Counter-Terrorism Action Plan – Russia

Purpose: Information
Submitted by: Russia

28th Counter Terrorism Task Force Meeting
Jakarta, Indonesia
29-30 January 2013
Objective: Where appropriate, to self-assess progress against APEC Leaders’ and Ministers’ counter-terrorism commitments, and to identify capacity building needs to assist the CTTF to identify priority areas for future cooperation.

## EXECUTIVE SUMMARY

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Summary of main achievements/progress in implementing Leaders and Ministers’ commitments since last update.</td>
</tr>
<tr>
<td>2.</td>
<td>Summary of forward work program to implement Leaders’ and Ministers’ commitments.</td>
</tr>
<tr>
<td>3.</td>
<td>Summary of capacity building needs and opportunities that would accelerate/strengthen the implementation of APEC Leaders’ and Ministers’ commitments by your economy and in the region.</td>
</tr>
</tbody>
</table>
### A. ENHANCING THE SECURE FLOW OF TRADE AND PEOPLE IN THE APEC REGION

#### A.1 Protect Cargo

<table>
<thead>
<tr>
<th>LEADERS’ AND MINISTERS’ COMMITMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Implement the common standards for electronic customs reporting developed by the <a href="#">World Customs Organization</a> (WCO) that provide data to target high-risk shipments and facilitate trade (2002).</td>
</tr>
<tr>
<td>- Implement as practicable as possible a container security regime that facilitates the smooth flow of trade while enhancing the integrity of containers (2002).</td>
</tr>
<tr>
<td>- Promote private-sector adoption of high standards of supply chain security, as developed by the private sector and law enforcement officials (2002).</td>
</tr>
<tr>
<td>- Work towards more consistent security measures that reduce transaction costs, and to enhance cooperation with the private sector (2007, 2011).</td>
</tr>
<tr>
<td>- Continue work on the Trade Recovery Program to work toward an operational system for ensuring trade recovery and resilience across the region in the wake of natural disasters and other major disruptions, such as terrorist attacks.</td>
</tr>
</tbody>
</table>

**MEASURES UNDERTAKEN SINCE LAST UPDATE TO IMPLEMENT COMMITMENTS**

In the Russian Federation, the security of air transport cargo delivery is ensured in accordance with the ICAO Standards and Recommended Practices, specified in Annex 17 "Security" to the Chicago Convention on International Civil Aviation and pursuant to "Pre-flight and Post-flight Inspection Rules" approved by the Order No. 104 dated 20 July 2007 of the Ministry of Transport of the Russian Federation (Chapter 9: Pre-flight inspection of cargo, mail and on-board supplies of the aircraft), as well as the federal aviation regulations described in "Aviation Security Requirements for Airports", approved by the Order No. 142 dated 28 November 2005 by the Ministry of Transport of Russia.

In the airports of the Russian Federation, the cargo, mail and in-flight supplies of an aircraft are subject to pre-flight inspection before their loading to the aircraft. For inspection, technical and special facilities are used: stationary X-ray television introsopes, portable (handheld) metal detectors, equipment for detecting explosives (detectors of vapours of explosives, stationary installations for detection of explosives) and other technical and special facilities, as well as sniffer-dogs in canine departments.

If it is impossible to inspect the content of the cargo with technical and special means, or manually (contact method), or visually, or if any information exists concerning the threat of an act of illegal intervention to the departing aircraft, the following additional measures are also used in the Russian Federation:
detention of the cargo in safe conditions before its loading on board for a period that is at least two hours longer than the expected duration of the flight of the aircraft to the destination;

− cargo test in a decompression chamber for a period equal to the estimated time of the flight of the aircraft to the destination;

− canine inspection of air cargo.

According to para 4.6.6 of the ICAO Security Manual for Safeguarding Civil Aviation against Acts of Unlawful Interference (Doc 8973), the systemic approach is also provided for implementation of aviation security measures during air-freight operations. The notions of a known consignor and a registered agent are defined.

A decision on the introduction of the regime of registered agents for ensuring aviation security in air-freight operations is made by individual States to reduce the economic costs of air cargo inspection.

Currently, selected consignors maintain records of registered agents in the Russian Federation.

According to Russian experts, the introduction of registered agents and aviation security risk assessment method for air-freight operations should be perceived only as complementary measures that do not substitute a full-scale inspection.

For the purpose of operational control of cargo by state authorities and staff of aviation security services, software products and information systems are deployed to support staff of state authorities and aviation security services with preliminary information prior to aircraft and cargo arrival to the air base, and to enable preliminary decision-making on the use of required resources, methods and means for a full cycle of prescribed activities needed for ensuring aviation security and implementation of border, customs and other control. By now, such information systems have been developed as "Prior Informing" (system informing on arriving cargo), "Dossier" (a system for registration of freighters), "Russland-Airport" (a resource management support system) and "Russland-Cargo" (an inventory control system).

Furthermore, leading Russian manufacturers of technical inspection facilities and research-and-engineering associations constantly work on development, improvement and introduction of complex systems of explosives detection, as well as complex devices for large-size cargo in the transport infrastructure facilities. One example is the inspection radiometric complex to inspect motor cars and large-size cargo, which was developed in the Russian Federation.

Taking into account the growth in transit air cargo transportation, the Russian Federation considers the issue of concluding bilateral inter-governmental agreements with certain APEC economies on recognizing aviation security measures applied to cargoes in departure airports as sufficient (similar) in order to cancel pre-flight inspections of transit cargoes in transit airports on the basis of the security declaration provided by the carrier (agent).

The pre-flight inspection and dangerous cargo transportation are carried out in line with the requirements of Annex 18 to the Chicago Convention on "Safe Transport of Dangerous Goods by Air" and "Technical Instructions for the Safe Transport of Dangerous Goods by Air" (Doc 9284 AN/905), as well as the Federal Aviation Rules entitled "Rules of Dangerous Cargo Transportation on Civil Aircraft", approved by the Order No. 141 of the Ministry of Transport of Russia dated 5 September 2008.
### LEADERS AND MINISTERS’ COMMITMENTS

- Review of the plans for ensuring the ship and port facilities security; installation of the automatic identification systems (AIS) on certain ships (2004).
- Support of the international efforts to fight piracy (2002, 2008).
- To facilitate the implementation of the International Ship and Port Facility Security Code (2004).
- Implementation of the cooperation between the APEC economies on training the specialists in the field of ensuring the ship and port facilities security in the region (2002).
- Implementation of the cooperation with the International Maritime Organization regarding technical inspection of small boats that may constitute potential threat to maritime security (2009).
- Enhancement of the ability to identify, conduct the assessment and share information on threats to transportation facilities, means of transportation, people and cargo in order to prevent and combat acts of unlawful interference (2011).

