

# PROGRAMMA NAZIONALE ISF

## IDENTIFICAZIONE DELLE AUTORITÀ DESIGNATE

### Autorità competenti responsabili dei sistemi di gestione e di controllo

Autorità	Nome dell'autorità	Nome della persona responsabile per l'autorità	Indirizzo	Indirizzo di posta elettronica	Data di designazione	Attività delegate
Autorità responsabile	PREFETTO MARIA TERESA SEMPREVIVA	MINISTERO DELL'INTERNO –DIPARTIMENTO DELLA PUBBLICA SICUREZZA – DIRETTORE DELL'UFFICIO PER IL COORDINAMENTO E LA PIANIFICAZIONE DELLE FORZE DI POLIZIA	PIAZZA DEL VIMINALE, 1 00186 ROMA	dipps.fondieuropei.segr@interno.it	12-set-2018	
Autorità di audit	DOTT. GIANCARLO VERDE	MINISTERO DELL'INTERNO – DIPARTIMENTO PER LE POLITICHE DEL PERSONALE DELL'AMMINISTRAZIONE CIVILE PER LE RISORSE STRUMENTALI - DIREZIONE CENTRALE PER LE RISORSE FINANZIARIE E STRUMENTALI	VIA CAVOUR, 6 - 00186 ROMA	giancarlo.verde@interno.it		

### Sistema di gestione e di controllo

L'AR, nominata con Decreto del Capo della Polizia-Direttore Generale della Pubblica Sicurezza del 22.04.2014, da ultimo modificato il 12.09.2018, è preposta al coordinamento del Fondo, attuato mediante i seguenti processi:

- programmazione e revisione;
- selezione progetti;
- monitoraggio e avanzamento della spesa;
- controlli finanziari, amministrativi e in loco;
- flusso finanziario;
- *reporting* annuale a CE;
- comunicazione e pubblicità.

Nello svolgimento delle funzioni, l'AR è supportata da una struttura di gestione, la STA, composta da 5 Uffici (Affari generali; Gestione ISF1; Gestione ISF2; Controlli; Economico Finanziario).

L'AdA, nominata con Decreto del Capo Dipartimento PPACRS del 13.08.2014 ed in osservanza al criterio di indipendenza funzionale e gerarchica, garantisce l'efficace funzionamento del SiGeCo e assicura procedure di verifica in linea con gli Standard Internazionali di *Internal Audit*.

CCI	2014IT65ISNP001
Titolo	Italy National Programme ISF
Versione	6.1
Primo anno	2014
Ultimo anno	2020
Ammissibile a partire dal	1-gen-2014
Numero della decisione della CE	C(2020)5620
Data della decisione della CE	13-ago-2020

AUTORITÀ COMPETENTI RESPONSABILI DEI SISTEMI DI GESTIONE E DI CONTROLLO .....	1
SISTEMA DI GESTIONE E DI CONTROLLO .....	1
<b>1. SINTESI .....</b>	<b>4</b>
<b>2. SITUAZIONE DI PARTENZA NELLO STATO MEMBRO .....</b>	<b>6</b>
SINTESI DELLA SITUAZIONE NELLO STATO MEMBRO AL DICEMBRE 2013 IN RELAZIONE AI SETTORI PERTINENTI PER IL FONDO .....	6
1 - SOSTEGNO PER UNA POLITICA COMUNE IN MATERIA DI VISTI .....	11
2 - FRONTIERE .....	14
3 - SOSTEGNO OPERATIVO .....	20
5 - PREVENZIONE E LOTTA ALLA CRIMINALITÀ .....	22
6 - RISCHI E CRISI .....	25
<b>5. INDICATORI COMUNI E INDICATORI SPECIFICI PER PROGRAMMA.....</b>	<b>33</b>
<b>6. QUADRO PER LA PREPARAZIONE E L'ATTUAZIONE DEL PROGRAMMA DA PARTE DELLO STATO MEMBRO.....</b>	<b>35</b>
6.1 COINVOLGIMENTO DEI PARTNER ALLA PREPARAZIONE DEL PROGRAMMA.....	35
6.2 COMITATO DI SORVEGLIANZA.....	35
6.3 QUADRO COMUNE DI MONITORAGGIO E VALUTAZIONE .....	36
6.4 COINVOLGIMENTO DEL PARTENARIATO NELL'ESECUZIONE, NEL MONITORAGGIO E NELLA VALUTAZIONE DEL PROGRAMMA NAZIONALE .....	37
6.5 INFORMAZIONE E PUBBLICITÀ.....	37
6.6. COORDINAMENTO E COMPLEMENTARITÀ CON ALTRI STRUMENTI.....	38
6.7 BENEFICIARI .....	39
6.7.1. <i>Elenco dei principali tipi di beneficiari del programma</i> .....	39
6.7.2 <i>Aggiudicazione diretta (se del caso)</i> .....	39
<b>7. PIANO DI FINANZIAMENTO DEL PROGRAMMA .....</b>	<b>40</b>
TABELLA 1: PIANO DI FINANZIAMENTO ISF-FRONTIERE .....	40
TABELLA 2: PIANO DI FINANZIAMENTO ISF-POLIZIA .....	41
TABELLA 3: IMPEGNI ANNUALI COMPLESSIVI DELL'UE (IN EUR) .....	42
MOTIVAZIONE DI EVENTUALI SCOSTAMENTI DALLE QUOTE MINIME FISSATE NEI REGOLAMENTI SPECIFICI .....	42
<b>DOCUMENTI.....</b>	<b>43</b>
<b>RISULTATI DI CONVALIDA PIÙ RECENTI .....</b>	<b>44</b>

## 1. SINTESI

Il Programma Nazionale (PN) dell'Italia è stato definito a seguito di un ampio processo di concertazione (Cfr. par.6.1). Il PN individua i principali fabbisogni di medio termine nei settori dei visti, delle frontiere e della sicurezza interna, declinandone gli obiettivi prioritari e le attività funzionali al loro conseguimento. Il carattere pluriennale del PN garantisce flessibilità alla programmazione a fronte di nuove sfide che possono emergere in corso di attuazione.

Nell'attuale quadro nazionale, in linea con le Direttive generali del Ministro per l'attività amministrativa e per la gestione 2014 e 2015, volte a definire annualmente priorità politiche, obiettivi e risultati attesi dello SM, risulta prioritario considerare il tema della **sicurezza interna** in relazione al carattere transnazionale che sta facendo emergere minacce globali legate all'instabilità dell'area geopolitica e alla permeabilità delle frontiere.

Relativamente al tema dei **visti e delle frontiere** (OS1 e OS2), al fine di governare il fenomeno migratorio destinato a perdurare nel tempo in termini di intensità, è necessario mettere in campo strategie, risorse e capacità organizzative volte a razionalizzare gli strumenti a presidio delle frontiere per contribuire al rafforzamento dello spazio di libertà, sicurezza e giustizia europeo.

Accanto alla necessità di intensificare il dispositivo di sicurezza alle frontiere e ottimizzare il rilascio visti, la globalizzazione del crimine impone una maggior cooperazione in ambito transnazionale volta a sviluppare strategie di **prevenzione e contrasto** in una logica di sviluppo degli scambi informativi e di comunicazione tra i sistemi di *intelligence* (OS5 e OS6).

Gli **obiettivi** che si intendono raggiungere sono:

**OS1:** armonizzare ed elevare gli standard di qualità ed efficienza del VIS al fine di migliorare le procedure d'ingresso legale di cittadini non comunitari e innalzare gli standard di sicurezza, ottimizzare le procedure di rilascio di visti, potenziare la rete di scambio con le sedi consolari per diminuire i tempi di esecuzione, rafforzando le competenze del personale.

**OS2:** (i) rafforzare la capacità di sorveglianza e contrasto dei flussi migratori illegali con l'acquisto di mezzi e strumenti per la sorveglianza delle frontiere; (ii) potenziare i sistemi informativi per l'analisi del rischio e il quadro situazionale nazionale per uno scambio integrato di informazioni attraverso lo sviluppo della rete EUROSUR–NCC; (iii) rendere più efficienti i controlli sulle persone presso i BCPs attraverso il potenziamento delle dotazioni strumentali, dei sistemi informativi (SIS-II, SDI, Dati API, I-VIS, BCS) e l'introduzione di nuove tecnologie (ABC gates, SIF-IS, EES); (iv) sviluppare le competenze degli operatori di frontiera, anche per innalzare la capacità di identificazione dei migranti; (v) a seguito di accordi di cooperazione con Paesi Terzi, potenziare la capacità di controllo dei flussi dai Paesi di origine e/o transito mediante l'invio di ILO'S e Esperti Immigrazione, l'assegnazione di risorse strumentali per scambio informazioni e l'erogazione di formazione alle FFPP straniere.

**OS3:** garantire continuità ed efficienza delle acquisizioni prevedendo misure di assistenza tecnica e manutenzione di sistemi e infrastrutture, di sostituzione attrezzature per il controllo delle persone e la comunicazione/scambio dati, di

supporto logistico di mezzi, di ristrutturazione di immobili e corsi di formazione.

Lo strumento ISF2-Borders&Visa assegna a OS1 il 3,01% delle risorse, a OS2 il 79,23% (di cui 28,07% Frontex equipment), a OS3 il 14,63% e alle attività AT il 3,13%.

