

# NATIONAL PROGRAMME ISF

## IDENTIFICATION OF THE DESIGNATED AUTHORITIES

### Competent authorities responsible for management and control systems

Authority	Name of the authority	Name of the person responsible for the authority	Address	E-mail address	Date of designation	Activities delegated
Responsible authority	Federal Public Service (FPS) Home Affairs, Unit European Funds	Secretary-General of FPS Home Affairs	Leuvenseweg 1, 1000 Brussels	AMIF-ISF@ibz.fgov.be		
Audit authority	Inspectorate of Finance (Ministry of Budget)	Superintendent of Inspectorate of Finance	De Lignestraat 37, 1000 Brussels	Pierre.Reynders@inspf.in.fed.be		

### Management and control system

One unit will manage ISF fund, as opposed to SOLID funds. The RA is located in the FPS Home Affairs, as well as the Monitoring Committee (strategic decisions by public partners and representatives of relevant ministers) Payments will be executed by the accounting unit of 'home affairs', based on orders from the RA. Projects will be selected using awarding method: preferably open calls but direct awards in the case of legal monopolies. Selection will be done by selection committees with relevant partners such as representatives of cabinets, RA and administrations. Agreements will be concluded with all project partners, funding will be provided through cash or budget transfers. Main principles of control, evaluation, monitoring, reporting, audit etc remain basically the same as for the existing system with minor modifications.

CCI	2014BE65ISNP001
Title	Belgium National Programme ISF
Version	2.1
First year	2014
Last year	2020
Eligible from	01-Jan-2014
EC Decision Number	C(2017)6193
EC Decision Date	11-Sep-2017

## 1. EXECUTIVE SUMMARY

### 1. *ISF Borders*

Belgium (BE) intends to continue and, where possible, enhance the actions developed under the preceding funding programmes.

The national strategy concerning **visa related matters**, (+/- 35% of ISF Borders) aims at fast and efficient delivery of Schengen visa to bona fide travellers and the fight against abuse of visa procedures and the use of false or fraudulent documents. Abroad, BE focuses on upgrading infrastructure in certain visa sections as well as on creating a more efficient access to visa information for applicants. To reach these goals an information sharing platform will be developed, in order to better identify trends and risks and so steer different stakeholders on the operational level: the Federal Police's border guard trainers, Foreign Affairs' document verification officers (DVO), the Immigration Office's Immigration and Liaison Officers' (ILO). BE will seek to build closer synergies with different Member States by increasing the consular cooperation with i.a. the setup of Schengen Houses and of a Consular Cooperation Mechanism. Belgium will participate equally in the Specific Action lead by Portugal on the establishment of a Common VISA Application Centre in Saõ Tome. The full implementation of the VIS is a priority, for which operating support will be used.

Within the field of **border control and border surveillance**(+/- 26% of ISF Borders), the primary focus will go to the innovation of equipment and a thorough fight against false & falsified documents. To reach these goals investments in Automated Border Control (ABC), access to the Public Key Directory / Public Key Infrastructure (PKD/PKI) and upgrading equipment to read and analyse documents at border posts will be done. Data exchange programmes such as national single window and Advanced Passenger Information (API) systems will be developed, leading to an enhanced use of interoperable modern technologies in line with European standards. The National Coordination Center for Eurosur will be finalized with support of the fund. Aviation awareness raising by controls on illegal border-crossing through not-recognized border posts on smaller airports and heliports in

Belgium will be extended by an IT-platform. Under operating support the maintenance and upgrade of SIS II will be assured.(+/- 33% of ISF Borders)

## **2. ISF Police**

The national strategy on **preventing and combating crime** (+/-75%) brings in line strategic plans adopted at national level and the EU policy cycle for organized and serious international crime 2013-2017.

BE aims at a better understanding, exchange of information and operational co-operation between all partners at national and international level (EU Member States (MS), EU agencies and international organisations). Capabilities should be increased for Law Enforcement Agencies to detect and combat serious and organised crime. BE will also focus on more and better training for key players with regard to specific phenomena and existing possibilities of international cooperation and will create increased awareness among all stakeholders of the threats and possible counter-measures.

Regarding the exchange of information, BE will create effective international exchange systems. Depending on the outcome of negotiations, investments would also be made on the set up of a Passenger Information Unit. BE equally wants to participate actively in the EMPACT activities.

Finally, cross-border law enforcement (LE) cooperation will be improved through training. Special attention in this area will be given to the implementation of the EU Law Enforcement Training Scheme.

With regard to the **protection of critical infrastructure and crisis and security risk management** (+/- 18.8%) BE adopts an all-hazards approach, taking into account all kinds of security risks and threats.

Under infrastructure, BE intends to invest in projects that will result in improved cooperation and information exchange between all partners and target groups involved, increased knowledge among all actors (including the general public) and enhanced capabilities in terms of better technical equipment and training.

Concerning warning and crisis, awareness raising should be increased. A focus will be set on communication both with the population and on management level in the preventive stage as well as in response to a security-related incident. The development of communication tools and disaster plans might be significant additional actions in this framework. Training, (joint) exercises and the exchange of best practices should be organized at all relevant levels.

## **2. BASELINE SITUATION IN THE MEMBER STATE**

### **Summary of the current state of play as of December 2013 in the Member State for the fields relevant to the Fund**

#### **ISF Borders**

#### **1. VISA**

##### **1.1. Baseline situation**

The Immigration Office (IO) is responsible for Schengen visa applications. The IO closely collaborates with the Ministry of Foreign Affairs (FA) for visa issuing. In most cases, the latter is authorized to decide on visa applications. In case of doubt or a negative assessment of the visa application, FA can transmit the application file to the IO for decision. In 2012 BE registered 233.487 Schengen visa applications, in 2013 233.272.

Currently FA issues visas in 94 countries. For 22 of those posts, an external firm receives the visa applicants. In the remaining posts, FA receives visa applicants in its premises.

Next to the 94 countries in which visa are issued, BE is represented by another MS in 80 posts. In its turn, BE represents other MS in 60 consular posts. The issue of “representation” in the framework of visa issuing continues to grow in importance in the light of budgetary restrictions many MS are facing.

With financial support of the External Borders Fund (EBF), BE implemented several projects: set-up of CAC’s in Kinshasa (community action) and in Gaza as well as the employment of locally recruited field workers, who verify supporting documents submitted with the visa files in case of suspected document fraud. The national VIS was developed and diplomatic posts are equipped with biometric devices. VIS roll out is expected to be completed with EBF.

##### **1.2. National needs & requirements**

There is a need to enhance consular cooperation in third countries through representation, and to ensure adequate facilities to receive visa applicants.

Especially visa sections in Dakar, Nairobi, Ouagadougou and Lubumbashi require infrastructural changes to ensure a safe and efficient visa application process. As an example,

in Dakar, where BE received approximately 3000 applicants in 2013, there is an identified need to install appropriate emergency exits, a secured entry, an Air Conditioning and surveillance cameras in the visa applicants' waiting room, etc.

Enhanced services for bona fide applicants are not only a matter of better facilities, but similarly a targeted approach against fraudulent visa applications will add to the efficiency with which visa personnel can process applications.

A cooperative initiative will be launched to fight document fraud and visa abuse, based on an analysis of trends in visa abuse, document fraud and illegal migration.

Mala fide visa applications for countries represented by BE lead to an increasing workload for the IO. It is necessary to improve the knowledge of visa agents concerning Schengen-related entry-legislation in order to motivate refusals.

There is a need for the expansion of a reliable, fast and efficient system for visa delivery and to maintain and upgrade IT material for the registration of biometric data and to ensure adequate data protection.

### 1.3. National resources

IO: 37,75 FTE visa officers, estimated at € 2.265.000

Although difficult to calculate, the cost of buildings of FA, used to facilitate the visa process, both in Brussels and consulates abroad can be roughly estimated at around € 3.2 M on a yearly basis.