### MEASURES UNDERTAKEN SINCE LAST UPDATE TO IMPLEMENT COMMITMENTS

1. Initial compliance checkouts of the protection system were carried out in order to issue International Ship Security Certificates for 164 vessels.
2. Interim checkouts of the protection system were carried out to confirm International Ship Security Certificates for 150 vessels.
3. Checkouts were carried out to resume International Ship Security Certificates for 48 vessels.
4. 85 vulnerability assessments were carried out for transportation means of internal water transport.
5. 38 port facilities protection plans were approved.
6. Equipment of water area of 1 seaport and 1 waterworks facility with engineering and technical facilities of ensuring transport security was completed.
7. Projects for equipping with engineering and technical facilities of ensuring transport security for water area of 14 seaports were elaborated and adopted by the State Commission.
8. Equipping with engineering and technical facilities of ensuring transport security is carried out for water area of 9 seaports.
9. Safe passage was carried out by 49 trade vessels of different countries through piracy prone areas of the Gulf of Aden and the north-west of the Indian Ocean by escorting with the Russian Navy ships (September 2011 – April 2012).
### FURTHER MEASURES PLANNED TO IMPLEMENT COMMITMENTS

1. To continue carrying out the initial checkouts of protection systems on the vessels that were reacquired and whose owner/operator or flag state were changed.
2. To continue carrying out the interim checkouts on vessels.
3. To carry out checkouts in order to resume International Ship Security Certificates.
4. 23 port facilities protection plans that are under review/development are to be approved.
5. To develop projects for equipping with engineering and technical facilities of ensuring transport security for water areas of 23 seaports.
6. To equip 2 seaports with engineering and technical facilities of ensuring transport security.
7. To continue escorting trade vessels of different countries with the Russian Navy ships through piracy prone areas of the Gulf of Aden and the north-west of the Indian Ocean.
A.3  Protect International Aviation

The Operational Coordination Center was set up and is functioning within the Federal Air Transport Agency with a view to receiving and sending operational information about emergency situations and accidents related to civil aviation, including those involving acts of unlawful interference with civil aviation.

OCC is an organizational unit of the Transport Security Department which works around the clock and performs the functions of the Coordination Center on Aviation Security and Civil Aviation of the Russian Federation.

The OCC (Coordination Center on Aviation Security and Civil Aviation of the Russian Federation) contact information:
Operational Coordination Center (OCC) of the Federal Air Transport Agency.
Address: 37, Leningradsky prospect, A-167, GPS-3, Moscow, 125993, Russian Federation;
Tel.: +7 (499) 231-52-92; cell phone: +7 (916) 224-68-24;
Fax: +7 (499) 231-56-83;
E-mail: occ@scaa.ru

<table>
<thead>
<tr>
<th>LEADERS’ AND MINISTERS’ COMMITMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Introduce highly effective baggage screening procedures and relevant equipment in all APEC international airports as soon as possible; and accelerate implementation of standards for reinforced flight deck doors for passenger aircraft wherever possible (2002).</td>
</tr>
<tr>
<td>• Enhance air cargo security by promoting adoption of the guidelines developed by the ICAO (2002).</td>
</tr>
<tr>
<td>• Examine emerging approaches to air cargo security; share information on efficient screening technologies and training; and harmonise aviation security measures (2009).</td>
</tr>
<tr>
<td>• Adopt strict domestic export controls on Man-Portable Air Defense Systems (MANPADS); secure stockpiles; regulate production, transfer, and brokering; ban transfers to non-state end-users; and exchange information in support of these efforts (2003).</td>
</tr>
<tr>
<td>• APEC economies which did not do so before 2007 to conduct one MANPADS’ assessment of a major international airport using the MANPADS’ Vulnerability Assessment (MVA) guide established by the ICAO or similar international guidelines (2005).</td>
</tr>
<tr>
<td>• Work towards continuous improvement of aviation security oversight and quality control (2009).</td>
</tr>
<tr>
<td>• Implement effective capacity building programs for air cargo and air traveller protection, which help develop institutions and mobilize expertise and resources efficiently (2010).</td>
</tr>
</tbody>
</table>
### MEASURES UNDERTAKEN SINCE LAST UPDATE TO IMPLEMENT COMMITMENTS

At the international airports and airports of federal significance of the Russian Federation, canine units are being created to detect explosive substances.

Airport check-points are being equipped with automated control and staff access management systems. Transport check-points are being equipped with means for stopping motor vehicles by force.

The Moscow hub airports are obliged to use a three-tier system of pre-flight luggage inspection:

- **Tier one** implies that 100 per cent of luggage is screened using high-speed X-ray television introsopes with automated (unmanned) explosives detection capabilities;
- **Tier two** implies that suspicious luggage not admitted to the secure area after tier one is inspected using computer tomography scanners or other equipment ensuring reliable detection of explosive substances;
- **Tier three** implies that luggage not admitted to the secure area after tier two is inspected manually. Manual inspection is carried out in the presence of the passenger, a police officer and an explosives expert.

At the moment, newly opened international airport complexes in the Russian Federation have multi-tier automated luggage processing and inspection systems.

At the airport entrances there are passengers, hand-luggage and hold-luggage inspection points equipped with X-ray television introsopes, as well as stationary and hand-held metal detectors. Hundred per cent of the airport visitors is inspected.