**OS5:** (i) promuovere la cooperazione tra FFPP degli SM e istituzioni europee mediante investimenti in tecnologie performanti e la creazione di piattaforme per lo scambio di esperienze e *best practice* negli ambiti del traffico di stupefacenti, armi e rifiuti, immigrazione illegale, sfruttamento sessuale e pedopornografia, indagini finanziarie, segnalazioni sospette, falsificazione e riciclaggio, infiltrazione negli appalti pubblici e nella PA, corruzione, crimine informatico e controllo del territorio; (ii) ottimizzare gli strumenti di prevenzione basati sull'interoperabilità, attraverso l'integrazione di banche dati, sistemi informativi e centrali operative; (iii) potenziare la prevenzione e la vigilanza dei tentativi di infiltrazione mafiosa negli appalti pubblici ed intensificare le misure di antiriciclaggio dei proventi illeciti delle cosche.

**OS6:** promuovere interventi volti a prevenire situazioni di crisi ed emergenza in materia di terrorismo, CBRN-E, *cybercrime*, sicurezza alimentare e protezione delle infrastrutture critiche informatiche, orientando la strategia verso attività di intelligence, formazione qualificata, sviluppo di infrastrutture IT e nuove funzionalità dei sistemi per lo scambio dati.

Lo strumento ISF1-Police assegna a OS5 il 78,09% delle risorse, a OS6 il 17,21% e alle attività di AT il 4,7%.

## 2. SITUAZIONE DI PARTENZA NELLO STATO MEMBRO

### Sintesi della situazione nello Stato membro al dicembre 2013 in relazione ai settori pertinenti per il Fondo

#### OS1

Il MAECI dispone di **166 Uffici Consolari**, di cui **162** emettono **visti Schengen** con investimenti ordinari di oltre 106M€. La RMV collega il MAECI con le sedi consolari, secondo le specifiche tecniche e normative del VIS (13,3M€ da EBF di cui: 3M€ per sviluppo SW; 6,8M€ per gestione VIS; 3,5M€ per acquisto attrezzature HW/SW). Il VIS è composto da L-VIS, FeVIS e N-VIS (con componente I-VIS) ed è connesso al C-VIS e al SIF-II. Le funzionalità del VIS MAIL (fase I e II), Vision e M-VIS sono aggiornate.

Nel 2014, a seguito di un aumento delle domande di visti (+6% rispetto al 2013) e del numero crescente di visti emessi da 400 operatori pari a ca. 2.062.501 +7% rispetto al 2013), unitamente alla complessità delle procedure, alla gravosità economica e ai cambiamenti normativi, è emersa la necessità, seppur disomogenea tra le Sedi, di:

- aggiornare i sistemi IT che elaborano i visti per migliorarne l'efficienza;
- garantire armonizzazione e efficienza delle procedure di rilascio visti;
- riqualificare le competenze degli operatori per garantire l'applicazione uniforme delle procedure (nel 2014, con EBF, formati 339 operatori nazionali e 92 operatori per ca. 200k€).

Nel quadro della cooperazione consolare, l'Italia ha aderito nel 2014 alla *Maison Schengen Kinshasa*. A tal proposito, si ritiene necessario rafforzare con altri SM la rete di contrasto al fenomeno dei falsi documentali nelle domande di visto mediante elaborazione di procedure *ad hoc*, condividendo relative *best practices* che consentano di delineare i fattori di rischio (*profiling*).

#### OS2

L'Italia è uno dei principali Paesi Schengen di destinazione e/o transito dei flussi migratori lungo le rotte del Mediterraneo. Nel 2014 sono sbarcati ca. 170.100 migranti irregolari (+396% rispetto al 2013).

Il bilancio 2013 mostra un impegno finanziario nazionale per la gestione ed il controllo delle frontiere esterne pari a ca. 398M€. Il controllo delle frontiere esterne e il contrasto dei flussi migratori illegali è coordinato dal MI-DCIF, con il concorso di GdF, MM, CdP-GC.

Il dispositivo di **sorveglianza delle frontiere** impiega 328 mezzi marittimi (di cui 43 EBF), 104 mezzi aerei (di cui 13 EBF) e oltre 1600 mezzi terrestri (principalmente acquisiti con EBF) per pattugliare il territorio, l'NCC e la Sala EUROSUR a cui fanno capo 7 Sistemi e Servizi informativi e le relative dotazioni tecnologiche presso le aree sensibili o a bordo dei mezzi citati, preposti alla raccolta e successiva analisi/elaborazione delle informazioni, oltre che alla rappresentazione degli scenari (quadri situazionali) tra i Centri di Coordinamento Nazionali e Regionali. I dati raccolti dalla GdF (C4I), MM (SMART) e CdP-GC (SAFE SEA NET e PELAGUS) o dai Servizi Satellitari realizzano un flusso informativo verso i sistemi SIA e SATM della PS (15M€) e da questi, successivamente, verso l'NCC e la Sala EUROSUR. L'NCC (ca. 7,9M€ di cui 6,9M€ da fondi ordinari) opera come cabina di regia per il

monitoraggio e la gestione di eventi migratori, tramite il dialogo con le Centrali Operative di GdF (ICC), MM (CINCNAV) e CdP-GC (Comando Generale di Roma).

I **controlli delle persone** alle frontiere sono svolti ai valichi marittimi e aerei, tramite 167 *Border Cross Point* (54 aerei e 113 marittimi), 4800 operatori di frontiera, 3 sistemi centrali di frontiera (SIF-IS, BCS per 69,5M€ di cui 67,5 M€ da fondi ordinari e I-VIS per 10,3M€ comunitari, oltre 1M€ EBF), 9 sistemi informativi centrali di back end (N-VIS, C-VIS, CEN-PKI/EAC e PSE, SDI, SIS II, SIDAF/FADO, AFIS e MIPGWEB), 817 postazioni SIF Client (5M€ da fondi ordinari), 600 postazioni mobili per accesso a SDI/SIS II (2,2M€ da fondi ordinari), 8 varchi automatici *eGates* sperimentali a FCO, strumenti IT e servizi di 2 linea per verificare l'identità della persona e controllare i documenti alterati o falsi. I passeggeri extra Schengen che, nel 2013, hanno attraversato le frontiere sono oltre 39M: ca. 7.000 sono stati respinti e oltre 5.000 documenti contraffatti sono stati sequestrati. Il trasferimento di migranti, nel 2014, ha richiesto investimenti nazionali per 22M€. A supporto dei dispositivi di sorveglianza e controllo, la PS ha sviluppato il **sistema SMSI-RA** per l'analisi dei rischi per le rilevazioni FRAN (500k€ con EBF e 1,5M€ da fondi ordinari).

L'Italia ha operato in chiave preventiva con forme di **cooperazione con i Paesi Terzi** per contrastare le organizzazioni criminali che lucrano sul traffico di migranti (187M€ negli ultimi 10 anni, di cui oltre 17M€ con fondi comunitari), rafforzando le competenze degli operatori di frontiera (più di 1.000 formati nel 2014).

Secondo le raccomandazioni della Commissione Schengen, l'Italia ha rafforzato il dispositivo di gestione delle frontiere. EBF ha contribuito al pattugliamento aereo, marittimo e terrestre (145M€, 65M€ e 38M€), all'implementazione di sistemi e strumentazioni ICT (203M€) e alla formazione (17M€). Tuttavia, l'evoluzione dello scenario internazionale (nel 2014 +396% migranti e +126% eventi emergenza/SAR), i fenomeni di mobilità globale (EXPO 2015, Giubileo...), unitamente alle incerte evoluzioni geopolitiche, porteranno un aumento straordinario ed incontrollato dei flussi alle frontiere. Sarà necessario agire in maniera preventiva e operativa, attraverso investimenti in sistemi e infrastrutture per rafforzare lo scambio di informazioni e la cooperazione tra le autorità nazionali nel quadro EUROSUR. Tali investimenti, unitamente all'acquisto di mezzi e attrezzature, miglioreranno la conoscenza situazionale e la capacità di reazione alle frontiere esterne permettendo di individuare, prevenire e combattere l'immigrazione clandestina, la criminalità transfrontaliera e contribuire alla protezione e la salvezza della vita dei migranti. Inoltre, è necessario continuare a rafforzare le competenze degli operatori presenti sul territorio nazionale e nei Paesi Terzi per armonizzare le conoscenze e diffondere *best practices* in materia di controllo e gestione delle frontiere. In tema di prima accoglienza, la mediazione culturale e l'interpretariato sono assicurate durante le operazioni di soccorso e nelle zone di sbarco.

## SO5 e SO6

Nel 2014, l'attività di **prevenzione e contrasto alla criminalità** ha registrato l'arresto di 175.241 soggetti (di cui 72.584 stranieri); sono stati, inoltre, arrestati 1616 soggetti per crimini mafiosi, di cui 64 stranieri. L'Italia, *driver* di 2 priorità del **Policy Cycle 2011-13**, proseguirà tale impegno nel 2014-17, ove ricoprirà tale ruolo in 3 priorità su 8.