FA: 49 visa officers, local personnel abroad, yearly cost of visa-personnel in the central administration is estimated at € 12.000.000

350.000 stickers were purchased (€ 276.000).

## **2. BORDERS**

### 2.1. Baseline situation

BE is, with its 30 158 km<sup>2</sup>, one of the smaller countries of the EU, but its central position between FR and DE and the relatively short distance to the UK, gives rise to specific migration problems. The length of external land borders is 3 km, sea borders is 109 km.

The IO organizes and controls the set-up of border control in close cooperation with the Federal Police (FedPol).

BE does not have a "border-guard"-structure as such. Border control is carried out by FedPol. For the implementation of border control tasks, this personnel receives an additional and specifically oriented training, which complements basic training. Hence, these trainings are already developed and are in line with SQF and Fundamental Rights courses.

BE has 13 Schengen external border crossing points: 6 ports, 6 airports and a HST-terminal (entry through the latter is checked by FR on UK territory since 2004).

Approximately 19 M passengers travelled through *Brussels International Airport* in 2013. Over the past years, the number of passengers in *Gosselies Airport* has risen sharply to 6,7 M in 2013, especially on account of the presence of low fare carriers.

The number of decisions issued by the IO in 2013 at the external borders provides an additional measure of migration pressure: refusals at the border (1897), asylum applications at the border (502), visa C for seamen (7421), other visa C (878), removal from another country (Schengen and non-Schengen) with transit on a BE Airport with FedPol's assistance (590), detection of unaccompanied alien minors (16).

The number of refusals at the border is unevenly split between air and sea borders:

- Air borders: 1773 in 2010, 2701 in 2011, 2358 in 2012 and 1860 in 2013
- Sea border : 90 in 2010, 34 in 2011 and 45 in 2012 and 37 in 2013

With the financial support of EBF BE implemented several projects:

BE invested in the purchase of new equipment to enhance the border controls and checks. 4 video cameras were purchased to mount on helicopters, used i.a. for control of the maritime border. Night viewers were obtained to use when patrolling the sea border. At the border posts in the airports new passport readers and fingerprint scanners were installed and upgraded to be compatible with VIS. In Brussels International Airport the installation of e-gates started under the EBF AP 2012 and is still going on.

Development and implementation of SIS II in Belgium is carried out by FedPol.

To tackle problems of border surveillance between extra-Schengen border posts the airport police executed an action to increase awareness of small airport holders and pilots. 168 violations were registered in the starting year 2008, while in the years after the number of violations decreased with 45 to 80 %, demonstrating the impact of the action which means an improvement for border control in general. Comparable problems were identified and tackled concerning entry of the territory by water.

Trainings in recognizing fake and forged travel documents were given in third countries to employees of airline companies, diplomatic posts and local authorities. An exchange of best practices was set up between 2nd line border guards of different MS.

BE became member of the PKD Board in October 2013 and is prepared to develop PKI/PKD technology in the future.

### 2.3. National needs & requirements

There is a continuous need for modern technology at border posts. The implementation of the Schengen Acquis, the development of EUROSUR and the upgrading and maintenance of modern technologies at the border are key issues for BE.

BE only recently started with an Automated Border Control project under the EBF but this is still in a start-up phase.

It is necessary to invest in the further development of ABC as well as to develop IT systems such as inter alia API, single window systems, PKD/PKI technology and investment in equipment (hardware) in order to obtain an efficient border control. It is equally necessary to invest in the upgrade and the maintenance of the future Smart Border systems.

BE is also bound to set up a National Coordination Centre by the end of 2014 to be connected to Eurosur.

As SIS II has only been developed and implemented under EBF, there is an operational need for maintenance and upgrading and to develop a back-up system of the mainframe in order to make the recent setup useful.

## 2.4. National resources

FedPol employs a workforce of approx. 880 persons in border control. The IO employs 18 FTE in the Border Control Unit.

For IT systems related to visa and border control (VIS, SIS II and start-up of ABC) a budget of approx. € 8 M was earmarked in 2013.

## **ISF Police**

### **1. Prevention of and fight against crime**

#### 1.1. Description of the baseline situation

BE is confronted with several types of serious and organized crime, most of which have an international character. In the context of the ISF, the following phenomena are considered as priorities: drug trafficking (in 2013 ca. 2.600 criminal facts were registered with regard to the import/export of drugs and ca. 1.500 with regard to production of drugs), with focus on cocaine (ca. 450 cases in 2013), synthetic drugs (220 cases), and cannabis (300 major cases); cyber-crime (in 2013 more than 17.000 cases of ICT-crime were registered); trafficking in human beings (386 facts in 2013); facilitating illegal migration; organised property crime (we estimate that 30% of the more than 400.000 thefts that took place in BE in 2013 were committed by mobile organised crime groups); armed robbery (almost 4.400 facts in 2013); social, fiscal, or waste management fraud; illicit trafficking, supply and use of firearms.

Although the number of terrorist incidents in BE is rather low (2 in 2012; 0 in 2013), the BE authorities remain vigilant about the terrorist threat and violent radicalisation processes.

In 2007-2013, BE has successfully carried out several ISEC-projects. In fact, the EU policy cycle on serious and organized crime originated from BE ISEC-project 'Harmony'. Other projects focused on specific phenomena (e.g. child pornography, radicalization, cybercrime) or types of law enforcement cooperation (e.g. Airpol; ENFAST).

#### 1.2. National needs & requirements



According to the partners consulted in preparation of this national programme, there is a need for closer operational cooperation and a better information-exchange between the competent authorities, both at national and international level.

Since criminals often use modern technology, which continues to evolve at high speed, technical capabilities of our law enforcement agencies also need to be improved. Finally, it appears that the various stakeholders' knowledge of particular phenomena and/or existing possibilities for international cooperation needs to be improved.

When selecting projects in this field, BE will evaluate their coherence with existing strategies at national level (e.g. national security plan, national cyber-security strategy, national strategy for the prevention of radicalization) and take into account key issues of the policy dialogue with the EC, i.e. to improve the fight against drug trafficking, to prevent and combat radicalization towards terrorism and violent extremism and to enhance cyber-security and step up the fight against cybercrime, as to implement the LETS and eventually to set up a PNR-system.

### 1.3. National resources

Given the great number of actors involved (i.a. FedPol and 195 Local Police forces, Ministry of Interior, judicial authorities, Customs, ... ), it is impossible to give precise figures on the total budget spent at national level on the prevention of and fight against crime. As an indication, we can quote following figures for some of the main actors involved:

- FedPol: total budget 2013 = 1,8 billion €; ca. 12.000 staff members.

DGA = General Administrative Direction: 3677 staff members, general staff cost € 265 m .

DGJ = Juridical Police: 4186 staff members, general staff cost € 302 m.

CGSU = Direction of Special Units: 539 staff, general staff cost € 38 m.

- Ministry of Interior – General Directorate Security and Prevention: total budget 2013 = € 93,5 m; ca. 150 staff members

## 2. Security-related risks and crisis

## 2.1. Description of the baseline situation

The National Crisis Centre of the Ministry of Interior monitors 24/7 and identifies every security and safety-related incident on the BE territory. In case of a major incident, it will coordinate the response at the federal level.

With regard to the protection of critical infrastructure, BE adopts an all-hazards approach, focusing on every event which could lead to damage.

Except for the OPLON-project of FedPol (protection of the EU institutions during EU summits), BE public authorities have made little or no use of the CIPS-programme.

## 2.2. National needs & requirements

During the policy dialogue, it was agreed that BE needs to improve the protection of critical infrastructures on its territory, and increase the preparedness of the various stakeholders concerned in relation to crisis and security risk management. Our projects in these fields will build upon the existing legislation (e.g. our national law on the security and protection of critical infrastructures), methods (e.g. our multidisciplinary approach in crisis and security risk management), and division of tasks (e.g. the specific role of the Coordination Unit for Threat Analysis) at national level.