A pre-flight inspection includes the following activities:

- **a)** application of technical means and various physical (X-ray, gas analysis, nuclear quadruple resonance, neutron, etc.) methods for detecting explosive substances and explosive devices on bodies and in clothing, hand-luggage or hold-luggage of passengers;
- **b)** inspection of passengers’ outerwear, headwear, footwear (except for footwear with heels less than 2.5 cm and sole thinner than 1 cm) and waist belts (if they are wider than 4 cm or thicker than 0.5 cm) by means of X-ray television introsopes;
- **c)** personal, manual (contact) inspection of passengers in places of potential concealment of explosive devices or screening with a graphic-image X-ray scanner as an alternative to manual (contact) inspection;
- **d)** psychological testing of passengers.

In addition, the inspection means of a number of airports are undergoing modernization with a view to installing high-speed X-ray television introsopes with the function of automated detection of explosives, as well as computer tomography systems.

In the Russian Federation, aviation personnel and aviation security services staff are trained in conformity with the ICAO Standards and Recommended Practices, as well as the Russian legislation and according to the four consecutive levels: basic training, special training, professional training and advanced training. Special training software is used.
**Luggage inspections**

In the Russian Federation, luggage inspections are carried out in accordance with the Pre-flight and Post-flight Inspection Rules approved by Order No. 104 of the Ministry of Transport of Russia of 20 July 2007.

In compliance with the Federal aviation regulations set out in the Aviation Security Requirements for Airports approved by Order No. 142 of the Ministry of Transport of Russia of 28 November 2005, international airports are equipped with multi-tier automated pre-flight luggage inspection systems.

At the airport entrances there are passengers, hand-luggage and hold-luggage inspection points equipped with X-ray television intscopes, stationary metal detectors and video surveillance systems.

As of January 2011, hundred per cent of the international airport visitors are inspected.

At the airports, canine units are used to inspect hand-luggage, hold-luggage and cargoes.

Order No. 96 of the Ministry of Transport of Russia of 16 April 20012 amended the Pre-flight and Post-flight Inspection Rules approved by Order No. 104 of the Ministry of Transport of Russia of 20 July 2007, stipulating that footwear with heels less than 2.5 cm and sole thinner than 1 cm and waist belts less than 4 cm wide and 0.5 cm thick are not subject to inspection by means of X-ray television intscopes.

**Aviation security equipment installed in aircraft**

In accordance with paragraph 4 of the Aviation Security Standards, Rules and Procedures annexed to Regulation No. 897 of the Government of the Russian Federation of 30 July 1994 on *the Federal system for ensuring protection of civil aviation activities from acts of unlawful interference*, aircraft with a maximum certified take-off mass exceeding 45,500 kg or passenger capacity of more than 60 people are equipped with:

– bullet-proof doors which can be securely locked and unlocked from each pilot’s seat and partitions isolating pilot cockpit from passenger cabin;

– special signalling devices and intercoms for communication between flight crew members and stewards (flight attendants);

In compliance with the ICAO Standards and Recommended Practices and paragraph 4 of the Aviation Security Standards, Rules and Procedures annexed to Regulation No. 897 of the Government of the Russian Federation of 30 July 1994, the majority of aircraft of the major Russian air carriers are equipped with television surveillance systems for observing the entire door adjacent area outside the pilot cockpit from each pilot’s seat.

Order No. 1285-p of the Government of the Russian Federation of 30 July 2010 approved the Complex program to ensure public transport security, which provides for carrying out research and development activities aimed at equipping the TU-204 aircraft with audio and video surveillance systems using radio and data transmission channels, including satellite channels.
**Efforts to facilitate mandatory aviation security audits, conducted by the International Civil Aviation Organization (ICAO)**

From 28 August to 6 September 2006 the Russian Federation was audited by the ICAO aviation security commission in the context of the first cycle of the ICAO Universal Security Audit Programme (USAP), and later, in June 2008, the ICAO auditor monitored the adequacy of measures taken by the Russian Federation to fulfill the recommendations made by the ICAO commission in 2006. The ICAO auditor praised the preparedness of the Russian Federation for the audit and noted the considerable work done to fulfill the ICAO recommendations.

In March 2011 the Russian Federation was audited by the ICAO experts in the context of the second cycle of the USAP. After the audit the ICAO commission reported that the Russian Federation had developed and launched an effective aviation security oversight and monitoring system. Experts indicated high standards of aviation security oversight and monitoring activities in the Russian Federation, comprehensiveness and good quality of elaborated regulatory legal acts, as well as documentation on airports and airlines quality control.

By the ICAO criteria, the general aviation security oversight rate in the Russian Federation is about 97 per cent, while the world average rates are 65-70 per cent (initial outcomes of the second cycle of the ICAO audits).

Nowadays the Russian Federation is elaborating the project of the plan of actions to fulfill the ICAO audit group recommendations.

The Russian Federation also supports the ICAO USAP sending certified professionals who have done an ICAO audit course to make an audit of other States in the framework of the USAP within an ICAO audit group.

**Measures for ensuring safe transportation of air cargoes**


In the airports of the Russian Federation cargoes, mail and on-board supplies of the aircraft are not taken aboard without a pre-flight inspection. Inspections are carried out using technical and special facilities, such as stationary X-ray television introscopes, portable (handheld) metal detectors, explosives detectors (detectors of fumes from explosives and stationary detectors of explosives) and other technical and special facilities, as well as sniffer-dogs from canine units.

Additional measures, taken in the Russian Federation when the contents of a cargo cannot be inspected using technical or special facilities or by hand (contact method), or by eye, or when the departing aircraft is reported to be under threat of unlawful interference, are the following:

- detention of the cargo in safe conditions before its loading on board for a period that is at least two hours longer than the expected duration of the flight of the aircraft to the destination;
- the cargo test in a decompression chamber for a period equal to the estimated time of the flight of the aircraft to the destination.
The work is being done to create technical means of oversized cargo screening as well as to improve complex explosives detection systems.

**Aviation security oversight and quality control system in the Russian Federation**

According to the requirements of Article 48, paragraph 4 of Federal Law No. 60-FZ of March 19, 1997 "Aviation Code of the Russian Federation", state control over the compliance of airports and aerodromes with the relevant requirements is exercised by the competent authority appropriately vested with the power to arrange and carry out mandatory certification procedures for civil aerodromes and airports.

