектности, внешних повреждений и т.п. В случае обнаружения нарушений подобного рода составляется Акт с участием представителя торгово-промышленной палаты Казахстана, о чем не позднее 3 (трех) рабочих дней средствами почтовой либо факсимильной связи с предоставлением копии указанного Акта уведомляется Поставщик *(для нерезидентов)*/Акт с участием Поставщика *(для резидентов).* В течение 45 (сорок пять) рабочих дней с момента получения такого уведомления и Акта, Поставщик обязан доставить за свой счет недостающее либо заменяющее Оборудование. В этом случае расходы за оформление повторных таможенных процедур недостающего или заменяющего оборудования в стране Покупателя производятся за счет Поставщика.

8.5. Покупатель вправе, в случае наличия у него замечаний к поставленному Оборудованию, не подписывать Акт приема-передачи Оборудования до устранения Поставщиком всех замечаний либо замены, в соответствии с пунктом 8.4. Договора.

8.6. Право собственности на поставляемое Поставщиком Оборудование переходит к Покупателю с момента подписания Акта приема – передачи Оборудования.

8.7. Переход рисков. Риск случайной утраты и/или повреждения до даты поставки Оборудования до Места назначения несет Поставщик. С момента подписания Акта приема-передачи Оборудования риск случайной утраты и/или повреждения (всех составляющих /комплектующих/ частей Оборудования) несет Покупатель.

9. Оказание Услуг

9.1. Поставщик приступит к оказанию Услуг в течение 10 (десять) рабочих дней с даты получения письменного уведомления от Покупателя о готовности производственных площадок, на которых будет монтироваться Оборудование, в соответствии с рекомендациями, которые будут даны Поставщиком после выполнения обследования мест установки Оборудования.

9.1. Поставщик приступит к оказанию услуг в течение 10 (десять) рабочих дней с даты получения письменного уведомления от Покупателя о готовности производственных площадок, на которых будет монтироваться Оборудование, в соответствии с рекомендациями, которые будут даны Поставщиком после выполнения обследования мест установки Оборудования.

9.2. Если Покупатель не выполняет условия, оговоренные в пунктах 5.8. и 9.1. Договора, Поставщик должен незамедлительно направить Покупателю письменное уведомление о факте задержки со стороны Покупателя и продлении срока оказания Услуг. После получения уведомления от Поставщика, Покупатель должен оценить ситуацию и, в случае необходимости, продлить срок предоставления Услуг на срок задержки.

9.3. Поставщик обязуется выполнить Услуги в сроки, указанные в пункте 5.1. Договора, при условии, что:

1) Покупатель получил и предоставил до запланированной для предоставления Услуг даты все требующиеся разрешения, согласно пункту 5.8. Договора;
2) места установки Оборудования подготовлены вовремя, согласно пункту 9.1. Договора;
3) срок окончания предоставления Услуг не был продлен по взаимному согласованию Сторон.

9.4. Поставщик несет полную ответственность за монтаж, настройку, проведение измерений и тестов Оборудования в соответствии с техническими требованиями Покупателя при условии, что Покупатель выполнит свои обязательства согласно условиям этого Договора.

10. Приемо - сдаточные испытания Оборудования, ввод в эксплуатацию

10.1. Оборудование должно быть сдано в эксплуатацию в течение 180 (сто восемьдесят) календарных дней с даты подписания Договора, при условии готовности инфраструктуры и мест монтажа Оборудования. Оборудование будет принято в эксплуатацию только после предоставления Поставщиком сертификатов соответствия безопасности (качеству) Республики Казахстан на установленное Оборудование. Датой ввода Оборудования в эксплуатацию считается дата подписания Акта окончательной приемки Оборудования в эксплуатацию (Приложение № 6 к Договору).

10.2. Испытания по вводу Оборудования в эксплуатацию будут проводиться после завершения монтажа, настройки и измерений совместно со специалистами Поставщика и Покупателя в соответствии с утвержденной Программой приемо-сдаточных испытаний. По факту выполнения всех тестовых процедур специалисты филиала, ответственные за проверку работоспособности поставленного оборудования и представители Поставщика подписывают Протокол приемо-сдаточных испытаний.