In coerenza con il PD e le strategie di Governo, si riporta la *baseline* dei temi individuati:

1) **Traffico di droga**: sequestrati stupefacenti per 152t (+111% del 2013) in 19.449 operazioni e segnalate all'Autorità Giudiziaria 29.474 persone. Sono in aumento rispetto al 2013 i sequestri di hashish (+211,3%),

marijuana (+15,9%) e eroina (+5,3%), in flessione quelli di cocaina (-21,9%). Le droghe sintetiche, reperite anche sul web, rappresentano la sfida futura (dal 2009 identificate oltre 370 nuove molecole).

Dal 2010 al 2014, la DCSA ha sequestrato 178,1t di droga alle frontiere marittime, di cui 73% riconducibili ad attività svolte prevalentemente con MAOC-N (già beneficiario I-SEC per circa 3,8M€). È necessario presidiare le rotte del narcotraffico valorizzando la cooperazione giudiziaria interforze (Convenzione di Vienna 1988 e Strasburgo 1990) e rafforzando le attività di contrasto in mare.

2) **Indagini finanziarie:** la crescente infiltrazione nell'economia e finanza anche attraverso circuiti alternativi (*money transfer*) per riciclare proventi illeciti richiede una capacità di analisi delle transazioni finanziarie anomale; nel 2014 sono pervenute 75.742 SOS, di cui 449 trattenute per scopi investigativi antimafia. L'assetto organizzativo nazionale per la specifica azione di prevenzione e contrasto prevede, nell'ambito del DPS, il coinvolgimento interforze della DIA e di ROS, SCO e SCICO.

La DIA ha sequestrato 3,167MLD€ e confiscato 642M€; ha inoltre eseguito 168 accessi ai cantieri con 4899 persone fisiche e 1234 persone giuridiche controllate.

Alla luce del Piano *Nazionale Anticorruzione* (introdotto l'11.9.2013) e nel rispetto delle leggi 190/2012 e 69/2015 (aumento delle pene sui reati contro la PA; falso in bilancio e associazione per delinquere di stampo mafioso), si mira a potenziare attività ispettive, investigative e di prevenzione dell'infiltrazione negli appalti pubblici anche mediante la costituzione di una rete europea antimafia (es. progetto CAPACI). Significativa risulta l'azione di collaborazione tra FFPP, ANAC e PA per prevenire la corruzione e aumentare l'uso efficiente delle risorse, riducendo i controlli formali anche mediante l'istituzione di Sezioni/Unità Anticorruzione presso le Squadre Mobili di PS, nonché l'avvio di interventi con Paesi terzi per sviluppare progetti *twinning* ed IPA (progetto "Balcani occidentali").

3) **Scambio di Informazioni:** in adesione alle Decisioni di Prüm, è stata istituita la banca dati nazionale del DNA per comparare profili genetici di persone implicate in procedimenti penali. È necessario proseguire l'adeguamento del sistema APFIS ai requisiti tecnici e livelli di servizio richiesti dall'UE.

E' necessario implementare infrastrutture ICT per scambio dati su: frodi documentali, armi da fuoco, voci di soggetti noti autori di reato, comunicazioni in situazioni di crisi, controllo del territorio, pronto intervento, soccorso pubblico

4) **Cybercrime:** dal 01.01.2013 al 31.10.2014 le FFPP hanno trattato 169.941 casi di *cybercrime*, con 9494 denunce e 106 arresti. Nel 2014, in materia di prostituzione minorile: 171 reati, 435 denunciati/arrestati e 71 vittime; in materia di pornografia minorile: 19913 siti web monitorati, di cui 1746 inseriti in *black list*, 343 reati, 408 denunciati/arrestati e 293 vittime (incluse vittime di adescamento). Lo SM ha istituito i CNAIPIC e CNCPO e supporta la prevenzione nelle scuole su pedopornografia e cyberbullismo. E' stato realizzato il progetto OF2CEN per lo scambio di informazioni, dati ed *early warning*. Il *cybercrime* richiede una collaborazione pubblico/privato (Conferenza ISS tra DGHHome e COSI, sett.2014) e ha condotto ad una collaborazione tra PS, CNR e professionalità accademiche per la creazione di un Centro di studi e ricerca.

5) **CBRN-E:** l'Italia è *focal point* per la predisposizione del piano di azione per uniformare l'approccio degli SM. È stato predisposto il "Piano nazionale di difesa da attacchi terroristici CBRN" che individua minacce, possibili scenari e contromisure da adottare. Il monitoraggio *real time* sul trasporto di sostanze nucleari è assicurato dalla



cabina di regia del MI-DPS; inoltre, per il rilevamento della radioattività, sotto l'egida del MI-DVFPDC, si dispone di una rete nazionale di ca. 1300 stazioni automatiche.

Circa il possesso illecito di armi ed esplosivi, nel 2014 sono state sequestrate 214 armi, 2 detonatori, e ca. 564 grammi di tritolo.

In futuro sarà necessario implementare la rilevazione dei dati CBRN sul territorio nazionale, nonché aumentare la dotazione individuale e dei reparti operativamente coinvolti in caso di attacchi.

6) **Radicalizzazione e terrorismo**: è stato istituito il CASA quale strumento di condivisione e valutazione delle informazioni e dei rischi per la sicurezza nazionale. Nel 2014 si è riunito 53 volte, affrontando 465 casi e tra questi ha vagliato 255 segnalazioni relative a criticità da approfondire, delle quali 212 hanno riguardato il contesto internazionale, Italia inclusa. L'Italia è interessata da due matrici terroristiche:

- nazionale: nel 2014, 64 attentati incendiari/esplosivi, 8 arresti e 333 intercettazioni;
- internazionale sul web: nel 2014, 13 espulsioni, 11 arresti e 248 intercettazioni.

Per prevenire e contrastare tali fenomeni, incluso il reducismo, si necessita di avanzati mezzi e strumenti d'intelligence, nonché di adeguata formazione e addestramento.

7) **Tratta e traffico di esseri umani**: nel 2014, 17 vittime accertate, di cui il 23,5% minori con provenienza da Nigeria, Romania, Albania, Bulgaria, Serbia e Montenegro. Il MI ha attivato, altresì, l'osservatorio OSCAD. Tra le iniziative di successo si segnala ITA.RO per il contrasto delle organizzazioni dedite alla tratta e il progetto per lo "sviluppo di linee guida per l'identificazione del THB" con Frontex. Appare necessario fronteggiare la tratta di esseri umani attraverso strategie interconnesse di prevenzione, tutela e contrasto a livello nazionale e transnazionale.

8) **protezione della catena alimentare**: nel 2014 oltre 10.000 reati e ca. 11.280 segnalazioni riferite a persone denunciate/arrestate in Italia in violazione della normativa sulla contraffazione alimentare, occorre quindi combattere il crimine alimentare attraverso la cooperazione tra FFPP.

9) **traffico illecito di rifiuti**: nel 2014 ca. 146 crimini e 710 condanne (violazione art. 259 del D.lgs. n.152/2006), occorre quindi contrastare traffico e smaltimento illecito di rifiuti mediante iniziative di formazione e sviluppo di soluzioni IT.

10) in materia di **protezione di testimoni**, l'Italia ha approvato disposizioni normative per regolamentare il *whistleblowing* in risposta ad accordi internazionali (L.112/2012, L.116/2009) ma l'unico tentativo di protezione si trova nella L.190/2012. Il governo ha incaricato l'ANAC di raccogliere le segnalazioni con il portale ALAC (da 12.2014 a 02.2015, ca. 40 segnalazioni).

Funzionale all'assetto delineato è il rafforzamento delle competenze degli operatori: nell'ambito delle attività di CEPOL l'Italia, nel 2014, ha formato ca. 700 rappresentanti delle FFPP.

Gli investimenti nazionali nel 2013, riconducibili a *Crime* sono 6.830,84M€ e a *Crisis* sono 23,34M€.

Gli investimenti ISEC e CIPS hanno riguardato: protezione e monitoraggio infrastrutture critiche (7,8M€), condivisione e gestione flussi di informazioni e dati (5,5M€), traffico esseri umani (4M€), gestione eventi critici (3M€), crimine organizzato (9M€), crimine minorile (5,6M€).

### 3. OBIETTIVI DEL PROGRAMMA

<b>Obiettivo specifico</b>	<b>1 - Sostegno per una politica comune in materia di visti</b>
----------------------------	---

L'Italia intende attuare un piano d'azione concreto ed integrato per rispondere alle sfide connesse al sostegno di una politica comune in materia di visti.

La strategia nazionale mira allo sviluppo della situazione raggiunta, anche grazie al sostegno di EBF, per rendere l'ingresso legale in Europa più efficace per i cittadini non comunitari, innalzando al contempo gli standard di sicurezza.

Con le risorse nazionali disponibili il MAECI sostiene costi relativi al supporto delle strutture centrali e periferiche, al finanziamento del personale di ruolo nazionale ed estero, alle attività di contenzioso relative ai visti, all'acquisto di *sticker*, alla gestione dell'infrastruttura S-RIPA.

Dall'analisi dei fabbisogni emersi, si ritiene prioritario assicurare l'adeguamento tecnologico, con riferimento al potenziamento del VIS e delle sue articolazioni, per il rafforzamento dei controlli alle frontiere in ragione dell'andamento crescente delle domande di visto e delle criticità registrate nella rete consolare. Inoltre, tale adeguamento risulta preminente per la complessità tecnica e delle esigenze di aggiornamento del VIS, dovute a innovazioni normative, richieste operative di gestione, informatizzazione di procedure più efficienti e rapide.