In accordance with paragraph 9 of the Civil Aviation Security Quality Control Programme of the Russian Federation, approved by Order No. 72 of the Russian Ministry of Transport on March 5, 2011, the Ministry of Transport of the Russian Federation, the Federal Air Transport Agency, the Federal Transport Oversight Service in cooperation with relevant federal executive bodies, within their competence and in compliance with the legislation of the Russian Federation, exercise quality control over the execution of activities aimed at protecting civil aviation against acts of unlawful interference.

According to the requirements of Article 28 of the Aviation Code of the Russian Federation the state control (supervision) over activities of bodies corporate and individual entrepreneurs in the field of civil aviation security is carried out by the Federal Transport Oversight Service in accordance with the Decision No. 409 of the Government of the Russian Federation on June 9, 2010 “On the Exercise by Officials of the Federal Service for Supervision over Transport of Control (Supervisory) Functions” by way of routine and unscheduled inspections.

According to Federal Law No. 294-FZ of December 26, 2008 "On the Protection of Bodies Corporate and Individual Entrepreneurs Rights during State Control (Supervision) and Municipal Control", inspections are carried out by the Federal Transport Oversight Service and its regional bodies.

Supervisory control over the compliance of aviation security measures with the requirements of the legislation of the Russian Federation regarding aviation security of bodies corporate responsible for aviation security, is carried out in accordance with federal aviation regulations. Supervisory control is exercised by the Federal Air Transport Agency or its regional bodies during the conformity certificate's validity period by way of routine (no less than once a year) and unscheduled inspections.

Routine supervisory control timeline is set by the Federal Air Transport Agency or its relevant regional body.

The Federal Air Transport Agency or its relevant regional body makes the decision about carrying out unscheduled supervisory control.

In accordance with paragraph 17 of the Civil Aviation Security Quality Control Programme of the Russian Federation, approved by Order No. 72 of the Russian Ministry of Transport on March 5, 2011, heads of airports (aerodromes), airlines and operators and other bodies corporate performing activities in civil aviation are responsible for:

- development and implementation of an internal aviation security quality control system complying with the requirements of this Programme, as well as norms, regulations and procedures concerning aviation security;
- appointment of responsible persons in charge of aviation security quality control, definition of their area of responsibility in carrying out internal quality control;
- analysis and synthesis of the data related to aviation security quality control and coordination of efforts aimed at improving;
– approval of security systems test plans and participation in performing them.

Internal inspection (audit) of aviation security quality control is arranged by the heads of airports, airlines and operators with reference to the programme of internal quality control in the area of aviation security and in accordance with the annual aviation security quality control inspection plan (paragraph 31).

In order to efficiently carry out activities aimed at implementing the set of measures provided for by the federal aviation security system and to take corrective actions, federal executive bodies collect and analyze information at the end of the inspections, as appropriate. An annual synthesis report should be compiled (paragraph 36).
A.4 Protect People in Transit

<table>
<thead>
<tr>
<th>LEADERS’ AND MINISTERS’ COMMITMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Implement as expeditiously as possible an Advance Passenger Information (API) system for the collection and transmission of advance passenger information (2002).</td>
</tr>
<tr>
<td>• Consider joining the Regional Movement Alert System (RMAS) (2006).</td>
</tr>
<tr>
<td>• Adopt and implement the agreed standards for machine readable travel documents, and use biometrics in entry and (where applicable) exit procedures and travel documents consistent with ICAO and the International Standards Organization (2002).</td>
</tr>
<tr>
<td>• Assure the highest possible integrity of all government officials who are involved in border operations (2002).</td>
</tr>
<tr>
<td>• Develop a standardized strategic safety and security master plan for tourists, a crisis management model, and promote the development by industry of simple-to-use safety and security measures for tourism businesses (2002).</td>
</tr>
<tr>
<td>• Voluntarily provide information on lost and stolen travel documents to the existing database of the International Criminal and Police Organization (ICPO-Interpol) on a best endeavours basis (2005).</td>
</tr>
<tr>
<td>• Implement APEC Travel Facilitation Initiative to facilitate regional international travel, while ensuring the security of the overall travel system. (2011).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MEASURES UNDERTAKEN SINCE LAST UPDATE TO IMPLEMENT COMMITMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Implement a system for the collection and transmission of advance passenger information</strong></td>
</tr>
<tr>
<td>Pursuant to paragraph 1 of Article 85.1 on Personal Data on Air Passengers of the Aviation Code of the Russian Federation of March 19, 1997, No. 60-FZ, in order to guarantee aviation security the air businesses shall ensure transfer of personal data on air passengers to automatic centralized bases of passenger personal data in accordance with the legislation of the Russian Federation on transport security and legislation of the Russian Federation on personal data during international flights, as well as to the authorized institutions of foreign States in accordance with the international treaties of the Russian Federation or the legislation of foreign States of departure, destination or transit in the amount provided by the legislation of the Russian Federation.</td>
</tr>
<tr>
<td>In order to fulfill the requirements of its Federal Law No. 16-FZ on Transport Security of February 9, 2007, the Russian Federation is currently creating a single state information system of transport security (SSIS TS). The key element of the SSIS TS is a single centralized automated base of passenger personal data that will incorporate all the databases of Russian and foreign airline businesses flying to the territory of the Russian Federation.</td>
</tr>
<tr>
<td>At present, the Order No. 1285-r of the Government of the Russian Federation of July 30, 2010 has established a Comprehensive Programme to Ensure Security for Population on Transport envisaging the creation of the SSIS TS.</td>
</tr>
</tbody>
</table>
| Pursuant to paragraph 2 of Article 85.1 of the Aviation Code of the Russian Federation the procedure of transfer of personal data on air passengers shall be determined by the Russian Government. The indicated procedure involves cooperation of competent bodies of the Russian
Federation in the exchange and use of this information. The information contained in the indicated database is planned to be included into a single international base of passenger personal data.

Russian air travel companies transfer advanced information on passengers in APIS (Advanced Passenger Information System) to 18 States, including the USA, Canada, South Korea, the UK, Germany, Japan, Spain, the Czech Republic, and Hungary.

Passenger information will be transferred to the international base of passenger personal data.