10.3. В случае, если приемо-сдаточные испытания проведены успешно, т.е. не было обнаружено никаких дефектов или недостатков, влияющих на работоспособность Оборудования, филиалом, где было установлено Оборудование, подписывается Акт рабочей комиссии о приемке Оборудования в эксплуатацию с обязательным участием представителя Поставщика. На основании Акта рабочей комиссии филиала, подписанного без замечаний, Покупателем и Поставщиком подписывается Акт приемки-сдачи оказанных услуг, одновременно с этим подписывается Акт окончательной приемки оборудования в эксплуатацию по форме, указанной в Приложении 6 к Договору.

10.4. В случае наличия в Протоколе приемо-сдаточных испытаний непринципиальных замечаний, не влияющих на технологический процесс работы Оборудования, но при этом требующих устранения до момента приемки Оборудования в эксплуатацию, Рабочая комиссия подписывает Акт рабочей комиссии о приемке Оборудования в опытную эксплуатацию с указанием всех замечаний и срока опытной эксплуатации, в течении которого должны быть устранены указанные замечания, но не более 60 (шестьдесят) календарных дней. На основании Акта Рабочей комиссии о приемке оборудования станционных сооружений в опытную эксплуатацию подписывается Акт предварительной приемки Оборудования в эксплуатацию с приложением всех замечаний и сроков их устранения по форме, указанной в Приложении 5 к Договору. После Акта предварительной приемки подписывается Акт приемки-сдачи оказанных услуг.

10.5. По завершении периода опытной эксплуатации и устранения замечаний, указанных в Акте предварительной приемки, Рабочая комиссия принимает решение о готовности Оборудования к эксплуатации и подписывает Акт Рабочей комиссии о приемке станционных сооружений в эксплуатацию. На основании Акта рабочей комиссии филиала о приемке станционных сооружений в эксплуатацию, Покупателем и Поставщиком подписывается Акт окончательной приемки оборудования в эксплуатацию.

10.6. Если в течение 30 (тридцать) календарных дней после уведомления Поставщиком об устранении всех замечаний, отраженных в Акте предварительной приемки и готовности приемки оборудования в эксплуатацию.

10.6. Если в течение 30 (тридцать) календарных дней после уведомления Поставщиком об устранении всех замечаний, отраженных в Акте предварительной приемки и готовности Оборудования к сдаче в коммерческую эксплуатацию Поставщик не получает подписанный Акт окончательной приемки Оборудования в эксплуатацию или письменно обоснованное объяснение Покупателя об отказе от приемки, то считается действительным Акт окончательной приемки Оборудования в эксплуатацию, подписанный только Поставщиком.

11. Гарантии. Качество. Рекламации

11.1. Поставщик гарантирует высокое качество поставляемого Оборудования, материалов и комплектующих, а также качество производственной технологии, отвечающей самым современным мировым стандартам и нормам. Качество поставляемого Оборудования подтверждается сертификатом соответствия безопасности (качеству), а количество и номенклатура поставки должна соответствовать Спецификациям, указанным в Приложении № 1 к Договору.

11.2. Гарантийный срок составляет 12 (двенадцать) месяцев с момента подписания Акта окончательной приемки Оборудования в эксплуатацию при условии соблюдения требований, указанных в технической документации на Оборудование, предписаний Поставщика, а также стандартных норм и правил на поставляемое Оборудование. Поставщик в течение гарантийного периода должен обеспечить ремонт оборудования, сопровождение программного обеспечения (устранение ошибок, загрузка новых версий ПО и др.), устранение аварий.

Если в течение гарантийного периода будут выявлены дефекты Оборудования или его несоответствие условиям Договора, Поставщик за свой счет обязуется отремонтировать или заменить дефектное Оборудование на новое в течение 45 (сорок пять) рабочих дней со дня отправки на ремонт. В случае замены вышедшего из строя блока на новый во время гарантийного периода, срок гарантийного периода на данный блок продлевается на срок, в течение которого этот блок находился в нерабочем состоянии. Все расходы по ремонту или замене дефектного Оборудования, в том числе, связанные с таможенной очисткой и транспортировкой, также несет Поставщик на условиях поставки, предусмотренных Договором.