In general, the main requirements in both areas can be summarized as follows:

- A need for improved cooperation and information exchange between all partners and target groups concerned, both in the preventive stage and in response to a security-related incident.
- More and better equipment to protect critical infrastructure is needed.
- There is a need to limit the impact of security-related incidents related to the level of awareness of the stakeholders (including the population)
- Improved communication through capacity building, information management and communication tools is required.
- Training, (joint) exercises and the exchange of best practices should be organized at all relevant levels.
- There is a need for improved disaster plans and an analyzing structure.

## 2.3. National resources

Again, precise figures cannot be given, due to the great number of competent authorities, partners and target groups involved. Indicative figures:

- Ministry of Interior – General Directorate Crisis Centre: total budget 2013 = 15,8 million €;  
ca. 78 staff members

- National Centre for Cybersecurity: total budget 2014 = 3,7 million € ; ca. 10 staff members

- Coordination Unit for Threat Analysis (CUTA): total budget 2014 = 1,398 million €; ca. 51  
staff members.

### 3. PROGRAMME OBJECTIVES

<b>Specific objective</b>	1 - Support a common visa policy
---------------------------	----------------------------------

In Belgium the Common Visa policy is a key objective given the increasing number of visa processed by Belgium : main challenges are to increase efficiency through an improved visa capacity abroad, targeted fight against fraud, cooperation with other MS to create scale effects and new and enhanced IT applications.

To ensure a high quality of services for visa applicants Belgium will provide improved information on visa policy to visa officers . Moreover Belgium seeks to upgrade the infrastructure of visa sections in Dakar, Nairobi, Ouagadougou and Lubumbashi. The necessary importance will be given to safety measures.

Furthermore Belgium will focus on better "consular coverage" in Schengen visa issuance to avoid a disproportionate effort for the visa applicants to have access to consulates - through e.g. the use of ESP's or mobile biometric devices which will be financed by national budget.

Simultaneously, next to the facilitation of legal travel, Belgium seeks to prevent illegal migration activities. Belgium will build on lessons' learned from the projects of 'field worker' and 'border guard assistance' introduced under EBF in order to establish a more structured cooperation to fight Schengen visa-shopping and abuse, prevent illegal migration, and build relevant capacity in third countries. An information sharing platform involving FA, the IO and the FedPol will therefore be established.

Operational activities will be complemented by information campaigns in targeted countries/regions, to inform about facilitating legitimate travel and inform on the risks of illegal migration including trafficking and smuggling.

Via Specific Actions, Belgium will seek to build closer synergies with other MS where there is a common interest through a Specific Action aimed at deploying joint Document Verification Officers (DVO's), joint immigration liaison officers (ILO's), building capacity and launching information campaigns in third countries. Belgium will also invest in enhanced consular cooperation by taking the lead in the setup of "Schengen Houses" in selected countries, in the light of increasing representation requests (see under Specific Actions). In that view Belgium creates more efficient operations and customer-friendly service to visa applicants through increased consular cooperation.

<b>National objective</b>	1 - National capacity
---------------------------	-----------------------

Under ISFBorders, Visa, National Capacity there are 3 main actions which are at the same time funding priorities.

1. Improving information to visa-applicants (by organizing information sessions for visa officers , the production of target group-oriented visa leaflets and improving existing websites) with regard to European Visa policy.

The desired outcomes are to offer visa applicants more customer-friendly services

2. Renovating and refurbishment of visa sections to improve reception of visa applicants and ensuring the safety of visa personnel and visa applicants, especially where BE represents other MS ( Indicative list: in Dakar, Nairobi, Ouagadougou and Lubumbashi . Potential other premises could be identified in the future.)

The desired outcome is visa reception and processing areas to meet European standards and allow for an efficient work-flow

3. A third action is the establishment of a national information sharing platform gathering authorities from the Ministries of Foreign Affairs (DVO's and ESP's), Home Affairs (Immigration Office, ILO's) as well as the Federal Police (ALO's). On an operational level DVO's investigate supporting documents, ALO's organize trainings and controls, and ILO's set up prevention campaigns and build capacity *of national authorities* in third countries.

The platform meets on a regular basis allowing all stakeholders to share information on planned activities and existing resources, trends and findings linked with visa abuse and document fraud. During these consultations statistics are analysed and strategies for joint actions are developed.

The desired outcomes are:

- maximize the output of these resources by jointly analysing trends and responses to fighting visa abuse, document fraud and illegal migration

- shorter Schengen-visa processing times hence a higher quality of visa services.
- prevent irregular migration by fighting visa abuse and travel document fraud
- to create synergies and to use the means in the most efficient and effective way *through a closer cooperation between the relevant authorities.*

<b>National objective</b>	2 - Union acquis
---------------------------	------------------

No specific key issue has been identified under this priority during the policy dialogue.

Possible recommendations of the Schengen Evaluation Mechanism will be handled, where necessary and possible with ISF funding.

<b>National objective</b>	3 - Consular cooperation
---------------------------	--------------------------

<b>Specific action</b>	1 - Consular cooperation
------------------------	--------------------------

Specific Action 1 and 2:

Ensuring adequate operational structures and visibility as single Schengen visa-issuing presence in Kigali and Bujumbura in the framework of MS cooperation through consular representation.

Desired Outcomes:

- Better service is offered to visa applicants.
- Economies of scale as regards processing applications and issuing visas are generated.

Participating MS : Austria, Czech Republic, Germany , Estonia, France , Greece, Hungary, Lithuania, Luxembourg, The Netherlands, Norway, Portugal, Slovakia, Slovenia, Sweden

Budget : 1.100.000 EUR:

- 550.000 EUR for the project Schengen House in Kigali
- 550.000 EUR for the project Schengen House in Bujumbura

## **Role of the partners:**

The partner MS are co-beneficiaries of the grant and will designate national staff to train visa agents and local staff of the Schengen Houses.

### Specific Action 3:

Establish, in close collaboration with partner MS, a **Consular Cooperation Mechanism (CCM)** on Schengen Visa Processing in commonly agreed third countries. This mechanism relies on three operational pillars:

- *Joint assessment of risks and trends* between MS at capitals and field level in visa abuse, document fraud and irregular migration;
- *Deployment of joint document verification officers* or document verification services, to investigate the authenticity and reliability of information submitted in the ambit of Schengen-visa applications;
- *Joint training of MS and consular staff* in assessing supporting documents emitted by third countries, in analysing trends in Schengen-visa abuse, detecting false and forged identity and travel documents; and where relevant, joint training of third countries' authorities to reinforce the reliability of Schengen-visa source documents.

### Desired Outcomes:

- International analyses on trends and risks are elaborated.
- Joint document verification officers are deployed.
- Consular staff of MS to equally assess visa documents and trends in Schengen-visa abuse is jointly trained.

Participating MS: Estonia, France, Hungary, Italy, Poland, Portugal, Romania, Spain, Switzerland, and The Netherlands

Budget : 3.120.000 EUR

Most of the partner MS will take the lead in a specific project location, in order to:

- contract and supervise the activities of the joint DVO/ joint external document verification services;
- organize and chair the local anti-fraud working group;
- report to the project Steering group.

BE is also partner in the following SA:

Specific Action “Schengen Visa Centre in São Tome and Principe”, for which Portugal is lead MS. The project aims to set up consular cooperation instruments regarding visa applications and the issuing of visas in S Tome and Principe in cooperation with other MS. Belgium will participate at a no-cost basis.

<b>Specific objective</b>	2 - Borders
---------------------------	-------------

In the Belgian National Security Plan (2012-2015) the strategy for an integrated border surveillance and control at the external borders is described. In order to implement EU necessary requirements in the daily operations of the police at border crossing points, certain preconditions have to be met, such as support of IT systems and enhancing knowledge, integrating EU border guards training programmes in the national training plan, taking initiatives to promote the use of modern technology at the borders (including use of biometrics, passport readers, etc. ), and the improvement of work processes and ICT systems to reduce administrative burden.

Belgium will continue to participate in the development, management and execution of operations organized by Frontex. FedPol will have a sufficient level of training and an appropriate reserve capacity to participate in the RABIT'S- operations and the Joint Operations.