**Use machine readable travel documents.**

The Russian Federation has implemented a package of measures to adopt and implement procedures for the use of machine readable travel documents.

Travel documents fully conform to the requirements of ICAO Doc 9303 on machine readable travel documents.
A.5 Combating threats to security

**LEADERS AND MINISTERS’ COMMITMENTS**

- Eliminate the severe and growing danger posed by the proliferation of weapons of mass destruction and their means of delivery by strengthening non-proliferation regimes and adopting and enforcing efficient export control measures (2003, 2004, 2005, 2006); take appropriate individual and joint measures to protect legitimate financial and commercial system from abuse (2006).
- Ensure that any counter-terrorism measures comply with all relevant obligations under international law, in particular international human rights, refugee and humanitarian law (2005).
- Relevant APEC economies to take steps towards ratification and implementation of, or undertaking commitment to ratify all basic universal antiterrorist conventions (2004, 2008).
- Increase and enhance coordination of counter-terrorism activities where appropriate through effective collaboration, technical assistance and capacity building, as well as cooperation between APEC Counter-Terrorism Task Force and relevant international, regional and functional organizations (2003) in accordance with the corresponding APEC rules and practices.
- Continue efforts and cooperation to defend food supply from terrorist threat in accordance with the APEC voluntary Food Defense Principles (2007).
- Implement the APEC Consolidated Counter-Terrorism and Secure Trade Strategy aimed at increasing the security level, efficiency and sustainability of trading transactions and movement of physical persons in the region (2011).

**MEASURES UNDERTAKEN SINCE LAST UPDATE TO IMPLEMENT COMMITMENTS**


As a result of measures taken in the Russian Federation in 2011, the number of registered extremist crimes declined to 622 (in 2011 – 656). The number of registered violent extremist crimes has plunged even more significantly, including murders committed on grounds of extremism has declined by 72.2%, intentional infliction of bodily harm, battery, torture and threat of homicide on the same grounds – by 16.3%.

In 2011, in a number of regions the activity of more than ten separate radical nationalist groups that committed grave crimes on the grounds of nation, race or religion was precluded.

The Federal List of Extremist Materials contains more than 1000 materials included on the resolution of judicial authorities, 235 of them have been included into the abovementioned list in 2011.
Responding to contemporary challenges and threats the high-level officials of the country, uppermost the President, the Government and the Federal Assembly of the Russian Federation keep taking legislative, organizational, operational and preventive measures aimed at counteracting the destructive activity of terrorist and extremist entities, their leaders and ideologists.

Virtually in all the regions, law-enforcement coordination councils have been created and, under each head of subordinate entity, working groups for interethnical communication harmonization operate.

In order to enhance coordination of State authorities of all levels there have been involved the resources of the Interagency Commission of the Russian Federation on Counteracting Extremist Activities established in accordance with the Decree No. 988 of 26 July 2011 of the President of the Russian Federation.

Last year, the Commission did an important job, it held one organizational meeting and eight visiting missions to all federal districts of the countries in which civil society, mass-media, clergy, science and education representatives took part.

In its work, the Commission focuses its attention on prevention of extremism manifestations, improvement of the existing legislation taking into consideration the necessity to guarantee stable and harmonized relations within different social groups.

In March 2012, there was held a regular meeting of the Commission, and in April, a Russian-wide conference – a seminar for heads of counter-extremism units of territorial bodies of the Ministry of the Interior of Russia where the existing problems of operative activity and duty and prospects of further work in the area were discussed.

Russian law-enforcement authorities keep actively applying foreign experience of counteracting extremism and terrorism. Relations with corresponding international organizations, including regional ones, are being strengthened.

Building-up cooperation with foreign partners on the platform of the Global Counterterrorism Forum (GCTF) inaugurated in September 2011 is considered promising. In April 2012, the Russian inter-agency delegation took part in a constituent meeting of the GCTF Working Group on Countering Violent Extremism (Abu Dhabi, UAE).
B. HALTING TERRORIST FINANCING:

Contact Person: Alexander Klimchenok  
Title: State-Secretary – Rosfinmonitoring Deputy Head

Telephone Number: (495) 627 33 68  Email Address: info@fedsfm.ru

<table>
<thead>
<tr>
<th>LEADERS’ AND MINISTERS’ COMMITMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Enhance law enforcement and regulatory capabilities by establishing or identifying a financial intelligence unit (FIU) in each member economy, and enhancing information sharing with other FIUs (2002).</td>
</tr>
<tr>
<td>• Relevant economies to implement UN and other international instruments (2002).</td>
</tr>
<tr>
<td>• Implement, where applicable, the FATF’s Special Recommendations on terrorist financing, including those relating to non-profit organizations, alternative remittance systems and illicit cash couriers (2002, 2008).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MEASURES UNDERTAKEN SINCE LAST UPDATE TO IMPLEMENT COMMITMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>While developing legal framework related to terrorist financing, the Russian Federation has extended its &quot;National strategy on combating legalization (laundering) of criminally gained income and financing of terrorism&quot; for 2011-2012. At the same time, the Russian Federation is drafting a strategic plan for the national system on combating legalization (laundering) of criminally gained income and financing of terrorism up to 2020.</td>
</tr>
<tr>
<td>In the part related to gaps in criminalization of the terrorist financing (FATF special recommendation IV), such gaps have been removed by the Federal Law No.197-FZ of July 27, 2010 on the Amendments to Certain Legislative Acts of the Russian Federation in the area of combating legalization (laundering) of criminally gained income and financing of terrorism. The Federal Law stipulates that financing of crimes, related to illegal handling of nuclear materials, is considered to be terrorist financing (Articles 220, 221 of the Criminal Code).</td>
</tr>
<tr>
<td>The Rosfinmonitoring Order No.103 dated May 8, 2009 on Adoption of recommendations for developing criteria for detecting and identifying signs of unusual transactions is designed to significantly enhance the effectiveness of the system.</td>
</tr>
<tr>
<td>Moreover, the Rosfinmonitoring Order No.43 dated February 14, 2012 has significantly expanded the list of criteria and signs of unusual transactions (deals) in the part related to terrorist financing contained in the Recommendations on developing criteria for detecting and identifying signs of unusual transactions adopted by the Rosfinmonitoring Order No.103 dated May 8, 2009. At the same time, the list of criteria and signs in the part related to terrorist financing is not exhaustive but contains a special reference for institutions to include other criteria/signs at their own discretion.</td>
</tr>
<tr>
<td>Obligation of notifying institutions to draft and send notifications about suspicious transactions related to terrorist financing is contained in the Federal Law No.115-FZ dated August 7, 2001 on Combating legalization (laundering) of criminally gained income and financing of terrorism, Article 7, part 2, 3 and 10.</td>
</tr>
<tr>
<td>Information Letter No.17 dated August 2, 2011 also describes signs of transactions, types and conditions of clients’ activities, which bear...</td>
</tr>
</tbody>
</table>
a high risk of being made for the purposes of terrorist financing. Otherwise, if transactions (deals) or clients’ activities are considered to be of high risk, the institution focuses on operations (deals) carried out by this client, in order to detect suspicious and unusual transactions and provide Rosfinmonitoring with information on such transactions.