11.3. Гарантия не распространяется на дефекты, вызванные неправильной эксплуатацией или несанкционированным использованием Оборудования Покупателем и/или третьей стороной, а также, если имели место обстоятельства непреодолимой силы (стихийные бедствия, пожар, наводнение и др.), повлекшие за собой повреждение и выход из строя Оборудования.

11.4. Претензия (рекламация) по вопросам качества и количества поставленного Оборудования предъявляется Покупателем к Поставщику:

а) по количеству - не позднее 30 (тридцать) календарных дней с даты поставки Оборудования;

б) по качеству – в течение гарантийного периода.

Поставщик обязан рассмотреть претензию (рекламацию) в течение 5 (пять) рабочих дней с момента ее получения. Если Поставщик не дал ответа в названный срок, такая претензия считается признанной Поставщиком.

12. Ответственность Сторон

12.1. В случае нарушения Поставщиком срока поставки Оборудования, установленного пунктом 5.1. Договора, Покупатель вправе предъявить письменное требование об уплате пени, а Поставщик при получении такого требования уплачивает Покупателю пеню в размере 0,1% от стоимости не поставленного в срок Оборудования за каждый день просрочки, но не более 10% от стоимости не поставленного Оборудования.

12.2. В случае превышения по вине Поставщика сроков оказания Услуг и с учетом выполнения Покупателем условий пунктов 5.8., 9.1. Договора, Покупатель вправе письменно потребовать, а Поставщик при получении такого требования должен оплатить Покупателю пеню в размере 0,1% за каждый день просрочки, но не более 10% от суммы неисполненного обязательства.

12.3. Если поставленное Оборудование не соответствует по качеству стандартам, иной документации или условиям Договора, а также, если поставлено некомплектное Оборудование, Поставщик меняет его или доукомплектовывает на Оборудование надлежащего качества. Если Оборудование не будет возвращено Покупателю в течение 45 (сорок пять) рабочих дней с момента предъявления Покупателем соответствующих требований, Покупатель вправе потребовать, а Поставщик в этом случае будет обязан уплатить штрафные санкции в размере 0,1% от стоимости неисправного/недопоставленного Оборудования за каждый день просрочки, но не более 10% от стоимости неисправного/недопоставленного Оборудования. Если Поставщик в установленный

Поставщик в этом случае будет обязан уплатить штрафные санкции в размере 0,1% от стоимости неисправного/недопоставленного Оборудования за каждый день просрочки, но не более 10% от стоимости неисправного/недопоставленного Оборудования. Если Поставщик в установленный Сторонами срок устранил дефекты в Оборудовании или доукомплектовал его, штрафы, предусмотренные настоящим пунктом, не взимаются.

12.4. При несвоевременной оплате Оборудования/Услуг, Поставщик вправе потребовать, а Покупатель в этом случае должен будет заплатить Поставщику пеню в размере 0,1 % от суммы просроченного платежа за каждый день просрочки, но не более 10% от суммы просроченного платежа. Действие этого пункта на предоплату не распространяется.

12.5. Если Поставщик не начнет поставку Оборудования или оказание Услуг по любой причине не по вине Покупателя в течение 140 (сто сорок) календарных дней с момента получения предоплаты, то Поставщик обязан вернуть сумму аванса, но не позднее 300 (триста) календарных дней с момента его перечисления.

12.6. В случае неисполнения Поставщиком обязательств по доле местного содержания, указанного в подпункте 2.1.9. Договора, Поставщик выплачивает штраф в размере 5%, а также 0,15% за каждый 1% невыполненного местного содержания, от общей стоимости договора, но не более 15% от общей стоимости Договора. За несвоевременное предоставление отчетности по местному содержанию и предоставление недостоверной отчетности Поставщик выплачивает Покупателю штраф в размере 15% от общей стоимости Договора *(в случае наличия местного содержания)*.