Belgium will step-up preparations to establish the National Coordination Centre (NCC) of the EUROSUR network in the course of 2014 (pilot project). All relevant authorities will be involved in the NCC and the national situational picture would need to be established by end 2014. There should be compliance with **EUROSUR** standards and establishment of the National Situational Picture (NSP).

Belgium successfully switched over to the **SIS II** on 9 April 2013. Although the system is very stable, a back-up site has not yet been established. In terms of the security of the system, it is fully integrated into the security policy of FedPol's IT infrastructure and an audit has started in 2013 to identify and subsequently address potential weaknesses. The SIS II system needs maintenance and upgrades in the future, as well as a back-up-mainframe in order to keep the system operational at all times. The key objectives to reach for SIS are:

- SIS II available and in operation (has started under EBF);
- SIS II has a full disaster recovery/ business continuity plan
- SIS II national system is resilient to cyber-attacks in terms of physical, computer and data security.

Belgium will take into account and carry out recommendations of SCHEVAL with respect to air, land and sea borders, where necessary. In order to implement SCHEVAL recommendations Belgium plans under Union Acquis to tackle illegal border crossings through non-recognised border posts at smaller airports and heliports.

Investments to increase the national capacity and lead to an enhanced use of interoperable modern technologies in line with European standards such as data exchange mechanisms (API, single window systems), reading equipment and PKD/PKI technology are necessary to develop an efficient border control. Belgium also intends to continue to install ABC-gates which should also be compatible with the possible future smart borders initiative to speed up passenger flows.

<b>National objective</b>	1 - EUROSUR
---------------------------	-------------

EUROSUR is a project of FedPol (Waterway police) to implement the European Regulation 1052/2013 of 22-10-2013 of the European Parliament and the Council to install the European border control system EUROSUR. The project EUROSUR exists mainly to be able to feed the server, which is provided by Frontex, from different points (from SPN/MIK, SPC/Eurostar, SPA/brunat and LPA/gosselies to the National Contact Point where the server of Frontex will be installed). Belgium will step-up preparations with a view to establishing the National Coordination Centre (NCC) in 2014 to allow Frontex to connect it to the EUROSUR network on a pilot basis in the course of 2014. All relevant authorities will be involved in the NCC and the national situational picture would need to be established by end 2014.

The main action and funding priority through ISF funding is the finalization of EUROSUR

example actions:

- Establishing connections (investments in upgrades) with different servers.
- Investments in hardware in order to make all elements compatible and make data transfer possible.

Desired Outcome: the NCC is operational.

Costs will be rather limited because of the relatively small migration pressure on Belgium's external borders, the small geographical volume of the external borders to guard and the existing infrastructure and staff resources (the NCC will be embedded in the *National Incidence Point*, this point secures the operational aspects of the international police cooperation).

<b>National objective</b>	2 - Information exchange
---------------------------	--------------------------

<b>National objective</b>	3 - Common Union standards
---------------------------	----------------------------

The main action to increase the national capacity of Borders is to invest in infrastructure in order to obtain a more efficient border control and to meet the common Union standards regarding border control.

The main action and funding priority is therefore the investment in ABC.

The **Automated Border Control system** is linked to PKI/PKD; Belgium wants to install the ABC-gates in Brussels and Gosselies airport. The ABC project is a continuation of the current ABC-project financed by EBF. ABC consists in the installation of e-gates at the terminals which support the existing manual Schengen border control. The requests and processing of information in this way have been automated for 6 gates under EBF at Brussels National Airport (Brunat). Through ISF-Borders funding, 12 extra gates should be placed at Brunat. Depending on the selection of projects which imply budgetary consequences during the ISF implementation, the ISF might also serve financing the preparation and the implementation of the regional airport ABC-gates.

Targets (desired outcomes) of the action is to create a time efficient and effective border control which will evoke more passengers being checked on a short time, while at the same time BE wishes to use modern interoperable technology at the border to be in line with European standards.

<b>National objective</b>	4 - Union acquis
---------------------------	------------------

Main actions:

1. Enable exchange of information with extra-schengen countries concerning illegal border crossings through non recognized border posts of small airports and heliports in Belgium. This action is a follow-up action off the AVIA project implemented under the EBF (EBF-2011-9). In view of an enhanced situational picture of border crossings the AVIA project implemented under the EBF will be extended in order to manage and decrease border crossing through non-recognised border posts at the smaller airports and heliports.

Example actions:

- Develop an IT platform to facilitate the exchange of information.

The desired outcomes are:

- The implementation of the Schengen acquis – border surveillance.
- A decrease of illegal border crossings through non-recognised border posts at the smaller airports and heliports.

2. Implement recommendations of the future Schengen Evaluation Mechanism or other EU agencies analyses. Implementation of these recommendations will, where possible, be financed through ISF funding.

Example actions are to be decided, based on the EU and Schengen analysis

Desired outcomes are to have complied with the received recommendations.

<b>National objective</b>	5 - Future challenges
---------------------------	-----------------------

<b>National objective</b>	6 - National capacity
---------------------------	-----------------------

The main action to increase borders national capacity by investing in infrastructure, hardware and software to obtain a more efficient border control.

Example actions will be funded and increase the effectiveness of border checks.

- **PKI/PKD** : Chips of e-passports contain Public Key Infrastructure (PKI) certificates that can be verified at border control in order to ensure the document’s authenticity. In order to enable the verification of e-passports from travellers arriving from another country, Belgium needs to be able to read the certificate in the chip. The exchange of certificates between members of the PKD board is managed by the Public Key Directory. The ISF funding will be used for the installation to be able to read the digital certificates (PKI) in e-passports. It does not concern the purchase of equipment which can read these certificates, but rather the development of a database.
- purchase of **document investigation equipment** at border posts (all official border posts): Belgium wishes to invest in document investigation equipment. These document scanners serve to check the authenticity of travel and identity documents. Biometric passport readers and digital fingerprint scanners had been funded under EBF to be used in first line control. Under ISF the document investigation equipment will serve for second line control in order to check the authenticity of documents.
- development of **data exchange mechanisms** such as national single window systems (part passenger flows); development API-software system in coherence with the

implemented Automated Border Control in order to create efficient border control in a limited period of time.

- development, upgrading and maintenance of the future **Smart Border Systems**. Development, upgrading and adaptation of national IT systems for connection to the Smart Borders systems; maintenance and upgrading of national components when they have become operational (depending on the outcome of the negotiations).

Targets (desired outcomes) of the actions are the use of modern technology at the border, for border control and checks in order to run the border control process in a more efficient and effective way and enhance the ability to intercept fraudulent travellers. Continued investment is leading to an enhanced use of interoperable modern technologies in line with European standards where they exist.

<b>Specific objective</b>	3 - Operating support
---------------------------	-----------------------

Belgium hereby confirms its compliance with the Union acquis on borders and visa.

Belgium hereby confirms its compliance with Union Standards and guidelines for good governance on borders and visa, in particular the Schengen catalogue for external border control, the Practical Handbook for borders guards and the Handbook on visa.

<b>National objective</b>	1 - Operating support for VISA
---------------------------	--------------------------------

Full implementation of the VIS is a priority. VIS roll out in consular posts is expected to be completed within the framework of the Operational Support of the External Borders Fund.

Belgium wants to finance the maintenance and necessary upgrading of the VIS under the Operating Support mechanism.

The ministry of Home Affairs is responsible for the development and functioning of the VIS. The ministry of Foreign Affairs is responsible for the reception of visa applications and issuance of visa.

Objective: continued functioning of the VIS, as well as a high quality of services for visa applicants is ensured

Tasks and services: maintenance and upgrading of the national VIS, online training of VIS-users, training sessions for VIS-users, upgrading of the VIS soft and hardware in consulates, as well as ensuring adequate data-protection on visa information through adequate software.