In particolare, sarà determinante concentrare gli investimenti di ISF in:

- aggiornamento/evoluzione dei sistemi informatici che elaborano i Visti, garantendo che tutte le componenti dell'infrastruttura diventino pienamente operative;
- armonizzazione e semplificazione delle procedure di emissione dei visti, assicurando al contempo la securizzazione dei dati contenuti;
- migrazione della connettività di rete, eliminando pericolosi *bottleneck* che possono realizzarsi nell'interconnessione di nodi di rete;
- sistema di *disaster recovery*;
- attività di dematerializzazione di documenti cartacei in formato digitale e sicuro;
- sistema di *data warehouse* con relativo ampliamento del sistema SAN.

Posto che l'emissione dei visti dipende dalle capacità professionali degli operatori, si ritiene prioritario rafforzare le competenze tecniche del personale delle sedi consolari mediante l'erogazione di corsi sulla normativa e sulle funzioni operative dei sistemi informatici dedicati, al fine di omogeneizzare il livello professionale nelle aree geografiche.

Lo SM intende, inoltre, rafforzare la cooperazione consolare soprattutto laddove le esperienze nazionali sono limitate, collaborando e condividendo *know-how* e *best practices* con altri Paesi.

A fronte di *trend* crescenti delle domande di visto, sebbene l'Italia intenda promuovere la diffusione di forme innovative di organizzazione degli uffici consolari, allo stato non si ritiene di chiedere finanziamenti a valere su ISF in materia di cooperazione consolare Schengen. Fermo restando l'obiettivo di lungo termine di adottare Centri Comuni Europei, ad oggi, sono stati coinvolti solo piccoli Paesi.

L'Italia, grazie al finanziamento ISF, intende raggiungere i seguenti risultati:

**I. Miglioramento degli standard di qualità ed efficienza del VIS** con attività volte a potenziarne le *performance*, tenendo conto degli sviluppi tecnologici e normativi attraverso:

- l'adeguamento normativo del Sistema, l'evoluzione delle componenti del sistema I-VIS (centrale e periferico), anche nella componente di comunicazione con i sistemi di *back up e disaster recovery* e nella componente relativa ai servizi di interoperabilità e cooperazione con i sistemi nazionale **N-VIS**, comunitario **C-VIS** e di frontiera **SIF-IS**; l'accesso alla RMV e al DB dei visti extra Schengen da parte degli Uffici di Frontiera;
- lo sviluppo di SW per il rilascio visti con l'introduzione di nuove funzionalità, compresa una piattaforma *outsourcing* che, mediante il SW *VISA Out* ed in conformità con l'art. 43 del *VISA Code*, consenta alle agenzie esterne di accedere da remoto, tramite protocolli sicuri, e di inserire dati biometrici inviando la pratica all'Ufficio Consolare di competenza;
- sviluppo di SW per supporto agli utenti e SPoC (*Single Point of Contact*).

**II. Adeguamento dell'infrastruttura tecnologica in uso e rafforzamento della rete di scambio dei Server delle Sedi consolari**, anche in funzione di esigenze future, mediante:

- implementazione dell'interfaccia telematica del MAECI in un **Portale interattivo per i visti Schengen**, fruibile dagli addetti degli Uffici consolari e dagli *end user*;
- implementazione archivio informatico (*data warehouse*) per la raccolta ed elaborazione di dati relativi ai visti per fini analitici e statistici.

**III. Potenziamento della connettività delle Sedi Consolari** per ottimizzare i tempi di *processing* in termini di gestione, stoccaggio e costi di conservazione della documentazione, mediante l'acquisto di HW e SW per:

- Mobile-VIS volto ad acquisire pratiche di visto e biometrie da una postazione itinerante; il Test-VIS (T-VIS) finalizzato ad effettuare test di verifica; il *VISA Out*;
- *disaster recovery* e *business continuity*;
- **l'aggiornamento dei sistemi centrali/periferici** (nuovi server; ampliamento rete *Storage Area Network* per adeguamento spazio memorizzazione dati; aggiornamento postazioni client con PC e periferiche).

**IV. Potenziamento delle infrastrutture informatiche per migliorare l'efficienza e la rapidità del VIS e promuoverne l'interconnessione con i Partner Schengen**, mediante l'evoluzione della piattaforma integrata per la verifica di test congiunti con i Paesi Schengen (*Provisional System Acceptance Test*), per la validazione degli applicativi presso il C-VIS, per le modifiche al T-VIS riportate nel nuovo *Test Design Description* pubblicato dall'Agenzia Europea riguardanti i nuovi messaggi, l'adeguamento del carico per i *load test* e la generazione di specifico traffico simulato.

L'attuazione effettiva ed efficace dell'*acquis* dell'Unione in materia di visti sarà garantita attraverso **l'aggiornamento del personale** già operante presso gli Uffici Visti delle sedi consolari e la **diffusione di conoscenze e competenze** a favore del nuovo personale assegnato, nell'ottica di assicurare continuità operativa al servizio di emissione visti.

L'obiettivo sarà implementato da un lato mediante **l'istituzione progressiva di standard condivisi** per gli operatori in materia di normativa, strumenti e pratiche comuni per l'espletamento delle attività, e dall'altro attraverso un **rafforzamento della specializzazione delle conoscenze**, anche al fine di incoraggiare l'utilizzo di tecnologie nuove ed avanzate. Si prevedono corsi di formazione da erogare durante l'intero periodo di programmazione, pianificati secondo le esigenze normative e operative.

Dall'analisi della situazione di partenza è emerso che le sedi consolari per le quali si è registrato un considerevole miglioramento della gestione dei processi sono quelle in cui il personale in servizio ha conseguito livelli di professionalità elevati, grazie all'adeguamento delle competenze raggiunto mediante la fruizione di corsi di formazione specifica. La volontà di proseguire **l'attività di formazione del personale** risponde altresì alle esigenze di mitigazione dei rischi connessi ad una cattiva gestione nel settore di visti Schengen.

Pertanto, è prioritario definire **piani di formazione ad hoc** che tengano conto del livello di competenza e della relativa distribuzione riscontrata nelle varie sedi consolari, al fine di raggiungere un livello omogeneo di preparazione in linea con gli standard comunitari.

Si prevede dunque la progettazione di varie tipologie di corsi di formazione, in modalità frontale ed e-learning. A seguito dell'individuazione di gap di competenze di ciascuna sede, saranno definiti **corsi modulari integrati**, al fine di fornire formazione mirata in relazione alle esigenze del personale operante. Si riportano di seguito - a titolo non esaustivo - i principali temi oggetto dei moduli formativi da finanziare con ISF:

- Normativa Schengen e UE (Codice visti, Regolamento VIS e Codice delle Frontiere Schengen);
- SIS II;
- Organizzazione degli uffici visti e valutazione delle pratiche di visto;
- Codice dei Visti: tipologie di visto;
- L'esame della domanda di Visto Schengen;
- Documentazione falsa;
- *Outsourcing* per la trattazione per le pratiche di visto Schengen;
- Cooperazione Consolare Locale;
- Codice etico: gestione del rischio e corruzione In connessione con i visti d'ingresso brevi.

Attraverso le attività di formazione, il risultato auspicato è **l'implementazione di attività efficaci che consentano la continuità operativa al servizio di emissione visti Schengen.**

<b>Obiettivo nazionale</b>	3 - Cooperazione consolare
----------------------------	----------------------------

<b>Azione specifica</b>	1 - Cooperazione consolare
-------------------------	----------------------------

**I. Consular Cooperation Mechanism on Schengen Visa Processing (CCM)**, avanzata dal Belgio (*leader*) con partnership del MAECI per la lotta alla falsificazione dei documenti in materia di visti e al fenomeno del *visa shopping*.

CCM si basa su:

- valutazione congiunta di rischi e trend nei Paesi terzi più a rischio in materia di falso documentale e immigrazione irregolare
- dislocamento di *joint document verification officers* per verificare l'autenticità dei documenti presentati a supporto delle domande di visto Schengen
- dislocamento di ILO'S ed *Schengen Visa Experts* per formare SM e operatori consolari locali nell'analisi di documenti emessi dai Paesi Terzi e trend di abusi
- rafforzare la *capacity building* nei Paesi terzi per aumentare l'affidabilità dei documenti a supporto dei visti Schengen.

Le attività sono:

- invio di *document verification officers* in 7 Paesi terzi (scelti dallo *Steering Group*);
- invio di *Joint Immigration Officers* e *Schengen Visa Experts* per formare: (i) gli operatori consolari e *document verification officers*; (ii) le autorità nazionali su scambio informazioni, *best practice* e metodi di prevenzione/lotta agli abusi;
- creazione e mantenimento a livello centrale di uno *Steering Group* per il controllo strategico del progetto. A livello locale, costituzione di un *Gruppo di Lavoro Antifrode* per condividere informazioni e analizzare i trend.

L'Italia sarà direttamente coinvolta a livello centrale nelle attività dello *Steering Group* e auspica una fattiva partecipazione a livello locale. La contribuzione sarà di natura finanziaria nella misura di 5.200 €/anno a valere sui fondi nazionali.

**II. Regional Schengen Cooperation Officers (RSCO)** avanzata dall'Olanda (*leader*) con partnership del MAECI per la creazione di uffici di cooperazione Schengen in 4 Sedi in Paesi terzi ad alto rischio migratorio allo scopo di rafforzare il processo di emissione visti e la lotta alla falsificazione.