The Annex to the "General Requirements to the Rules of Internal Control of Credit Organizations to Combat Legalization (Laundering) of Criminally Gained Income and Financing of Terrorism" No. 375-II dated March 2, 2012 has a special list of signs of possible financing of terrorism, according to which the Rosfinmonitoring is provided with information on transactions.

In addition to the above mentioned, the Rosfinmonitoring activities to prepare the list of organizations and individuals who are reported of complicity in extremist activities or terrorism (hereinafter the List), and submission of this List to organizations, which carry out transactions with funds and other assets, remain one of the key elements of functioning of the system on combating the terrorist financing.

Explanation on the Modus Operandi of the List and notifications of the Rosfinmonitoring take place on a permanent basis.

In 2011, from organizations that carry out transactions with funds and other assets, there have been received and studied 1258 notifications on involvement of the players from the List with identification code 7001 (mandatory control). Upon daily processing of notifications, there have been sent 379 information letters to relevant law enforcement authorities, 9 transactions with involvement of persons from the List detected and suspended by Rosfinmonitoring, 9 decisions on suspension of transactions with funds and other assets issued. Under identification code 6001 and additional identification code on the signs of unusual transactions 401 (suspicion of terrorist financing), there have been received and studied 2566 notifications from organizations, which carry out transactions with funds and other assets.

Under legalization of the procedure of exclusion from the List of those who have been acquitted or absolved and justified, Rosfinmonitoring has amended the basic law on combating legalization (laundering) of criminally gained income and financing of terrorism in the part concerning the inclusion of grounds for exclusion from the List (the Federal Law No.197-FZ of July 27, 2010 on the Amendments to Certain Legislative Acts of the Russian Federation in the area of combating legalization (laundering) of criminally gained income and financing of terrorism, entered into force on November 20, 2010).

The Decree of the Government of the Russian Federation No. 211 dated March 24, 2011, on Amendments to the Decree of the Government of the Russian Federation No. 27 dated January 18, 2003, on Approval of the provision on the procedure of identification of the list of organizations and individuals, in respect of which there is evidence of their complicity in extremist activities, and provision of such information to the organizations, which carry out transactions with funds and other assets, identifies the procedure for amending the List (the document has entered into force since July 1, 2011). In 2011, 493 individuals and one legal entity have been already excluded from the List.

Rosfinmonitoring has considered the issue of introduction of additional mechanisms of "freezing" funds with involvement of individuals from the List. Rosfinmonitoring’s proposals were reflected in the Federal Law No.162-FZ dated June 27, 2011 on Amending some Russian laws in connection with adoption of the Federal Law No.161-FZ dated June 27, 2011 on the National payment system, which envisages relevant amendments to the Federal Law No.115-FZ dated August 7, 2001 on Combating legalization (laundering) of criminally gained income and financing of terrorism. In particular, it envisages freezing of funds upon courts decision, which is cancelled upon request of Rosfinmonitoring in accordance with the established procedure, or an administrative freeze up to 30 days.
Moreover, the adoption of the Federal Law No.161-FZ dated June 27, 2011 on the National payment system promoted the creation of a legal regulatory basis for transactions with the use of electronic money.

Rosfinmonitoring, in cooperation with the concerned ministries and institutions, considered the issue of transition from monitoring of certain transactions, carried out by individuals and legal entities, in respect of which there is evidence of their complicity in extremist or terrorist activities, to monitoring of their accounts and accounts of organizations and individuals who are related to them.

On the basis of Rosfinmonitoring’s proposals, some amendments were made to the Federal Law No.308-FZ dated November 8, 2011 on Amendments to the Federal Law dated August 7, 2001 on Combating legalization (laundering) of criminally gained income and financing of terrorism, which expands Rosfinmonitoring’s powers to request additional information about clients’ transactions, including flow of funds in their accounts (deposits), from organizations, which carry out transactions with funds and other assets. In this connection, the organizations are obliged to provide such information. The Government of the Russian Federation has defined the procedure of sending written requests by Rosfinmonitoring through its Decree No.375 dated April 23, 2012 on Amendments to the Decree of the Government of the Russian Federation No.245 dated April 17, 2012.

Within the Customs Union, the Russian Federation signed the Treaty on combating legalization (laundering) of criminally gained income and financing of terrorism while transporting the currency and (or) monetary instruments across the customs frontier of the Customs Union, which has the capacity to stop the transmission of the currency and (or) monetary instruments across the customs frontier of the Customs Union, if there is suspicion that such currency and (or) monetary instruments can be used for the purposes of terrorist financing.