12.7. В случае расторжения Договора в одностороннем порядке, по основаниям, указанным в разделе 15. Договора, виновная Сторона выплачивает штраф в размере 5% от общей стоимости Договора.

12.8. Уплата пени и штрафов не является основанием для освобождения Сторон от обязательств по Договору. Уплата неустоек и штрафов осуществляется Сторонами в течение 20 (Двадцати) банковских дней с даты получения соответствующего уведомления.

12.9. В случае применения к Поставщику штрафных санкций, Покупатель вправе удержать начисленную сумму пени и/или штрафа из сумм, подлежащих выплате Поставщику за исполненные обязательства согласно условиям Договора.

13. Форс-мажорные обстоятельства

13.1. Ни одна из Сторон не несет ответственности перед другой Стороной за невыполнение обязательств по Договору, возникших помимо воли и желания Сторон, которые нельзя предвидеть или избежать, включая объявленную или фактическую войну, гражданские волнения, эпидемии, блокаду, эмбарго, землетрясения, наводнения, пожары и другие стихийные бедствия.

13.2. Свидетельство, выданное компетентным органом, является достаточным подтверждением наличия и продолжительности действия непреодолимой силы.

13.3. Сторона, для которой стало невозможным выполнение своих обязательств по Договору должна дать извещение другой Стороне в течение 7 (семь) рабочих дней о начале и прекращении действия обстоятельств, воспрепятствовавших выполнению обязательств по Договору. В случае несвоевременного извещения о наступлении форс-мажорных обстоятельств, соответствующая Сторона лишается права освобождения от обязательств по настоящему Договору.

13.4. Если обстоятельства непреодолимой силы действуют на протяжении 3-х (трех) последовательных месяцев и не обнаруживают признаков прекращения, настоящий Договор может быть расторгнут любой из Сторон путем направления уведомления другой Стороне.

14. Срок действия Договора

14.1. Договор вступает в силу с момента его подписания и внесения обеспечения возврата аванса и действует до полного и надлежащего исполнения Сторонами своих обязательств по Договору.

15. Расторжение Договора в одностороннем порядке

15.1. Покупатель вправе в одностороннем порядке расторгнуть Договор путем направления другой Стороне уведомления за 10 (десять) рабочих дней до даты расторжения в случаях:

- поставки Оборудования ненадлежащего качества с недостатками, которые не могут быть устранены в приемлемый для Покупателя срок;
- не поставки Оборудования/не оказания Услуг в срок свыше 60 (шестьдесят) календарных дней с момента, указанного в пункте 5.1. Договора;
- не внесения обеспечения возврата аванса (предоплаты) в соответствии с условиями, оговоренными в подпункте 2.1.1. Договора.

- не поставки Оборудования/не оказания услуг в срок свыше 60 (шестьдесят) календарных дней с момента, указанного в пункте 5.1. Договора;
- не внесения обеспечения возврата аванса (предоплаты) в соответствии с условиями, оговоренными в подпункте 2.1.1. Договора.

Покупатель вправе требовать от Поставщика возврат ранее уплаченной суммы, за вычетом документально подтвержденных расходов, понесенных Поставщиком в связи с исполнением Договора до момента расторжения Договора, при этом возврат осуществляется в течении 30 календарных (тридцать) дней с момента получения уведомления о расторжения Договора

15.2. Поставщик вправе в одностороннем порядке расторгнуть Договор путем направления другой Стороне уведомления за 10 (десять) рабочих дней до даты расторжения в случае:
- нарушения Покупателем сроков оплаты более чем на 60 (шестьдесят) календарных дней.

16. Гарантийное обслуживание

16.1. Гарантийное обслуживание, оказываемое Поставщиком в рамках данного Договора, должно включать в себя ремонт оборудования, сопровождение программного обеспечения (устранение ошибок, загрузка новых версий ПО и др.), устранение аварий, консультирование с целью разрешения технических проблем по телефону, факсу или электронной почте (по вопросам функционирования, эксплуатации и конфигурации Оборудования).