Il progetto prevede l'invio di *Regional Schengen Cooperation Officers*, esperti dei Paesi aderenti deputati a raccolta e diffusione di informazioni necessarie per la valutazione delle domande di visto in tema di immigrazione clandestina, lotta alla falsificazione e formazione.

L'Italia auspica una diretta e fattiva partecipazione a livello locale. La contribuzione potrebbe essere di natura finanziaria o *in kind*; si fa riserva di comunicare ulteriori informazioni.

<b>Obiettivo specifico</b>	<b>2 - Frontiere</b>
----------------------------	----------------------

Per la sicurezza interna dell'UE, l'Italia conferma una politica incentrata sulla gestione integrata delle frontiere esterne, anche attraverso operazioni congiunte Frontex e accordi di cooperazione con Paesi Terzi e organizzazioni internazionali, d'intesa con l'UE e in linea con i principi di cooperazione interistituzionale in materia di gestione delle frontiere dell'UE definiti nel *2013 Guideline for cooperation between border Guards and customs administration*.

L'approccio strategico ed operativo che si intende perseguire al fine di soddisfare le sfide identificate nella *baseline* si incentra, pertanto, sulle seguenti priorità:

**I. Rafforzamento della Governance**, da condividere con Frontex, mediante lo sviluppo della capacità di analisi dei rischi. È fondamentale continuare a sviluppare i sistemi a vocazione europea (SIS II) e nazionale (SMSI-RA) di elaborazione e analisi dei dati per identificare tendenze e minacce relative ai flussi migratori, determinare i principali fattori di rischio, individuare i Paesi Terzi con i quali cooperare.

È, altresì, indispensabile assicurare il pieno utilizzo delle potenzialità di EUROSUR e le autorità nazionali continueranno a sviluppare l'NCC e la sala EUROSUR, le centrali operative nazionali di rispettiva competenza, al fine di promuovere il dialogo tra Stati Membri, Frontex e le autorità nazionali stesse. A tal fine, l'Italia si doterà di una strumentazione atta a prevenire reati transfrontalieri e, al contempo, ad individuare e fornire assistenza e soccorso alle imbarcazioni di migranti, nel rispetto degli obblighi europei e internazionali.

**II. Sorveglianza delle frontiere e contrasto dei flussi migratori illegali** attraverso le attività di pattugliamento, sorveglianza e controllo in mare, la raccolta dei dati dei viaggiatori che attraversano la frontiera portuale e aeroportuale, la supervisione dello spazio aereo e delle acque territoriali e l'identificazione/verifica dei migranti presso gli Uffici di Frontiera. È necessario implementare nuove componenti, funzioni e servizi, limitate o non disponibili, sui principali sistemi informativi in uso (SIA, SATM, SIF-IS, BCS, C4I, SAFESEANET...) e acquisire attrezzature tecnologiche, aggiuntive o in sostituzione di quelle esistenti.

**III. Controllo delle persone e sorveglianza efficace dei BCP** aerei e marittimi, applicando strumenti e protocolli in armonia col Codice Schengen. Determinante l'utilizzo di nuove tecnologie (es. *ABC Gates*, EES) e la cooperazione di tali strumenti con i sistemi informativi di frontiera ed i sistemi centrali di *back end* (SIF-IS, BCS, I-VIS, SIS II, SDI, Interpol, PSE, StranieriWeb, PKI/EAC, ecc.).

**IV. Rafforzamento delle competenze** del personale coinvolto in operazioni di controllo, pattugliamento e soccorso dei naufraghi e degli *end user* di mezzi/sistemi. In tema di prima accoglienza, rafforzamento di mediazione culturale e interpretariato da assicurare nelle operazioni di soccorso e nelle zone di sbarco.

<b>Obiettivo nazionale</b>	1 - EUROSUR
----------------------------	-------------

Per garantire il pieno utilizzo di EUROSUR e assicurare lo scambio d'informazioni tra le autorità nazionali e Frontex, l'Italia propone iniziative per la progressiva attuazione del sistema di gestione integrata delle frontiere UE, conformemente a norme, protocolli e standard operativi/tecnici internazionali, comunitari e nazionali.

Le azioni da finanziare sono finalizzate a ricondurre "a sistema" il complesso flusso informativo che perviene all'NCC e a ridistribuirlo tra tutte le istituzioni (nazionali e non) in modo più performante.

Considerato il complesso assetto istituzionale e la convergenza sull’NCC di tutte le autorità nazionali coinvolte nella gestione dei flussi, ai fini della realizzazione del NSP appare prioritario orientare le attività verso l’adeguamento delle funzionalità esistenti, il miglioramento delle procedure operative e la creazione di nuove interconnessioni.

Le priorità, finalizzate all’evoluzione e al **potenziamento tecnologico/operativo** sono:

- acquisizione ed installazione di strumenti tecnologici ed apparati per la comunicazione (es. apparati radio, antenne satellitari e apparecchiature TX/RX di segnali audio video e dati) e ottimizzazione delle operazioni di tracciamento e identificazione di mezzi e/o individui in mare;
- evoluzione dei sistemi informativi e delle attrezzature ICT preposti alla sorveglianza e/o ai controlli presso la frontiera marittima ed aerea. Gli applicativi saranno oggetto di una reingegnerizzazione per renderli conformi e coerenti con i protocolli tecnici ed operativi, nazionali e comunitari, in continua evoluzione.

Inoltre, sarà curata **la riorganizzazione e l’adeguamento delle infrastrutture informatiche** deputate a localizzazione, tracciamento e identificazione di natanti e/o migranti mediante:

- adeguamento tecnologico dei siti radar e delle reti informatiche per la predisposizione di sensori atti a localizzare e identificare individui in mare;
- acquisizione di radar, camere, sensori, sistemi di gestione video/immagini, per la scoperta e il tracciamento degli assetti aeronavali e la classificazione/identificazione di persone;
- ammodernamento, riorganizzazione e reingegnerizzazione di NCC, della sala EUROSUR, della Centrale Operativa dell’*Italian Maritime Rescue Coordination Center* e delle *server farm* in uso.

Infine, potranno essere finanziati interventi volti al rafforzamento della capacità operativa delle Amministrazioni impegnate nel controllo e sorveglianza delle frontiere esterne dell’Unione, che concorrono alla **gestione dell’emergenza epidemiologica da COVID 19**.

I risultati che l’Italia auspica raggiungere sono:

- **ottimizzazione e integrazione dei flussi informativi *real time* e *near real time*** raccolti dagli attuali sistemi nazionali di sorveglianza;
- **aggiornamento costante della NSP.**

<b>Obiettivo nazionale</b>	2 - Scambio di informazioni
----------------------------	-----------------------------

L’NCC e la Sala EUROSUR assicurano uno scambio immediato tra autorità nazionali, altri SM e Frontex di informazioni sulla situazione alle frontiere e di relazioni analitiche e di *intelligence*, tramite NSP. Per garantire un flusso informativo efficace ed efficiente, le priorità finanziarie di ISF sono:

- lo sviluppo di componenti per interconnettere NCC, Sala Eurosur, Frontex, nodi/sistemi classificati nazionali e internazionali;



- l'evoluzione di sistemi e apparecchiature per scambio informazioni *real-time* con i sistemi e servizi informativi e di comunicazione (SIF, BCS, SIA e SATM, Servizi Satellitari e di accesso a *Registri Navali*, ...);
- l'aggiornamento e l'adeguamento tecnologico componente *data center* dei mezzi impegnati nel controllo delle frontiere;
- la securizzazione e il consolidamento del flusso informativo, anche mediante sistemi di *back-up* e *disaster recovery*, dei sistemi di bordo per la protezione delle infrastrutture da minacce alla sicurezza;
- l'adeguamento della componente tecnologica a bordo dei mezzi impiegati in operazioni di pattugliamento ed eventualmente coinvolti in operazioni SAR (art. 3(5) del Reg. (UE) 515/2014) per incrementarne la comunicazione ed assicurare lo scambio di informazioni tattiche.

In linea con l'art.3(3b) del Reg. (UE) 515/2014 sono previsti interventi di potenziamento e rinnovo della rete di scambio e dei sistemi preposti all'analisi del rischio (SMSI-RA) e alla definizione del COB. Saranno altresì potenziati strumenti tecnologici per raccogliere dati di monitoraggio (tramite SIA-Terze Sezioni, SATM-registro Lloyd's, dati satellitari e motore semantico) e supportare gli Uffici preposti all'analisi del rischio.

Mediante il potenziamento del sistema di supporto alle decisioni nella componente relativa alle frontiere sarà possibile affiancare all'archivio dati lo specifico *data warehouse* che, insieme al package SW di Business intelligence, sosterrà lo sviluppo del COB per disporre di dati utili all'analisi del rischio e alla permeabilità delle frontiere.

Tutte le suddette priorità permetteranno di combinare le informazioni ottenute, classificate e non, mediante indirizzamento al dispositivo di sorveglianza dell'NCC, per costruire una NSP e una mappa del rischio (con relativo COB). Tramite apposite apparecchiature di separazione e collegamento monodirezionale, tali input confluiranno sulla rete informativa della Sala EUROSUR, ove convergono tutti i collegamenti e le informazioni classificate; sistemi, Enti/Organismi che trattano informazioni classificate, saranno collegati a questa Sala.