The Rosfinmonitoring Order No.103 dated May 8, 2009 on Adoption of recommendations for developing criteria for detecting and identifying signs of unusual transactions is designed to significantly enhance the effectiveness of the system.
Measures undertaken within the Customs Union to address the shortcomings identified by the FATF experts

In order to implement the FATF special recommendation IX, the bodies and agencies of the Russian Federation and the Member States of the Customs Union have taken the following measures:

a) The Customs Code of the Customs Union authorized the customs bodies to take measures within their competence to combat legalization (laundering) of criminally gained income and financing of terrorism while supervising the transmission of the Customs Union Member States’ currency, securities and (or) currency values and traveller's checks across the customs boundary.

b) The Treaty No. 51 of July 5, 2010 on the procedure of transportation of currency and (or) monetary instruments across the customs frontier of the Customs Union by natural persons (hereinafter referred to as "the Treaty"), according to which in order to combat legalization (laundering) of criminally gained income and financing of terrorism it is required to submit information in the passengers customs declaration on the natural person transporting currency and monetary instruments, the source of currency and (or) monetary instruments and their owners, as well as their assumed usage, itinerary and way of conveyance of currency and (or) monetary instruments, has been developed and adopted by the Decision of the Interstate Council of the Eurasian Economic Society.

c) Within the process of creation of the Customs Union, the form of the passenger customs declaration and the form filling procedure have been affirmed by the Decision No. 287 of June 18, 2010 of the Customs Union Commission. As stipulated by this legal act, in case of transporting currency and travel checks in the amount exceeding the equivalent of 10 thousand USD across the customs frontier of the Customs Union, declarant shall fill in the additional Currency Declaration Form of the passenger customs declaration where in accordance with the requirements of Article 6 of the Treaty the additional information envisaged by the Treaty is provided.

The new form of the passenger customs declaration has been introduced since June 1, 2010.

In addition, the Treaty on combating legalization (laundering) of criminally gained income and financing of terrorism while transporting the currency and (or) monetary instruments across the customs frontier of the Customs Union was signed at the meeting of the Supreme Eurasian Economic Council at the level of heads of State in December 2011.

The Treaty legally authorized the customs bodies to suspend currency and monetary instruments in case the law enforcement or financial monitoring agencies report that transported currency and (or) monetary instruments are related to legalization of criminally gained income or financing of terrorism.

Measures undertaken to implement the FATF special recommendation IX

a) The Federal Law on the Customs Regulation in the Russian Federation No. 311-FZ of November 27, 2010 envisages giving to the customs bodies of the Russian Federation the function of providing, in accordance with the international treaty of the Customs Union Member-States, measures for combating legalization (laundering) of criminally gained income and financing of terrorism while supervising the transmission of the Customs Union Member States’ currency, securities and (or) currency values and traveller's checks across the customs frontier of the Customs Union.

b) The General Prosecutor’s Office of the Russian Federation, the Ministry of the Interior of Russia, the Federal Security Service of Russia, the Federal Drug Control Service of Russia, the Federal Customs Service of Russia, the Investigative Committee and Rosfinmonitoring...
have issued a Joint Decree No. 309/566/378/318/1460/43/207 of August 5, 2010 approving the Instruction on information exchange related to combating legalization (laundering) of monetary funds and other assets obtained by criminal means. This Instruction establishes a unified procedure for information exchange between the law enforcement agencies and Rosfinmonitoring to prevent, detect, suppress, solve and investigate crimes related to legalization (laundering) of funds and other assets, as well as predicate crimes, i.e. crimes preceding legalization of currency and other property;

   c) Information on the transportation of currency and monetary instruments within the framework of statistical reporting is being collected.

   In accordance with the Agreement No. 01-08/12 and No. 01-1-13/1 of April 20, 2007 on cooperation between the FCS of Russia and Rosfinmonitoring in the field of information exchange, the FSC of Russia provides monthly information to the financial intelligence units on the natural persons transporting large amounts of currency and monetary instruments.

   Information on natural persons transporting large amounts of currency and monetary instruments is also provided to the Federal Security Service of Russia, the Ministry of the Interior of Russia and the Federal Drug Control Service of Russia.

   d) Draft model Agreement on cooperation between the Federal Customs Service and respective agencies in the countries of contracting Parties in the field of exchange of information on combating legalization (laundering) of criminally gained income and financing of terrorism has been worked out.

   The subject of the Agreement is the cooperation of the Parties in the field of information exchange necessary for the adoption of measures to combat legalization (laundering) of criminally gained income, financing of terrorism and related criminal activity while transporting currency and (or) monetary instruments across the border by natural persons.

   e) The additional section on Compliance with the Requirements of the FATF Special Recommendation IX has been included in the education program of the Institute of Additional Professional Education, Retraining and Training of the Russian Customs Academy and the Institute of Law Enforcement Activity. The introduction of the mentioned section to the education program will contribute to improving professional knowledge of the customs bodies' officials.

   f) Additional data on the source, owner or assumed usage of currency, as well as monetary instruments details were included in the statistical reporting form No.1 - "gross", "Information on bringing currency and (or) monetary instruments by natural persons in or out of the country", which served to improve statistical control over the transportation of currency and (or) monetary instruments across the customs frontier of the Russian Federation. Provision of additional data in the statistical reporting form also facilitated prompt preparation and submission of analytical materials to the interested FSC units, as well as the information on requests of the law enforcement agencies and financial intelligence units.

   Measures undertaken within the Customs Union of the FCS of Russia to implement the FATF special recommendation IX

   In order to implement the Treaty on combating legalization (laundering) of criminally gained income and financing of terrorism while transporting the currency and (or) monetary instruments across the customs frontier of the Customs Union, the following measures have been taken:
a) The JEC draft decision approving the form of the act on suspending transmission of currency and (or) monetary instruments across the customs frontier of the Customs Union has been agreed with the interested ministries and agencies of the Russian Federation and sent to the Joint Economic Commission.

At the present time, the draft form of the act finalized on the basis of observations and proposals of the ministries and agencies of the Russian Federation, as well as Belarus and Kazakhstan has been submitted for a second round of consultations;

b) The proposal on the need to create a common database on the transportation of currency and (or) monetary instruments within the Customs Union by natural persons has been submitted to the Joint Economic Commission.

c) The proposals on the information exchange among the law enforcement agencies, authorized bodies and (or) customs bodies of the Parties within the Treaty on combating legalization (laundering) of criminally gained income and financing of terrorism while transporting the currency and (or) monetary instruments across the customs frontier of the Customs Union have been prepared and submitted to Rosfinmonitoring.