<b>National objective</b>	2 - Operating support for borders
---------------------------	-----------------------------------

1. Belgium successfully switched over to the SIS II on 9 April 2013. Although the system is very stable, a back-up site has not yet been established. In terms of the security of the system, it is fully integrated into the security policy of the Federal Police's IT infrastructure and an audit has started in 2013 to identify and subsequently address potential weaknesses. The Federal Police is responsible for the development and functioning of the SIS II.

The national objective is to finance the maintenance of this main frame as well as the development of the back-up capability through the Operating Support mechanism of ISF. The back-up of the SIS II is essential to continue the implementation of SIS II.

The back-up of the main frame ensures the system to be resilient to cyber-attacks in terms of physical, computer and data security.

Tasks and services: Implementation, maintenance and upgrade of the SIS II including development of back-up capability

2. The Federal Police is responsible for border control using checks in the VIS. Information in the BELVIS, the application used at the border control connected with VIS, will be provided by national links with other national databases (e.g. ANG).

Tasks: development of national links with the BELVIS application

<b>Specific objective</b>	5 - Preventing and combating crime
---------------------------	------------------------------------

Taking into account the needs identified in the baseline situation (i.e. shortcomings in the operational cooperation and information exchange; insufficient technical capabilities; lack of specialized knowledge), Belgium will focus on three operational objectives of the Specific Regulation on ISF Police:

- To strengthen our capability to prevent crime and combat cross-border, serious and organised crime including terrorism;
- To promote and develop administrative and operational coordination, cooperation, mutual understanding and information exchange at national and international level;
- To promote and develop training.

In each area, Belgium will adopt a strategic approach, based on our national strategies and the EU policy cycle for organised and serious international crime. The most comprehensive plan at national level is our National Security Plan (NSP), which is adopted every four years by the Ministers of Justice and Home Affairs, after consultation of all partners concerned.

Belgium has identified the following phenomena, which all occur as priorities in the NSP 2012-2015 and/or the EU policy cycle 2013-2017, as priorities for our national programme under ISF Police: terrorism and violent radicalisation; drug trafficking; cybercrime; trafficking in human beings; facilitating illegal migration; organised crime against property; armed robbery; social, fiscal, or waste management fraud; illicit trafficking, supply and use of firearms.

Three of those phenomena will be given special attention under ISF Police:

- Improve detection, investigation and prosecution of drug trafficking;
- Radicalisation towards terrorism and violent extremism;
- Cyber-security and fighting cyber-crime.

Belgium currently takes part in 8 out of the 9 EMPACT projects and will continue to participate actively in the EU policy cycle on serious and organised crime. We will also continue to take initiatives to improve cross-border law enforcement cooperation through training.

Finally, a significant share of the national programme could be devoted to the setting up of a Passenger Information Unit, depending on the outcome of the negotiations on the EU PNR Directive.

When selecting for funding, the Belgian authorities will take into account the existing national strategies for the specific issues concerned. Actions in the field of cyber-security and cyber-crime will have to be in line with the national cyber-security strategy that was adopted by the Belgian Government in December 2012, while projects in the area of preventing radicalisation will have to focus on (one of) the 6 axes of the national strategy that was approved in April 2013 (*inter alia* a better knowledge and collective awareness of radicalisation; increasing resilience among vulnerable individuals, groups and communities; fighting radicalism on the Internet and organising counter-speeches; ...).

<b>National objective</b>	1 - C - prevention and combating
---------------------------	----------------------------------

Belgium will carry out with regard to those phenomena that have been identified as priorities, the following actions by means of ISF funding:

1. Promote and develop cooperation between the competent organisations (public & private), in terms of joint activities as well as the exchange of information and best practices.

Examples: setting up multidisciplinary coordination centres (e.g. on cybercrime and platforms for the exchange of good practices and/or information (e.g. on the administrative approach against crime)).

**Desired outcomes:** improved administrative and operational coordination, cooperation, mutual understanding and information exchange between the competent organisations at national level.

2. At international level, BE will take part in joint actions depending on the operational needs in specific cases; (e.g. to combat drugs trafficking),

Example: joint investigation teams, joint patrols or control actions



**Desired outcomes:** enhanced cross-border cooperation with concrete operational results (arrests, seizures, ...).

3. Raise awareness among law enforcement officers (LEOs), public & private partners and the general public with regard to specific phenomena (especially cybercrime and radicalisation towards terrorism), develop expertise, organize trainings and spread best practises with regard to crime prevention.

Examples: Centres of excellence (cybercrime; crime prevention) and national support platforms for public authorities and civil society (e.g. for the prevention of radicalisation, de-radicalisation projects in prisons, or the development of a counter-narrative); research, awareness campaigns and trainings (e.g. resilience; de-radicalisation; coaching teams for police services).

**Desired outcomes:** lower crime rates through better crime prevention and increased awareness among all stakeholders.

4. Organize specialized training courses for LEOs, public authorities and practitioners: set up specialized training infrastructures.

Examples: cyber exercises; trainings on legal intrusion of protected IT-systems used by criminal organisations, training lab for the dismantling of production sites for synthetic drugs and cannabis.

**Desired outcomes:** high level of expertise among LEOs, public authorities and practitioners.

5. Develop the competent authorities' (technical) capabilities to detect and combat crime, both in the physical world (equipment; forensic techniques) and on the internet.

Examples : development or purchase of software for internet monitoring (e.g. websites of radical groups) and data analysis capacity; research on and implementation of new forensic techniques (e.g. rapid DNA); acquisition of tools and equipment for LEA (e.g. cargo scanners, automatic number plate recognition systems).

**Desired outcomes:** improved (technical) capabilities for the LEA.

<b>National objective</b>	2 - C - exchange of information
---------------------------	---------------------------------

The main actions that will be funded by means of ISF are:

1. Create effective systems for the exchange of information between all relevant national actors on the one hand and our neighbouring countries, other EU Member states, EU agencies and international organisations on the other hand.

Examples are:

- Enhancing our IT-systems for international information exchange with other EU member states (e.g. between SPOCs for operational cooperation in cybercrime cases or between DNA-agencies exchanging data), Europol (e.g. automated system for uploading data to the Europol Information System) and Interpol (interoperability project; automation of data transfers to/from the Interpol databases).
- Setting up and developing a Passenger Information Unit: developing/purchasing software and hardware for the collection, treatment, analysis and storage of data (the precise scope of this action and the extent to which it will be financed through the Internal Security Fund depends on the outcome of the negotiations on the EU PNR Directive).

Desired outcome: improved technical capabilities for information exchange, data collection and data analysis.

2. Participate in EMPACT activities as defined in the operational action plans, to the extent that these are not financed-through the budget for Union actions

Examples: Belgium takes part in 8 of the 9 actual EMPACT projects

**Desired Outcome:** improved operational cooperation between the LEA of the Members States involved.

<b>National objective</b>	3 - C - training
---------------------------	------------------

The main actions to be funded by means of ISF P are:

Organize trainings on cross-border cooperation, exchange of best practices, and develop other initiatives increasing to increase awareness and know-how capacity of LEOs in this area.

Special attention will be given to the implementation of the EU Law Enforcement Training Scheme. This will be done through regional cooperation on training with neighbouring countries, as training on instruments for international police cooperation is already part of the basic training of all Belgian police officers.

Example actions:

- Training and the development of supporting tools to improve law enforcement officials' knowledge on cross-border cooperation; e.g. the Meuse-Rhine Euregio vademecum: this IT-tool, which presents the existing possibilities regarding various forms of cross-border cooperation (operations, mutual legal assistance, information exchange, ...) in a concise but very comprehensible way to first-line police officers, needs to be updated, extended (all our neighbouring countries instead of only DE and NL) and made available on all major (mobile) IT-platforms.
- Specific trainings for LEOs on cross-border interventions or information-exchange, especially when new national or international regulations enter into force (e.g. our 2014 bilateral treaty with France; Belgian law implementing the Swedish framework decision; EIO).
- Intensifying training and exchange of best practices with regard to forensic expertise (e.g. DNA-analysis).