Il risultato che l'Italia intende perseguire è l'**incremento della capacità di controllo, comunicazione e scambio d'informazioni *real time*** tra gli assetti impegnati in attività di controllo e le Centrali operative regionali e nazionali.

<b>Obiettivo nazionale</b>	3 - Norme comuni dell'Unione
----------------------------	------------------------------

Per far fronte alla crescita esponenziale dei viaggiatori che attraversano le frontiere, l'Italia riconosce l'importanza dell'utilizzo di tecnologie avanzate e interoperabili, al fine di rafforzare il controllo delle frontiere e facilitare i movimenti di cittadini dell'UE e, nel futuro, anche di altri viaggiatori (TCN). Pertanto, risultano priorità finanziarie di ISF tutte le sotto elencate linee di intervento.

In linea con la normativa applicabile (D.lgs 196/2003; Direttiva UE 82/CE/2004, D.lgs 144/2007 e Decreto Interministeriale del 16.12.2010) il DPS-DCIF ha già realizzato e reso operativo il sistema BCS: un sistema in grado di trattare le informazioni fornite dai Vettori nella fase di *check-in* e di imbarco dei viaggiatori, per eseguire i controlli sulla persona e sui documenti prima dell'attraversamento della linea di frontiera, allertando se del caso gli operatori ed i sistemi preposti ai controlli manuali ed automatici (*eGates*). In tale ambito, mediante ISF l'Italia intende assicurare l'implementazione della "*frontiera virtuale avanzata*" marittima, similmente a quella già in uso per i Vettori aerei (sistema BCS – Dati API) attraverso il collegamento al sistema P-MIS delle Capitanerie di Porto.

L'Italia, inoltre con i finanziamenti di ISF mira ad un potenziamento dei sistemi di controllo automatizzati con l'utilizzo dei sistemi ABC (secondo gli standard di Frontex) presso i principali porti e aeroporti nazionali e la loro integrazione e cooperazione con il sistema informativo frontiere (SIF-IS), per usufruire di tutti i servizi di interoperabilità e di accesso alle banche dati di *back end* (per esempio, con il sistema I-VIS, SIS II, SDI, Interpol, PKI/EAC, SIDAF/FADO,...). In tal modo, anche attraverso il riuso delle librerie SW utilizzate nelle verifiche manuali (*SIF Client*), i controlli automatici e di verifica biometrica in ciascun *eGate* potranno essere considerati a tutti gli effetti equivalenti alle componenti di controllo automatico implementate nella postazione (*SIF Client*) di verifica manuale presso i varchi dei BCP. Le postazioni *SIF Client*, distribuite sia sulla prima che sulla seconda linea di controllo, sono strumenti in grado di supportare le verifiche di genuinità dei documenti cartacei ed elettronici anche di ultima generazione.

Il risultato atteso è il **rafforzamento del controllo dei valichi di frontiera** grazie all'utilizzo di **tecnologie avanzate ed interoperabili**, per assicurare dei controlli più performanti alle frontiere ed essere al contempo in linea con gli standard europei.

<b>Obiettivo nazionale</b>	4 - Acquis dell'Unione
----------------------------	------------------------

L'attuazione effettiva ed efficace dell'*acquis dell'Unione*, mediante le priorità finanziarie di ISF, sarà assicurata con la diffusione di conoscenze e competenze a favore del personale nazionale ed internazionale impiegato nelle operazioni di controllo delle frontiere (Codice Schengen) e dei flussi migratori, contrasto dell'immigrazione clandestina, pattugliamento delle frontiere esterne ed eventualmente soccorso dei naufraghi, nonché del personale dedicato alla gestione ed implementazione dei sistemi tecnologici.

In particolare le priorità finanziarie di ISF sono:

- corsi di **formazione specialistica** (addestramento) e *recurrent training* a favore del personale impiegato in attività di controllo delle frontiere, da seguire eventualmente all'estero;
- corsi di **formazione linguistica** (ad es. lingua inglese, francese, arabo etc.) a beneficio del personale e degli operatori di Frontiera, ed in generale della autorità nazionali competenti;
- corsi di formazione **per gli operatori impegnati lungo le frontiere aeree e marittime** sulle tecniche di controllo e di interrogatorio, nonché di approccio culturale che gli operatori devono seguire per interagire efficacemente con i migranti mediante comunicazione verbale e non;
- corsi di **formazione specialistica ICT** ed aggiornamento periodico per utilizzatori di sistemi/software per la gestione delle frontiere e apparecchiature di controllo documentale;
- corsi di **formazione per gli operatori delle polizie di frontiera in Paesi Terzi** aventi ad oggetto moduli su prevenzione e contrasto all'immigrazione irregolare per favorire lo scambio informativo e l'applicazione uniforme di *best practices* tra operatori nazionali ed esteri. Tali corsi potrebbero eventualmente essere oggetto di accordi di cooperazione con i Paesi Terzi per rafforzarne le capacità di gestione delle frontiere Schengen.

Nel generale potenziamento delle capacità di controllo dei Paesi più esposti al traffico dei flussi migratori si prevede altresì di finanziare con ISF corsi di formazione dedicata alle FFPP straniere (previa sottoscrizione di accordi internazionali) aventi ad oggetto modalità di contrasto all'immigrazione clandestina, rilevazione e investigazione di crimini transfrontalieri, falso documentale, tecniche investigative nei servizi di polizia, cooperazione e controllo alle frontiere, controllo del mare, scorte e sicurezza, guida nel settore nautico e terrestre.

I risultati auspicati sono, da un lato, istituire progressivamente **standard condivisi per gli operatori di frontiera in materia di normativa, strumenti e buone pratiche** per l'espletamento delle proprie attività e, dall'altro, **rafforzare le conoscenze e successivamente specializzare le capacità** al fine di incoraggiare l'uso delle tecnologie nuove ed avanzate.

<b>Obiettivo nazionale</b>	5 - Sfide future
----------------------------	------------------

Premesso che tutte le priorità nazionali del Programma rappresentano di per sé sfide future, al fine di rafforzare la capacità di far fronte a sfide imminenti, tra le priorità finanziarie di ISF a valere di questo ON vi è l'acquisto di aeromobili a pilotaggio remoto al fine di avviare una sperimentazione operativa di questa nuova tecnologia nelle attività di gestione e controllo delle frontiere esterne che consenta di rispondere alle sfide presenti e future connesse al fenomeno migratorio irregolare.

<b>Obiettivo nazionale</b>	6 - Capacità nazionale
----------------------------	------------------------

Il PN intende finanziare l'acquisizione di **infrastrutture, sistemi ed attrezzature** per i controlli e l'approvvigionamento di **mezzi aerei, marittimi e terrestri** per pattugliamento, SAR e trasporto migranti. Tra le priorità vi sono:

- acquisto di Uffici mobili e apparati fissi, mobili e trasportabili per verifiche biometriche e documentali e fotosegnalamento interoperabili con i principali sistemi in uso: SDI, SIS, AFIS e EURODAC
- adeguamento/realizzazione di infrastrutture per identificazione dei migranti, controllo delle persone alle frontiere o verifica della posizione di cittadini di Paesi Terzi presso *hotspot* e principali luoghi di sbarco, BCP e Uffici preposti al contrasto della migrazione illegale
- acquisto di mezzi aerei, marittimi e terrestri, dotati di sensori di sorveglianza aeromarittima e di telerilevamento per individuazione di persone in mare e pattugliamento delle frontiere
- acquisto di mezzi e l'installazione di attrezzature sanitarie per attività di primo soccorso e operazioni SAR
- adeguamento tecnologico e estensione della capacità di sistemi installati o da installare presso UUNN
- potenziamento della rete di *Esperti Immigrazione nei Paesi Terzi e Guardie di frontiera negli Stati Membri UE* (esperti ex l. 189 del 30.7.2002) e degli ILO'S, d'intesa con i Paesi Terzi interessati
- sviluppo e implementazione del sistema UE **EES**. Per questa azione prioritaria, i finanziamenti verranno allocati come indicato nella Sezione 7 del PN
- sviluppo e implementazione del sistema UE **ETIAS**. Per questa azione prioritaria, i finanziamenti verranno allocati come indicato nella Sezione 7 del PN
- supporto ad un aggiornamento rapido e efficace delle **componenti nazionali del SIS** in linea con le disposizioni del Regolamento (UE) 2018/1861. Per questa azione prioritaria, i finanziamenti verranno allocati come indicato nella Sezione 7 del PN
- rafforzamento dei controlli sistematici alle frontiere esterne anche in relazione ad eventuali raccomandazioni da parte di Organismi competenti (es. CE, Valutazioni Schengen)
- mediazione culturale e linguistica per agevolare la comunicazione tra FFPP e stranieri nelle fasi di soccorso e/o sbarco dei migranti, di preidentificazione e di foto-segnalamento

Si intende sviluppare pacchetto *Smart Borders* anche nella componente di comunicazione con sistemi di *backup e disaster recovery*, cooperanti con sistemi SIF-IS, I-VIS. Sono previsti interventi di aggiornamento/adeguamento infrastruttura SISII e applicazione SIRENE II, ex Reg. 987/2006 e Dec. 2007/533/GAI