16.2. Поставщик должен обеспечивать поставку ЗИП всех заменяемых плат, модулей, мелких деталей и прочих запасных частей, требуемых для техобслуживания после окончания гарантийного срока не менее 10 лет. Цены на ЗИП не должны повышаться не менее 7 (семь) лет после заключения Договора. Закупка ЗИП будет осуществляться на основе отдельно заключаемого Договора, в соответствии с законодательством Республики Казахстан и внутренними актами Покупателя.

16.3. По окончании гарантийного срока, услуги по технической поддержке и послегарантийному обслуживанию будут оказаны Покупателю на основе отдельного договора, заключаемого в рамках законодательства Республики Казахстан и/или внутренних актов Покупателя, регламентирующих порядок осуществления закупок.

17. Разрешение споров

17.1. В случае возникновения споров и разногласий по Договору, Стороны обязуются принять все меры к их урегулированию путем переговоров.

17.2. В случае невозможности разрешения споров и разногласий путем переговоров между Сторонами, то они подлежат разрешению в судебном порядке, в соответствии с законодательством Республики Казахстан.

17.3. Применимым правом является право Республики Казахстан. Спорные вопросы рассматриваются судами Республики Казахстан в соответствии с законодательством РК и на территории Республики Казахстан.

18. Прочие условия

18.1. Все изменения и дополнения к Договору будут иметь юридическую силу, если они не противоречат законодательству Республики Казахстан и/или иным документам, регламентирующим порядок осуществления закупок товаров, работ и услуг Покупателем, совершены в письменной форме, подписаны уполномоченными представителями Сторон и скреплены печатями Сторон.

18.2. Ни одна из Сторон Договора не может переуступать или передавать любые и/или все свои права либо обязательства третьей стороне без предварительного получения письменного согласия другой Стороны.

18.3. Поставщик имеет право с письменного согласия Покупателя нанять субподрядчиков, при условии предоставления Покупателю Договора субподряда. Наличие субподрядчиков не освобождает Поставщика от любых его обязательств или обязанностей по Договору. Поставщик гарантирует должный уровень профессионализма субподрядчиков. Такие отношения субподряда ни в коей мере не меняют сущность этого Договора на условиях «под ключ», а также не освобождают Поставщика от его обязательств по Договору относительно полной ответственности за установку и сдачу в эксплуатацию всего Оборудования. В рамках Договора Поставщик остается единственным партнером Покупателя.

18.4. Ни одна из Сторон не должна без предварительного письменного согласия другой Стороны раскрывать кому-либо содержание Договора или какого-либо из его положений, а также остается единственным партнером Покупателя.

18.4. Ни одна из Сторон не должна без предварительного письменного согласия другой Стороны раскрывать кому-либо содержание Договора или какого-либо из его положений, а также содержание технической документации, планов, чертежей, моделей, образцов или другой информации, связанных с заключением или исполнением Договора, за исключением того персонала, который привлечен для выполнения настоящего Договора. Указанные документы и/или информация будут использоваться Сторонами конфиденциально и исключительно в той мере, насколько это необходимо для выполнения договорных обязательств.

18.5. Договор составлен на русском языке в двух экземплярах, имеющих равную юридическую силу, один экземпляр Поставщику и один экземпляр Покупателю.

19. Юридические адреса, банковские реквизиты и подписи «Сторон»

Покупатель:	**Поставщик:**
АО «Казахтелеком» *Юридический адрес:* Республика Казахстан, 010000, г. Астана, р-он Сарыарка, пр. Абая, 31, *Почтовый адрес:* 050059, г. Алматы, ул. Фурманова, 240 б, РНН 600700017446, БИН 941240000193 *Банковские реквизиты:*	

Покупатель:	**Поставщик:**
____________________	______________________
«___»______________________2013г.	**«___»_____________________2013г.**
м.п.	**м.п.**

Приложение №1

к Договору о закупках товаров и услуг

№ _______ от ________________ 2013г.