**Desired Outcome:** a cross-border culture among law enforcement officers: they should be familiar with the legal framework and the (IT-)tools which are at their disposal, and consider it natural to closely cooperate with LEOs of other Member States in order to prevent and combat serious, international crime.

<b>National objective</b>	4 - C - victim support
---------------------------	------------------------

<b>National objective</b>	5 - C - threat and risk assessment
---------------------------	------------------------------------

<b>Specific objective</b>	6 - Risks and crisis
---------------------------	----------------------

Belgium will focus on two operational objectives of the Specific Regulation on ISF Police, i.e.:

- To strengthen our capability to protect critical infrastructure;
- To manage and secure links and effective coordination between the existing early-warning systems and crisis cooperation actors in order to enable the quick production of comprehensive and accurate overviews in crisis situations, coordinate response measures and share information.

Belgium will pay special attention to the communication with the public at large.

Actions that will be launched in the framework of ISF Police to remedy the existing shortcomings, will have to take into account the relevant policies at national level:

- The Belgian policy on the **protection of critical infrastructure** is set out by the law on the security and protection of critical infrastructures d.d. 01-07-2011 and the Royal Decree on critical infrastructures in the air transport sector d.d. 02-12-2011. It identifies four priority sectors (energy, transport, finance and electronic communication) and makes a distinction between European critical infrastructures, national critical infrastructures, points of federal interest and points of local interest. Some of the projects Belgium intends to finance through the ISF will not limit themselves to European critical infrastructures but will (also) improve the protection of other possible targets (e.g. the European Institutions during EU summits or soft targets such as large crowds during mass events).
- The Belgian policy on **crisis and security risk management** is set out in a Royal Decree d.d. 16-02-2006. It has a multidisciplinary approach (emergency services; medical, sanitary and psychological aid; police; logistics; information) and organizes both the emergency planning and the management of actual crises at different policy levels (municipality; province; national level), depending on the nature and the impact of the incident.

In both areas, Belgium adopts an all-hazards approach, taking into account all kinds of security risks and threats.

<b>National objective</b>	1 - R - prevention and combating
<b>National objective</b>	2 - R - exchange of information
<b>National objective</b>	3 - R - training
<b>National objective</b>	4 - R - victim support
<b>National objective</b>	5 - R - infrastructure

Our all-hazard approach requires that all partners and target groups take their responsibility and cooperate closely. Therefore, Belgium thinks that it is crucial to consider for funding by ISF the following actions in order to improve the protection of our critical infrastructure:

1. Establishment of effective coordination mechanisms involving all actors concerned,

Example actions:

- Development of a Centre for cybersecurity to identify gaps in our overall security system, create a comprehensive security plan and improve our digital resilience. It will be a multidisciplinary agency, uniting experts from the Belgian telecom regulator, the Federal Police, Fedict (the government's IT service), the Belgian State Security Service, and the Belgian Armed Forces.
- Development of cooperation mechanisms between the public authorities, the private sector and the academic world (cf. B-CCENTRE).
- Development of ICT-tools for the National Crisis Centre to establish National Incident Management Procedures.

Desired Outcome: Improved coordination and cooperation on security issues

2. Facilitate exchange of information in order to prevent threats as well as to warn all the relevant partners and target groups in case of a threat or alert.

Example actions:

- Development of a specific information system for processing security checks prior to issuing airport badges, bringing together information from various sources (Ministry of Justice, municipalities, police, Immigration Office and state security) .
- Purchase of equipment (e.g. telecommunication systems) to ensure an optimal management of security incidents through a fluid exchange of information between the competent authorities.
- Establishment of a secure and robust technical infrastructure for contact information about targets and target groups (hardware, software, maintenance and training).

Desired Outcomes: availability of information equipment and certain information systems in the framework of security information exchange

3. Purchase or develop equipment to protect facilities and infrastructure in order to avoid weak links in the security chain.

Example actions: purchase of equipment to protect the EU institutions during summits, such as vehicles for VIP-escorts, CBRN-E detection equipment, ...

Desired Outcome: the availability of adequate equipment to protect critical infrastructure

4. Organize joint exercises and specific trainings to increase the knowledge and expertise of the various actors concerned.

Example actions: development of specific training programmes for LEOs to ensure the protection of large crowds in public venues or during large-scale events (= soft target protection).

Desired Outcome: Various actors have increased their knowledge and expertise regarding the protection of critical infrastructure.

<b>National objective</b>	6 - R - early warning and crisis
---------------------------	----------------------------------

The ISF funding will support the following main actions:

1. Develop awareness raising activities about potential man-made risks, action perspectives and self-reliance in case of large-scale disasters

Example Actions: development of a portal for the population to inform them about potential man-made disasters and to increase their self-reliance in case of such an incident.

Desired Outcome: increased awareness among the population concerning risks and actions to take in case of disasters

2. Improve the communication with the population in case of a security-related incident. Perform capacity building in this field, in particular training for the staff of the competent authorities and the purchase or development of communication equipment.

Example Action: Establishment of an effective information management system to be used during crisis situations.

Desired outcome: Reduction of the impact of security-related incidents.

3. Develop better communication tools and training for the staff members of the various competent authorities involved.

Example action: Training and exercises for crisis managers on how to deal with data and information during a crisis situation.

Desired Outcome: Improved cooperation between the various competent authorities involved through a better information management

#### 4.Improve contingency plans

Example actions:

- development of contingency plans integrating forensic expertise in case of large-scale man-made disaster (e.g. a terrorist attack in a public venue like the Brussels metro).

Desired Outcome: improved contingency plans

5. Set up of a structure to analyse the occurrence and management of security-related threats and incidents. Its conclusions should be shared (preferably at EU level) in order to undertake further improvements in the field of risk and crisis management and to develop preventive measures.

Example Action: Development of a methodology and a network of (European) experts for the evaluation of the management of the above mentioned incidents, in order to build up knowledge and best practices to manage man-made crisis situations.

Desired Outcome: a developed structure which analyses the occurrence and management of security-related threats and incidents

<b>National objective</b>	7 - R - threat and risk assessment
---------------------------	------------------------------------



## INDICATIVE TIMETABLE

Specific objective	NO/SA	Main action	Name of action	Start of planning phase	Start of implementation phase	Start of closing phase
SO1 - Support common visa policy	a NO1 - National capacity	1	Renovate visa sections	2014	2015	2022
SO1 - Support common visa policy	a NO1 - National capacity	2	Improve information with regard to European visa policy	2014	2015	2022
SO1 - Support common visa policy	a NO1 - National capacity	3	Develop national information platform	2014	2015	2022
SO1 - Support common visa policy	a SA1 - Consular cooperation	1	Schengen Houses Burundi, Rwanda	2014	2015	2022
SO1 - Support common visa policy	a SA1 - Consular cooperation	2	CCM set up of Consular Cooperation Mechanism	2014	2015	2022
SO2 - Borders	NO1 - EUROSUR	1	Action NCC Eurosur	2014	2015	2022
SO2 - Borders	NO3 - Common Union standards	1	ABC	2014	2015	2022
SO2 - Borders	NO4 - Union acquis	1	Action Avia	2014	2015	2022
SO2 - Borders	NO6 - National capacity	1	increase border capacity	2014	2015	2022
SO3 - Operating support	NO1 - Operating support for VISA	1	Action VIS upgrade and maintenance	2014	2015	2022
SO3 - Operating support	NO2 - Operating support for borders	1	SIS II	2014	2015	2022
SO3 - Operating support	NO2 - Operating support for borders	2	Action Belvis	2014	2015	2022
SO5 - Preventing and combating crime	NO1 - C - prevention and combating	1	Develop cooperation between competent organizations	2014	2015	2022
SO5 - Preventing and combating crime	NO1 - C - prevention and combating	2	Participate in joint international joint actions	2014	2015	2022
SO5 - Preventing and combating crime	NO1 - C - prevention and combating	3	Awareness raising of LEOs	2014	2015	2022
SO5 - Preventing and combating crime	NO2 - C - exchange of information	1	Create effective systems for exchange of information	2014	2015	2022
SO5 - Preventing and combating crime	NO2 - C - exchange of information	2	Participate in EMPACT activities	2014	2015	2022
SO5 - Preventing and combating crime	NO3 - C - training	1	Organize trainings and exchange of best practices	2014	2015	2022
SO6 - Risks and crisis	NO5 - R - infrastructure	1	Establish effective coordination mechanisms	2014	2015	2022
SO6 - Risks and crisis	NO5 - R - infrastructure	2	Facilitation of exchange of information	2014	2015	2022