I risultati da raggiungere:

- incremento attività di **sorveglianza aerea e marittima**
- **potenziamento capacità** di far fronte al possibile incremento dei flussi migratori
- rafforzamento **capacità operativa per il controllo delle frontiere**

**Azioni Specifiche Borders:** EUR 8,786,137.50 assegnati ai sensi del Regolamento Delegato (UE) 2020/446

<b>Azione specifica</b>	<b>2 - Strumenti FRONTEX</b>
-------------------------	------------------------------

Nel quadro dell'art.7 del Reg. 515/2014, nel 2015, l'Italia ha formalizzato la proposta di acquisto di mezzi di trasporto e attrezzature operative ritenute necessarie per l'effettuazione di operazioni congiunte e da mettere a disposizione della *European Border and Coast Guard Agency – EBCGA* (ex Frontex) in conformità ai criteri di cui all'articolo 39, par. 5 e 9, del Regolamento(UE) n. 2016/1624 del Parlamento europeo e del Consiglio. A seguito di un complesso processo di valutazione, la Commissione Europea, con comunicazione e-mail del 16 marzo 2015, ha informato l'Italia circa l'ammissione a finanziamento di **tre Azioni specifiche**. Nello specifico, trattasi di:

- **Acquisto di n.1 Pattugliatore classe 300(SEA-OPV-01-SEAOP)**, l'evoluzione della classe 800, può contenere fino a 4 persone a bordo. Ha una capacità operativa di 16 ore e può navigare fino a 30 nodi;
- **Acquisto di n.1 Pattugliatore per operazioni marittime(SEA-CPV-02-SEAOP)**, un mezzo con autonomia operativa di 86 ore, può navigare ad una velocità di 40 nodi ed è dotato di alcuni sensori, tra i quali il sistema di navigazione e sorveglianza 2D;
- **Acquisto di n.1 Velivolo ad ala fissa per operazioni marittime(AIR-FWA-02-SEAOP)**, configurato per operazioni marittime, comprensivo di supporto tecnico, logistico e di formazione per piloti e specialisti.

Inoltre, il 21 Aprile 2017, l'Italia ha formalizzato due proposte progettuali sull'acquisto di attrezzature da mettere a disposizione dell' *EBCGA*, che a seguito del processo di valutazione sono state ammesse al finanziamento dalla CE e rese note con comunicazione Ares(2017)4444342 del 12/09/2017. In particolare, si tratta di:

- **Acquisto di n.1 Coastal Patrol Vessel**, una unità Classe 200 con autonomia di circa 600 miglia nautiche;
- **Acquisto di n.3 Coastal Patrol Boats**, vedette velocissime multiruolo con scafo performante in materiale composito, velocità massima di 50 nodi e lunghezza complessiva 20 metri.

Infine, in data 6 luglio 2018 l'Italia ha presentato diverse proposte progettuali per l'acquisto di attrezzature da mettere a disposizione in operazioni congiunte EBCGA, di cui sono state valutate positivamente le seguenti:

- **Acquisto di n.1 Off-Shore Patrol Vessel (OPV)**, un'imbarcazione con scafo performante in acciaio, della lunghezza di circa 55 mt. e velocità massima pari a non meno di 25 nodi;
- **Acquisto di n.3 Coastal Patrol Boat (CPBs)**, vedette velocissime della lunghezza tra i 18 e i 20 mt. e velocità massima pari a non meno di 30 nodi;
- **Acquisto di n.1 Coastal Patrol Vessel (CPV)**, un'imbarcazione della lunghezza di circa 80 mt. e velocità massima pari a non meno di 14 nodi.

<b>Obiettivo specifico</b>	<b>3 - Sostegno operativo</b>
----------------------------	-------------------------------

Italia conferma la sua conformità all'acquis dell'Unione in materia di frontiere e visti.

Italia conferma la sua conformità alle norme e agli orientamenti dell'Unione per la buona governance in materia di frontiere e visti, in particolare al catalogo Schengen sui controlli alle frontiere esterne, al manuale pratico per le guardie di frontiera e al manuale relativo ai visti.

<b>Obiettivo nazionale</b>	1 - Sostegno operativo per i visti
----------------------------	------------------------------------

□

La Polizia di Stato potrà disporre di quota parte del cofinanziamento di *Operating Support* di ISF per finanziare attività di assistenza tecnica e manutenzione del sistema I-VIS componente nazionale dell'N-VIS.

Il MAECI potrà disporre di quota parte del cofinanziamento di *Operating Support* di ISF da utilizzare per la manutenzione dei sistemi di competenza. A titolo esemplificativo, la manutenzione potrà riguardare:

- *software* dedicati alla gestione e al rilascio dei Visti;
- piattaforma integrata di test e validazione per il Sistema Centrale e l'interconnessione con i Partner Schengen, ai fini dell'adeguamento alle specifiche tecniche risultanti dalle direttive della CE.

Inoltre, il MAECI potrà disporre del cofinanziamento al fine di ristrutturare/ampliare le sedi consolari, esclusivamente per ricevere/processare domande di visto Schengen e l'ulteriore sviluppo della cooperazione consolare in materia di rilascio dei visti Schengen, anche allo scopo di migliorare l'accoglienza e la sicurezza delle stesse.

<b>Obiettivo nazionale</b>	2 - Sostegno operativo alle frontiere
----------------------------	---------------------------------------

□

La Polizia di Stato, la Marina Militare, la Guardia di Finanza ed il Corpo delle Capitanerie di Porto potranno disporre di quota parte del cofinanziamento di *Operating Support* per finanziare mediante ISF le seguenti attività:

- ristrutturazione di immobili, ed in particolare delle principali scuole di formazione (ad es: CAPS di Cesena), di hangar ed uffici per la custodia di velivoli e dei locali dell'attuale sede del Centro Nazionale di Coordinamento (NCC) - Sala EUROSUR - per il trattamento di informazioni UE *Restricted*;
- assistenza tecnica e manutenzione delle infrastrutture e della rete in fibra ottica degli Uffici di Polizia centrali e periferici; i cui costi saranno imputati al Fondo per la quota parte di competenza;
- potenziamento ed ammodernamento di infrastrutture logistico/operative ed apparecchiature di comunicazione e scambio dati (UHF, TCDL, sistemi satellitari e di comunicazione acustica, sistemi AIS, ecc.);
- manutenzione e/o sostituzione delle attrezzature per la verifica dei documenti e dell'identità delle persone al momento dell'attraversamento alle frontiere;
- assistenza tecnica e manutenzione di infrastrutture, sistemi ed attrezzature utilizzati per la gestione integrata delle frontiere (ad es: NCC; SIA; SATM; SIF-IS; SMSI-RA; BCS; C4Iecc);
- acquisto di licenze software e servizi di supporto specialistico per la gestione di malfunzionamenti dei sistemi informatici e *disaster recovery*;
- manutenzione e gestione operativa (compresa Manutenzione Correttiva - MAC e Manutenzione Evolutiva - MEV) dei Sistemi SIS II e SIRENE II;

- manutenzione e supporto logistico integrato di mezzi terrestri, aerei e marittimi per garantirne la continuità operativa nell'ambito di operazioni nazionali e/o congiunte (es. Frontex);
- costituzione di presidi tecnici volti a garantire l'efficienza e la continuità operativa delle postazioni radar costiere, nonché efficientamento/aggiornamento dei sistemi di sorveglianza radar e terminali satellitari;
- corsi di formazione specialistica/aggiornamento.

<b>Obiettivo specifico</b>	<b>5 - Prevenzione e lotta alla criminalità</b>
----------------------------	---

In linea con le strategie del COSI sulla base del SOCTA l'Italia adotterà misure di --prevenzione e contrasto nonché di coordinamento e cooperazione sulla base di un approccio integrato, flessibile e operativo a livello nazionale e internazionale (EUROPOL, EUROJUST, CEPOL, ecc).

Si intende assicurare il potenziamento di strumenti e tecnologie, lo sviluppo di processi di identificazione ed il rafforzamento di nuove forme di cooperazione tra le FFPP, anche in vista di EXPO 2015 e Giubileo 2016, nei seguenti ambiti:

- traffico illecito di stupefacenti, armi e rifiuti;
- favoreggiamento immigrazione illegale;
- sfruttamento sessuale e pedopornografia online;
- indagini di natura finanziaria, segnalazioni sospette, falsificazione e riciclaggio;
- infiltrazione negli appalti pubblici e nei diversi settori della Pubblica Amministrazione;
- prevenzione della corruzione a livello nazionale (in linea con il PNA approvato dall'ANAC) e locale;
- controllo del territorio, pronto intervento e soccorso pubblico;
- crimine informatico (anche tramite la partecipazione all'EC3).

Sul narcotraffico si intendono incrementare capacità e competenze degli operatori, le dotazioni dei laboratori forensi e il coordinamento delle FFPP, per rendere le indagini più rapide, efficienti ed efficaci.

Sul CBRN-E si potenzierà la capacità di prevenzione e risposta ad attacchi, migliorando le dotazioni degli operatori, anche attraverso l'utilizzo di tecnologie di disinnescamento ed una più qualificata formazione.

Si considera determinante lo scambio di informazioni, cooperazione internazionale e condivisione di esperienze/metodi operativi, anche in tema di radicalizzazione e terrorismo.