СПЕЦИФИКАЦИЯ ОБОРУДОВАНИЯ И УСЛУГ

№ п/п	Наименование комплектующих, входящих в состав оборудования	Ед. изм.	Цена, за ед.	Кол-во	Общая сумма

Покупатель: **Поставщик:**

____________________ ________________________

«___»______________________2013г. **«___»______________________2013г.**

м.п. **м.п.**

Приложение № 2

к Договору о закупках товаров и услуг

№ _______ от ________________ 2013г.

Техническое задание

Покупатель: **Поставщик:**

____________________ ________________________

____________________ ________________________

«___»______________________2013г. **«___»______________________2013г.**

м.п. **м.п.**

Приложение № 3

к Договору № _______________

от ___________________ 2013г.

Форма
Акта приема-передачи Оборудования

Место приемки Дата _________

Акционерное Общество «КАЗАХТЕЛЕКОМ» как «Покупатель», в лице __________________________, с одной стороны, и _________________ как «Поставщик», в лице_____________________, с другой стороны, составили настоящий Акт о нижеследующем:

В соответствии с условиями Договора ____________ от «_____» __________2013 г. Поставщик передает, а Покупатель принимает следующее Оборудование:

#	Код	Описание оборудования	Кол-во	Серийный номер	Цена	Сумма

Стоимость оборудования составляет _________ (__________________) тенге.

Претензии по комплектности и внешнему виду поставленного Поставщиком по Договору Оборудованию, стоимость поврежденного или недопоставленного Оборудования и сроки устранения претензий Поставщиком приведены ниже:

№	**Существо претензии**	**Срок устранения**	**Стоимость недопоставленного или поврежденного Оборудования**

От «Поставщика»: От «Покупателя»:

От «Поставщика»: От «Покупателя»:

_______________________ _______________________

Покупатель: **Поставщик:**

____________________ ________________________

«___»______________________2013г. **«___»_____________________2013г.**

м.п. **м.п.**

Приложение № 4
к Договору о закупках товаров и услуг

№ _______ от ________________ 2013г.

Форма
Акта приемки-сдачи оказанных Услуг

Дата: ___________ Место приемки. __________

Мы, нижеподписавшиеся представители АО «Казахтелеком», как «Покупателя» в лице _________________________, и __________________, как «Поставщик» в лице _____________________., составили настоящий Акт о том, что «Поставщиком» с _________________2013г. по _________ 2013г. оказаны согласованные Услуги, в соответствии с Договором №_____ от «_____»__________2013г., в следующем объёме:

Филиал	**Выполненные работы**	**Сумма,**	**НДС**	**Всего,**	**Номер заказа в SAP**
Итого:					

Выполненные «Поставщиком» услуги на территории _______________________________ соответствуют требованиям «Покупателя» и удовлетворяют условиям Договора.

Стоимость выполненных Услуг составляет _____________________________ (______________)

Услуги приняты **Услуги оказаны**

От «Покупателя»: **От « Поставщика»:**

_______________________ _______________________

Покупатель: **Поставщик:**

Покупатель: **Поставщик:**

____________________ ________________________

«___»_____________________2013г. **«___»_____________________2013г.**

м.п. **м.п.**

Приложение № 5
к Договору о закупках товаров и услуг
№ _______ от ________________ 2013г.

Форма

Акта предварительной приемки Оборудования в эксплуатацию

Договор № _____ от «____»_______________2013 г.

Стороны, подписывающие настоящий документ, при этом заявляют, что в соответствии с условиями Договора № ________ от «____»_____________2013 г.:

1. Оборудование ____________________ и услуги монтажа и пусконаладки «под ключ» для АО «Казахтелеком», поставленное и установленное _____________в соответствии с Договором №___ от «____»________2013г., соответствует согласованным спецификациям и, следовательно, передается и принимается для ввода в опытную эксплуатацию.
2. Услуги монтажа и пусконаладки на условиях «под ключ», включающие в себя:

- Установку, конфигурирование и пусконаладку оборудования:
- Проведение тестовых испытаний, ввод в эксплуатацию:

выполнены в полном объеме, предусмотренном Договором.