<b>Specific objective</b>	<b>NO/SA</b>	<b>Main action</b>	<b>Name of action</b>	<b>Start of planning phase</b>	<b>Start of implementation phase</b>	<b>Start of closing phase</b>
SO6 - Risks and crisis	NO5 - R - infrastructure	3	Purchase of equipment	2014	2015	2022
SO6 - Risks and crisis	NO6 - R - early warning and crisis	1	Awareness raising activities	2014	2015	2022
SO6 - Risks and crisis	NO6 - R - early warning and crisis	2	Improve communication with the population	2014	2015	2022
SO6 - Risks and crisis	NO6 - R - early warning and crisis	3	Develop communication tools for better cooperation	2014	2015	2022

## 5. COMMON INDICATORS AND PROGRAMME SPECIFIC INDICATORS:

Specific objective	1 - Support a common visa policy			
Indicator	Measurement unit	Baseline value	Target value	Source of data
C1 - Number of consular cooperation activities developed with the help of the Fund	Number	0.00	3.00	Specific Actions
C2.1 - Number of staff trained in common visa policy related aspects with the help of the Fund	Number	0.00	602.00	Projects
C2.2 - Number of training courses (hours completed)	Number	0.00	726.00	Projects
C3 - Number of specialised posts in third countries supported by the Fund	Number	0.00	12.00	Projects
C4.1 - Number of consulates developed or upgraded with the help of the Fund out of the total number of consulates	Number	0.00	94.00	Projects
C4.2 - Percentage of consulates developed or upgraded with the help of the Fund out of the total number of consulates	%	0.00	100.00	Projects
SC1 - Specific Actions: number of Consular Cooperation activities	number	0.00	3.00	Specific Actions
SC2-1 - Specific Actions: trained staff	number	0.00	332.00	Specific Actions
SC2-2 - Specific Actions: number of completed hours of	number	0.00	294.00	Specific Actions

<b>Specific objective</b>	<b>1 - Support a common visa policy</b>			
<b>Indicator</b>	<b>Measurement unit</b>	<b>Baseline value</b>	<b>Target value</b>	<b>Source of data</b>
training of staff				
SC3 - Specific Actions: Schengen Houses: number of specialized posts	number	0.00	2.00	Specific Actions

<b>Specific objective</b>	<b>2 - Borders</b>			
<b>Indicator</b>	<b>Measurement unit</b>	<b>Baseline value</b>	<b>Target value</b>	<b>Source of data</b>
C1.1 - Number of staff trained in borders management related aspects with the help of the Fund	Number	0.00	0.00	Projects
C1.2 - Number of training courses in borders management related aspects with the help of the Fund	Number	0.00	0.00	Projects
C2 - Number of border control (checks and surveillance) infrastructure and means developed or upgraded with the help of the Fund	Number	0.00	7.00	Projects
C3.1 - Number of border crossings of the external borders through ABC gates supported from the Fund	Number	0.00	14,000,000.00	Projects
C3.2 - Total number of border crossings	Number	0.00	49,000,000.00	Projects
C4 - Number of national border surveillance infrastructure established/further developed in the framework of EUROSUR	Number	0.00	1.00	Projects

Specific objective	2 - Borders			
Indicator	Measurement unit	Baseline value	Target value	Source of data
C5 - Number of incidents reported by the Member State to the European Situational Picture	Number	0.00	18,900.00	project

Specific objective	5 - Preventing and combating crime			
Indicator	Measurement unit	Baseline value	Target value	Source of data
C1 - Number of JITs and EMPACT operational projects supported by the Fund, including the participating Member States and authorities	Number	0.00	10.00	Projects
C2.1 - Number of law enforcement officials trained on cross-border-related topics with the help of the Fund	Number	0.00	700.00	Projects
C2.2 - Duration of the training (carried out) on cross-border related topics with the help of the fund	Person days	0.00	700.00	Projects
C3.1 - Number of projects in the area of crime prevention	Number	0.00	5.00	Projects
C3.2 - Financial value of projects in the area of crime prevention	EUR	0.00	1,000,000.00	Projects
C4 - Number of projects supported by the Fund, aiming to improve law enforcement information exchanges which are related to Europol data systems, repositories or communication tools (e.g. data loaders, extending access to SIENA, projects aiming to improving input to analysis	Number	0.00	1.00	Projects

<b>Specific objective</b>	<b>5 - Preventing and combating crime</b>				
<b>Indicator</b>	<b>Measurement unit</b>	<b>Baseline value</b>	<b>Target value</b>	<b>Source of data</b>	
work files etc.)					

<b>Specific objective</b>	<b>6 - Risks and crisis</b>				
<b>Indicator</b>	<b>Measurement unit</b>	<b>Baseline value</b>	<b>Target value</b>	<b>Source of data</b>	
C1 - Number of tools put in place or upgraded with the help of the Fund to facilitate the protection of critical infrastructure by Member States in all sectors of the economy	Number	0.00	5.00	Projects	
C2 - Number of projects relating to the assessment and management of risks in the field of internal security supported by the Fund	Number	0.00	9.00	Projects	
C3 - Number of expert meetings, workshops, seminars, conferences, publications, websites and (online) consultations organised with the help of the Fund	Number	0.00	36.00	Projects	

## **6. FRAMEWORK FOR PREPARATION AND IMPLEMENTATION OF THE PROGRAMME BY THE MEMBER STATE**

### **6.1 Partnership involvement in the preparation of the programme**

A questionnaire has been launched in May 2013 towards all key partners concerned, mostly governmental services like Foreign Affairs, Federal Police, Immigration Office... A majority of contacted partners responded to the questionnaire.

The first analysis of the results on the questionnaire has been discussed in a meeting in June 2013 with the competent ministerial delegations/policy makers. Subsequently, respondents of the questionnaire were given the occasion to validate the analysis or to provide additional information.

The results of the questionnaire served as the basic input to compose the Policy Dialogue and to draft the National Program. During the revisions of the draft NP, all partners were asked to deliver input and extra information, coordinated centrally by the ministry of Home Affairs. The input was given in different ways, mostly by e-mail exchange but also by bilateral meetings and telephone contacts. All partners had at all times access to the latest draft and the minutes of the policy dialogue. Each consulted partner provided the input for the field in which it is responsible, including the indicators. During discussions with the coordination unit these were refined when necessary. The formal submission finally took place on September 29th 2014. Comments received after the formal submission are just as before sent to the relevant partners and reaction is gathered on a bilateral basis.

### **6.2 Monitoring committee**

On 05/02/2014 on inter-ministerial level the decision has been made to set up a monitoring committee (MC). This MC will consist of the relevant cabinets and will be chaired by the president of the FPS Home affairs. The composition will be thematic or politically based upon the matters to be discussed/monitored. The main role of this MC is to validate all important decisions like the selection of projects and the annual reporting to the EC. It will meet when necessary but at least once a year for the annual reporting. These MC meetings can be preceded by a preparatory meeting at the level of the administrations.

The European Funds Unit is responsible to provide all necessary information, like reports, analyses, Audit reports, financial updates, etc. available in due time.

Besides the MC, relevant partners involved in the preparation and implementation will gather on a regular basis in other, more informal working groups. These will be on a project level, bringing together persons working on the project to discuss the progress and the NP in general. The results of these meetings will also serve as input for the MC discussing the progress and implementation on a broader level.