The FCS of Russia has taken the following additional measures

a) There has been prepared a draft order of the FSC of Russia approving the Instruction on the procedure for taking by the officials of the customs bodies a deposit of currency and monetary instruments which have been suspended.

b) In order to implement the FATF special recommendation IX it is planned to submit proposals to Rosfinmonitoring on the introduction of proportional and dissuasive sanctions with regard to persons making invalid declaration of currency and monetary instruments in order to implement a draft work plan of the Interdepartmental commission on combating legalization (laundering) of criminally gained income and financing of terrorism for 2012.

c) Besides, pursuant to the Order of the President of the Russian Federation of January 9, 2012 No. Pr-65, there has been established the Interdepartmental Working Group on Detection and Suppression of Illegal Financial Operations, consisting of the representatives of the Ministry of the Interior of Russia, the Federal Security Service of Russia, the Federal Tax Service of Russia, the Federal Customs Service of Russia, the Federal Drug Control Service of Russia, Rosfinmonitoring, Federal Service for Financial Markets of Russia, the General Prosecutor’s Office of Russia, the Investigative Committee of the Russian Federation, the Bank of Russia, as well as the Central Office of the Government of the Russian Federation.

The task of this Working Group is to coordinate the joint efforts of its agencies to eliminate the established schemes of income concealment and the shadow turnover of financial resources used by a number of companies, banks and professional mediators.
C. STRENGTHENING CYBER SECURITY

Contact Point: Oleg Rybakov
Title: Senior Specialist-Expert, Information Security Division, Department for the Creation and Development of Information Society, Russian Ministry of Communications and Mass Media
Telephone Number: (495) 771-89-30

LEADERS’ AND MINISTERS’ COMMITMENTS

- Countering terrorism by implementing and enhancing critical information infrastructure protection and cyber security to ensure a trusted, secure and sustainable online environment (2002).
- Enhance mutual cooperation on countering malicious online activities and engage in efforts to increase cyber security awareness (2010).

MEASURES UNDERTAKEN SINCE LAST UPDATE TO IMPLEMENT COMMITMENTS


This document specifies the main areas, principles, mechanisms and stages of the state policy in the sphere of ensuring security of automated management systems at the critical infrastructure facilities as well as the factors affecting its development.

For the purpose of a better understanding of modern threats and of searching for cooperative measures to combat them, the Russian Federation actively promotes the initiatives to raise the issue of ensuring international comprehensive information security at international level. This issue has been firmly anchored in the agenda of many international organizations, primarily of the UN, OSCE, SCO, CIS, Council of Europe, G8 and International Telecommunication Union. The purpose of Russian initiatives is to prevent the use of cyber technologies against security interests of the States.

Russian approaches to this issue are set forth in the following documents.

1. “The Rules of Conduct for International Information Security” jointly worked out by the representatives of the People’s Republic of China, the Russian Federation, Tajikistan and Uzbekistan (the SCO Member States) and submitted at the 66th session of the UN General Assembly.

The States that have acceded to the Rules assume the following commitments:

- To cooperate in the fight against criminal and terrorist activity which uses information and communication technologies, including nets, and to suppress the dissemination of terrorist, extremist and separatist information as well as undermining political, economic and social stability of the States, their cultural and spiritual patterns;
- To fully respect rights and freedoms in the information space, including those to seek, obtain, transfer and disseminate information in accordance with national legislation of each State;
- To contribute to a profound understanding by all social elements, including through state-private partnership in information and communication technologies, of their responsibility to ensure information security, in particular to build the culture of information security and to support the efforts aimed at protecting critical information infrastructure facilities.

The proposed Concept offers a basis for working out a universal convention under the aegis of the UN, which will allow to unite the efforts of the international community in this area.

The purpose of this document is to oppose the use of information and communication technologies for violating international peace and security. Under its provisions, the Member States undertake to cooperate with each other in the sphere of international information security for maintaining international peace and security and promoting international economic stability and progress, general well-being of peoples and international cooperation free of discrimination.

As the basic measures taken by the Member States to prevent offences in the information space, the Concept has determined the following ones:

- the use of efficient, commensurate and convincing punitive measures against those who have committed offences in the information space;
- establishment, execution and application of powers and procedures for the purpose of conducting specific criminal investigations or prosecute criminalized socially dangerous acts in the information space in accordance with the conditions and safeguards specified by the law of a Member State and providing adequate protection of human rights and freedoms, as well as with the proportionality principle;
- adoption of legislative or other measures needed to guarantee that sufficient volume of data on information flows, which will allow to identify service providers and the way by which a certain message has been transmitted in the information space, is supplied to the competent authorities of a Member State or to a person appointed by these authorities.

The main point of the Concept is to fully maintain the state sovereignty and national regulatory boundaries, including in the cyberspace.

The necessity of national efforts to build, promote and actively inculcate a sustainable global culture of cyber security repeatedly been indicated in international acts. The relevancy of the States’ activity to build a culture of cyber security is stated in the resolutions of the UN General Assembly – “Creation of a Global Culture of Cyber Security” dated 2002 and “Creation of a Global Culture of Cyber Security and the Protection of Critical Information Infrastructures” dated 2003, as well as in the provisions of the Declaration of Principles “Building the Information Society: A Global Challenge in the New Millennium” adopted on December 12, 2003. The resolution “Creation of a Global Culture of Cyber Security and Taking Stock of National Efforts to Protect Critical Information Infrastructures” was adopted at the session of the UN General Assembly in 2010.

The elaboration of draft guidelines for the state policy aimed at building the culture of information security of the citizens has become a result of the work of the Russian Federation in this field.

The draft defines the main areas, purposes, goals and principles of the state policy aimed at building the citizens’ culture of information security as well as the priority measures for its implementation.
**FURTHER MEASURES PLANNED TO IMPLEMENT COMMITMENTS**

The Russian Federation has been consistent in promoting the initiative to work out a universal convention under the UN aegis to combat information crime. This idea is reflected, in particular, in the final declaration of the 12th UN Congress on Crime Prevention and Criminal Justice (Brazil, 2010).

Russia proceeds from the need of an early completion of the comprehensive cybercrime study carried out under the aegis of the UN Office on Drugs and Crime and expects to work on equal terms with the APEC economies in promoting within the UN the improvement of the general international legal framework to combat this threat.