3. Все вышеуказанные работы осуществлены в сроки:

Начало: ______________ 2013г. Окончание: ______________ 2013г.

4. Место установки оборудования: __________________________ .
5. В ходе предварительной приемки Оборудования выявлены замечания, не влияющие на технологический процесс работы Оборудования, но требующие устранения в период опытной эксплуатации. Срок опытной эксплуатации – 60 календарных дней с даты подписания Акта предварительной приемки Оборудования. Замечания и сроки их устранения представлены в Приложении к настоящему Акту.

Приложение
к Акту предварительной приемки Оборудования в эксплуатацию

Приложение
к Акту предварительной приемки Оборудования в эксплуатацию

№	Замечание	Срок устранения	Примечание

Покупатель: **Поставщик:**

____________________ _______________________

«___»_____________________2013г. **«___»_____________________2013г.**

м.п. **м.п.**

Приложение № 6
к Договору о закупках товаров и услуг
№ _______ от ________________ 2013г.

Форма

Акта окончательной приемки Оборудования в эксплуатацию

Договор № _____ от «____»_______________2013 г.

Стороны, подписывающие настоящий документ, при этом заявляют, что в соответствии с условиями Договора № ________ от «____»_____________2013 г.:

1. Оборудование ________________ и услуги монтажа и пусконаладки «под ключ» для АО

Стороны, подписывающие настоящий документ, при этом заявляют, что в соответствии с условиями Договора № ________ от «____»_____________2013 г.:

1. Оборудование _____________ и услуги монтажа и пусконаладки «под ключ» для АО «Казахтелеком», поставленное и установленное ____________ в соответствии с Договором № ______ от «____» ________ 2013г., соответствует согласованным спецификациям и, следовательно, передается и принимается для ввода в эксплуатацию.
2. Услуги монтажа и пусконаладки на условиях «под ключ», включающие в себя:
   - Установку, конфигурирование и пусконаладку оборудования:
   - Проведение тестовых испытаний, ввод в эксплуатацию:

   выполнены в полном объеме, предусмотренном Договором.
3. Все вышеуказанные работы осуществлены в сроки:

   Начало: ______________ 2013г. Окончание: ______________ 2013г.
4. Оборудование должным образом сертифицировано. Копия Казахстанского Сертификата соответствия является неотъемлемой частью данного Акта окончательной приемки в эксплуатацию.
5. Место установки оборудования: _________________________ .
6. Замечаний и недоделок нет.
7. Гарантийный период: 12 месяцев с даты подписания настоящего Акта окончательной приемки в эксплуатацию.

Покупатель: **Поставщик:**

___________________ ______________________

«___»_____________________2013г. **«___»_____________________2013г.**

м.п. **м.п.**

Приложение 8
к Тендерной документации по электронному тендеру по закупке оборудования Пульта управления СОРМ с услугами монтажа и пуско-наладки "под ключ"

Критерии для расчета минимальной условной цены

№	Критерий	Варианты ответов
1	Потенциальный поставщик является отечественным товаропроизводителем закупаемого товара в соответствии с представленным оригиналом или нотариально заверенной копией сертификата происхождения товара (формы СТ KZ) либо копией, заверенной государственным или иным уполномоченным органом, выдавшим сертификат и состоит в Реестре отечественных товаропроизводителей.	да/нет
2	Потенциальный поставщик является добросовестным поставщиком в соответствии с Перечнем добросовестных поставщиков Холдинга	да/нет
3	Потенциальный поставщик является организацией инвалидов (физическим лицом - инвалидом, осуществляющим предпринимательскую деятельность), производящей закупаемый товар в соответствии с представленным оригиналом или нотариально заверенной копией сертификата происхождения товара (формы СТ KZ) либо копией, заверенной государственным или иным уполномоченным органом, выдавшим сертификат и состоит в Реестре организаций инвалидов (физических лиц - инвалидов, осуществляющих	да/нет