### **6.3 Common monitoring and evaluation framework**

Monitoring is an essential part of the management of the fund and is as such inherently a duty of the RA. The data for monitoring and evaluation will be included in the reports from the project implementers which they submit on defined dates to the RA (exact dates will be included in the grant agreements). In these reports there will be info on the defined common indicators but also on the impact of the project to be used for evaluating the project. The RA will check these data/information during the operational on-the-spot checks and will gather all these data in an electronic system (an excel table is envisaged) to be able to have a clear look on the progress at all time. These collected data will also be presented and discussed in the monitoring and working group meetings, allowing for revisions or improvements of the existing system/programme. The requested evaluations in 2017 and 2024 will preferably be done ‘in-house’, meaning specialized experts inside the administration but outside the RA. Close cooperation with the RA will be necessary to be able to perform a successful evaluation. Outsourcing remains a possibility but is not preferred as the subject requires specific knowledge. For these evaluations visits and interviews will complement the data gathered from reports.

### **6.4 Partnership involvement in the implementation, monitoring and evaluation of the national programme**

See also 6.1 and 6.2

The key partners involved in the preparation will also be involved in the preparatory meeting of the MC introduced in 6.2 (for the broader management of the NP). The partners involved in the preparatory meeting are the relevant administrations (e.g. Home affairs, Foreign Affairs, Federal Police,...). The partners in the MC are the political decision makers (cabinets of the ministers). The MC will decide on strategic issues and will ratify the selection of projects, respecting the agreed NP.

In the working group meetings (for the management on project level) all partners involved in the implementation will be present. They will not necessarily be the same partners as in the MC as they implement the projects and are not necessarily the political decision making partners. The partners in the working group meetings can include besides administration also NGO's, IGO, cities, social welfare institutions, red cross,.... At this level no decisions are taken but the progress of the NP is discussed, issues can be raised and problems can be solved.

There will be feed-back between these two levels of partnership as decisions or remarks made can have influence on both levels. The RA acts as the main interlocutor but most of the administrations will be present on both levels, ensuring a smooth flow of information between both levels.



## **6.5 Information and publicity**

The National Programme will be available on a website. All information about projects, procedures and management of the AMIF will be equally available on this specific website established only for this reason. The website will be regularly updated by the Responsible Authority. After closure of projects, information regarding the achieved objectives and the impact will also be made available for the public through this website.

Practical information on procedures, intermediary decisions and modifications of any kind on the application of the National Programme will be communicated to the project partners through the monitoring committee and working groups. (See 6.2. )

## **6.6 Coordination and complementarity with other instruments**

The NP is prepared in close cooperation with a broad range of partners, of which some are familiar with other Union instruments; no overlapping fields of objectives are present though, because of the very specific objectives of ISF.

In the NP separation is made for some activities which are intended to be complementary with AMIF actions. This too will be closely monitored by the RA, who is conveniently responsible for both the AMIF and the ISF. The ISF will be managed in synergy and complementarity with the European Maritime and Fisheries Fund (EMFF).

As regards the complementarity with other instruments further away from the field of the ISF (and AMIF), the information regarding the actions and projects will be distributed to all involved partners and to representatives and contact persons at different levels (cabinets, coordination units, etc.). Where possible coordination and/or complementarity with other instruments managed or monitored by them will be investigated.

## **6.7 Beneficiaries**

### *6.7.1 List of main types of beneficiaries of the programme:*

State/federal authorities, Local public bodies, International public organisations, Private and public law companies, Education/research organisations.

### *6.7.2 Direct award (if applicable)*

- The National Objectives of ISF Borders S01.001, S01.003, S02.001, S02.002, S02.004 and S02.006 are all related to the competences of governmental departments which have legal or de facto monopolies and will therefore probably use all the direct award.

Under the National Objectives of ISF Police S05.001, S05.002, S05.003 and S06.005 and S06.006 we will mostly use direct award as most of them are part of a competence which is a legal or de facto monopoly. To a lesser extent there will probably also be open calls (for example on cyber crime)

## 7. THE FINANCING PLAN OF THE PROGRAMME

**Table 1: Financing plan ISF-Borders**

<b>Specific objective / national objective</b>	<b>Total</b>
SO1.NO1 National capacity	3,611,979.40
SO1.NO2 Union acquis	
SO1.NO3 Consular cooperation	
<b>TOTAL NO SO1 Support a common visa policy</b>	<b>3,611,979.40</b>
SO1.SA1 Consular cooperation	3,798,000.00
<b>TOTAL SO1 Support a common visa policy</b>	<b>7,409,979.40</b>
SO2.NO1 EUROSUR	182,964.44
SO2.NO2 Information exchange	
SO2.NO3 Common Union standards	2,247,848.82
SO2.NO4 Union acquis	45,741.11
SO2.NO5 Future challenges	
SO2.NO6 National capacity	3,047,092.80
<b>TOTAL SO2 Borders</b>	<b>5,523,647.17</b>
SO3.NO1 Operating support for VISA	4,601,669.40
SO3.NO2 Operating support for borders	2,406,058.99
<b>TOTAL SO3 Operating support</b>	<b>7,007,728.39</b>
Technical assistance borders	1,375,966.04
<b>TOTAL</b>	<b>21,317,321.00</b>

**Table 2: Financial Plan ISF-Police**

<b>Specific objective / national objective</b>	<b>Total</b>
SO5.NO1 C - prevention and combating	9,412,540.00
SO5.NO2 C - exchange of information	5,725,284.60
SO5.NO3 C - training	672,324.00
SO5.NO4 C - victim support	
SO5.NO5 C - threat and risk assessment	
<b>TOTAL SO5 Preventing and combating crime</b>	<b>15,810,148.60</b>
SO6.NO1 R - prevention and combating	
SO6.NO2 R - exchange of information	
SO6.NO3 R - training	
SO6.NO4 R - victim support	
SO6.NO5 R - infrastructure	2,016,973.00
SO6.NO6 R - early warning and crisis	1,344,649.00
SO6.NO7 R - threat and risk assessment	
<b>TOTAL SO6 Risks and crisis</b>	<b>3,361,622.00</b>
Technical assistance police	1,219,566.40
<b>TOTAL</b>	<b>20,391,337.00</b>

**Table 3: Total annual EU commitments (in €)**

	<b>2014</b>	<b>2015</b>	<b>2016</b>	<b>2017</b>	<b>2018</b>	<b>2019</b>	<b>2020</b>	<b>TOTAL</b>
ISF-Borders	3,517,362.00	3,218,915.00	3,687,896.00	2,920,472.00	3,048,376.00	3,112,328.00	1,811,972.00	21,317,321.00
ISF-Police	2,667,592.00	2,703,393.00	2,506,457.00	4,994,524.00	2,506,457.00	2,506,457.00	2,506,457.00	20,391,337.00

**Justification for any deviation from the minimum shares set in the Specific Regulations**

Based on

- the relatively small migration pressure on the external borders (compared to Member States in the East and the South of the Union) and the expected work capacity
- the minimal geographical outline of the external border segments to guard and patrol and by way of embedding EUROSUR in the existing infrastructures and making use of the available capacities of the Belgian police.

**Belgium can fulfil the requirements of the Eurosur directive (art 2.1) with less budget than the 10% of the ISF Borders budget.**

## Documents

Document title	Document type	Document date	Local reference	Commission reference	Files	Sent date	Sent By
----------------	---------------	---------------	-----------------	----------------------	-------	-----------	---------

## Latest validation results

Severity	Code	Message
Info		Programme version has been validated.
Warning	2.15	New EC decision is required for versions > 1. New EC decision is required when fields belonging to the EC decision are modified/added/removed. These fields are all fields except those used in the Authorities section and the Management and Control System field. For the Financial Plan, amounts within a Specific Objective can be modified without the need for a new EC Decision, as long as the total per Specific Objective stays the same.
Warning	2.24.2	SO2.NO1 (Eurosur) (182,964.44) should be minimum 10 % of Total Borders Allocation (NOSO1 + NOSO2 + NOSO3 + TA) (1,751,932.10).