	заверенной копией сертификата происхождения товара (формы СТ KZ) либо копией, заверенной государственным или иным уполномоченным органом, выдавшим сертификат и состоит в Реестре организаций инвалидов (физических лиц - инвалидов, осуществляющих предпринимательскую деятельность) Холдинга	
4	Наличие у потенциального поставщика опыта работы на однородном рынке закупаемых товаров, услуг, в течение последних 5 лет, подтвержденного соответствующими оригиналами или нотариально засвидетельствованными копиями накладных, соответствующих актов, подтверждающих прием-передачу поставленных товаров, оказанных услуг.	да/нет
5	Наличие у потенциального поставщика сертифицированной системы (сертифицированных систем) менеджмента в соответствии с требованиями государственных стандартов Республики Казахстан, соответствующей предмету проводимых закупок, подтвержденной нотариально засвидетельствованной копией сертификата системы менеджмента или копией, заверенной организацией, выдавшей сертификат	да/нет
6	Местное содержание в товаре потенциального поставщика, являющегося предметом проводимых закупок, которое определяется на основании оригинала или нотариально заверенной копии сертификата происхождения товара (формы СТ KZ) либо копии, заверенной государственным уполномоченным органом, выдавшим сертификат;	да/нет
7	Заявление (декларацию), подписанную первым руководителем потенциального поставщика или уполномоченным им лицом, с указанием наименования закупаемого товара, производство которого потенциальный поставщик обязуется организовать на территории Республики Казахстан до полного исполнения договора и доли местного содержания в процентном выражении в товаре. При этом потенциальный поставщик должен быть отечественным товаропроизводителем товаров, однородных с закупаемым в соответствии с представленным оригиналом или нотариально заверенной копией сертификата происхождения товара (формы СТ KZ) либо копией, заверенной государственным или иным уполномоченным органом, выдавшим сертификат. В случае применения к заявке потенциального поставщика на участие в тендере критерия, определенного настоящим подпунктом, критерии предусмотренные подпунктами 1) и 6) настоящего пункта к заявке на участие в тендере данного потенциального поставщика не применяются.	да/нет
8	Потенциальный поставщик является участником специальной экономической зоны (СЭЗ) «Парк инновационных технологий» и поставляет товары, оказывает услуги, относящиеся к приоритетным видам деятельности, соответствующим целям СЭЗ «Парк инновационных технологий» и предмету закупок в соответствии с представленной нотариально засвидетельствованной копией договора об осуществлении деятельности в качестве участника СЭЗ «Парк инновационных технологий», заключенного между управляющей компанией и участником. В случае применения к заявке потенциального поставщика на участие в тендере критерия, определенного настоящим подпунктом, критерии, предусмотренные подпунктами 1) и 3) настоящего пункта к заявке на участие в тендере данного потенциального поставщика не применяются.	да/нет

Разбивка цен оборудования и услуг

№ п/п	Описание состава поставки товара	Ед. изм.	Кол-во	Цена ед., в тенге без НДС	Итого в Тенге, без НДС

№ п/п	Описание состава поставки товара	Ед. изм.	Кол-во	Цена ед., в тенге без НДС	Итого в Тенге, без НДС
Итого Оборудования:					
Итого Услуги монтажа и пуско-наладки:					
Общая Сумма:					

In Order

P_04 Verint Israel utility room
P_06 Kazakh telecom customer office, Kazakhstan
P_08 Techno park, Turkmenistan
P_12 Cyber Gym hacker simulation facility, Israel
P_27 SORM broker office, Kazakhstan
P_37 Nice Systems offices, Israel
P_50 Ministry of Communication, Uzbekistan
P_58 Data collection centre at Kazakh telecom, Kazakhstan
P_62 Abandoned facility for gathering and processing data during the Soviet Union,Kazakhstan
P_65 View towards the monitoring centre, Uzbekistan
P_70 City square, Turkmenistan
P_75 Ashkhabad Turkmenistan

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422v 4321
www.privacyinternational.org
Twitter @privacyint

UK Registered Charity No. 1147471