Per dare attuazione alle Dec.2008/615/GAI e 2008/616/GAI si intende potenziare le infrastrutture IT, e sviluppare le funzionalità del Portale IXP-BDN DNA per armonizzare le procedure e creare un unico sistema per gli uffici investigativi. Si intendono sviluppare anche dati integrate su specifiche tematiche tra cui indagini balistiche, armi, rilevamento di impronte, intercettazioni, etc.

Sarà garantita la formazione di operatori, anche *webinar*, su *cybercrime* (in collaborazione con centri di ricerca, CERTs e FFPP), terrorismo, antidroga, indagini finanziarie, falso documentale, contraffazione, in linea con buone pratiche di CEPOL. Si promuoverà la cooperazione per addestramenti comuni per il personale addetto ai servizi di sorveglianza e protezione.

Si contribuirà all'attuazione del PNR e si favoriranno lo scambio di informazioni e l'interoperabilità con i sistemi UE o sistemi di altri SM.

In materia di protezione di vittime non si ritiene di chiederne finanziamento su ISF per le valutazioni espresse nel NO4. Stessa considerazione per la valutazione dei rischi e minacce (NO5). Si fa riserva di riprogrammare interventi per sopraggiunte necessità. Con riferimento al *whistleblower* in assenza di una legislazione puntuale non si ritiene di poter presentare progetti e si fa riserva di presentarne nell'ambito della Revisione.

<b>Obiettivo nazionale</b>	1 - C - prevenzione e lotta
----------------------------	-----------------------------

Si prevedono interventi di:

- prosecuzione delle attività connesse al MAOC-N, in partenariato con altri SM, per il contrasto del traffico illecito di droga via mare e aerea;
- realizzazione di centri di indagine e reazione in caso di emergenze informatiche e allestimento presso il CNCPO di tecnologie per il rilevamento delle impronte delle sorgenti digitali ;
- acquisto di attrezzature per la prevenzione e il contrasto al *cybercrime*(es. abusi su minori *online* e frodi home banking e monetica);
- implementazione di sistemi IT per la prevenzione e contrasto al *terrorismo online*;
- creazione di strutture per attività investigative e di contrasto alle organizzazioni criminali (con Europol, Eurojust e CE) e di una *rete europea antimafia*;
- acquisto HW/SW per delle potenziare le capacità delle FFPP per di contrasto alla corruzione;
- realizzazione di un laboratorio forense avanzato per analisi chimiche molecolari, per identificare, ad esempio, droghe sintetiche;
- acquisto di strumenti IT per il contrasto dei traffici illeciti in porti, aeroporti;
- partecipazione al Policy Cycle ad es. sui temi di immigrazione illegale, contraffazione di beni, ecc.;
- acquisto di sistemi di intercettazione per l'identificazione e il monitoraggio di tentativi di comunicazione con l'esterno da parte dei reclusi e terroristi;
- acquisto di sistemi per la rilevazione di utenze mobili (es. GSM/UMTS/LTE);
- realizzazione di strutture anti-intercettazione per le FFPP a tutela della riservatezza in fase di indagini giudiziarie;
- acquisto di strumenti per la rilevazione di ordigni esplosivi e relativo disinnescio;
- rafforzamento della cooperazione tra le istituzioni pubbliche e private attraverso la maggiore interoperabilità degli strumenti tecnologici per il controllo del territorio e lo scambio di informazioni in *real time*;
- in linea con i contenuti dell'*EU Action plan to support the protection of public spaces*, realizzazione di sistemi evoluti di videosorveglianza ed analisi intelligente in contesti territoriali circoscritti per il rafforzamento della capacità investigativa delle FFPP in materia di antiterrorismo, traffici illeciti e criminalità organizzata;
- sviluppo di sistemi IT e analisi dati a supporto della capacità operativa delle FFPP;
- acquisto di servizi di interpretariato specialistico a supporto delle indagini;
- acquisto di strumenti IT per operazioni di fotosegnalamento e identificazione;
- acquisto di strumenti di intelligence ed ICT a sostegno dell'analisi investigativa e delle attività di indagine finalizzate anche alla lotta contro la criminalità transfrontaliera correlata alla tratta ed il traffico di esseri umani.

Il risultato previsto è di **aumentare la sicurezza delle informazioni e della rete, rafforzare la capacità di indagine e combattere la criminalità.**

<b>Obiettivo nazionale</b>	2 - C - scambio di informazioni
----------------------------	---------------------------------

Si prevede:

- potenziamento sistema di rilevazione dati digitali (AFIS) e palmari (APIS) per i reparti operanti sul territorio;
- potenziamento infrastrutture IT e implementazione delle funzionalità del sistema di scambio dati sulla comparazione e tipizzazione dei profili genetici (banca dati DNA);
- implementazione di dotazioni IT per il pattugliamento del territorio, facilitando lo scambio d'informazioni *real time* e la gestione di input informativi;
- realizzazione di un network integrato in campo balistico e miglioramento degli attuali sistemi 3D automatizzati per la memorizzazione e il confronto di residui di sparo/proiettili di armi da fuoco, interoperabile con altri sistemi, come, ad es. IBIN di Interpol (che collega gli IBIS nazionali) e TRAX 3D della PS;
- realizzazione di un sistema investigativo e di identificazione interfacciato con le banche dati contenenti informazioni sui soggetti detenuti;
- realizzazione di un banca dati per prodotti grafici e “specimen” documentali, per garantire il riconoscimento biometrico della scrittura e l'identificazione dei mezzi scriventi;
- adeguamento della banca dati nazionale SIDAF, così da condividere gli *alert* e velocizzare gli scambi di informazione tra le autorità competenti;
- implementazione di database di voci di soggetti autori di reato, accessibile da tutte le FFPP sia per l'inserimento che per l'identificazione dei singoli parlatori;
- potenziamento del canale SIENA, per un migliore quadro di *intelligence* relativo alla criminalità organizzata;
- creazione/organizzazione di piattaforme per lo scambio di esperienze e buone pratiche tra operatori delle FFPP, anche nell'ambito della prevenzione, della radicalizzazione e terrorismo;
- implementazione di attività e infrastrutture per scambio/utilizzo dati, per favorire la cooperazione tra SM ed UE, prevenire e contrastare il traffico transfrontaliero, ad esempio, di stupefacenti, la contraffazione dei mezzi di pagamento (anche attraverso la creazione di una banca dati della falsificazione dell'Euro) e il traffico illecito di rifiuti;
- sviluppo della *Passenger Information Unit* mediante implementazione di nuovi sistemi IT per il PNR;
- potenziamento/realizzazione di soluzioni IT per aumentare lo scambio di informazioni con altri SM e l'interoperabilità con i sistemi dell'UE o altri SM;
- ottimizzazione delle procedure di scambio dati tra il CNAIPIC e omologhi organismi internazionali, avviando lo sviluppo di sistemi di supporto all'analisi big data.

Il risultato atteso è il **rafforzamento delle capacità di analisi** per fenomeni delittuosi e criminali e il **miglioramento qualitativo dello scambio a livello centrale e periferico**. Saranno realizzati/implementati banche dati e sistemi IT volti all'archiviazione, tracciamento e identificazione delle diverse fonti dei dati.

<b>Obiettivo nazionale</b>	3 - C - formazione
----------------------------	--------------------

Con il finanziamento di ISF si prevede la realizzazione di piattaforme informatiche (*learning space*) integrate con i sistemi informativi già in uso, che supportino l'attuazione delle politiche UE in materia di formazione basata sul modello ETS - *European Training Scheme*, con particolare riferimento al programma LETS.



Inoltre, al fine di accrescere le competenze delle FFPP nel settore della prevenzione e contrasto dei fenomeni criminali internazionali, il Fondo ISF supporterà seminari e corsi di formazione rivolti al personale (anche di prima linea) impiegato nei seguenti ambiti:

- comparazione dei profili DNA, anche al fine di potenziare la cooperazione inter-istituzionale tra Italia, Stati Membri, Europol ed altri attori competenti;
- attività sotto copertura per la lotta al traffico illecito di sostanze stupefacenti;
- protezione interna ed esterna delle reti IT degli uffici addetti alla trattazione di documenti sensibili e informazioni riservate di rilevanza operativa su criminalità organizzata, terrorismo, radicalizzazione e cyber crime (*hackeraggio*);
- tecniche e tattiche di contrasto, prevenzione, indagine e custodia in materia di terrorismo, estremismo violento e criminalità organizzata;
- indagini economico-finanziarie, metodi investigativi nonché riciclaggio, circolazione transfrontaliera di valuta, corruzione, patrimoni illeciti, reati finanziari e finanziamento del terrorismo, anche per smantellare le reti criminali;
- custodia dei detenuti terroristi nelle sezioni penitenziarie di alta sicurezza e prevenzione del proselitismo e radicalizzazione nelle sezioni comuni;
- custodia dei detenuti sottoposti a regime di carcere duro;
- attività di tutela delle personalità pubbliche nazionali/estere e delle persone che, per le funzioni esercitate, sono soggette a pericoli o minacce;
- prevenzione e contrasto delle discriminazioni e nella rilevazione della presenza di crimini di odio (*hate crimes*);
- attività connesse alla realizzazione di una rete europea operativa antimafia volta a prevenire e contrastare infiltrazioni di stampo mafioso nel sistema degli appalti;
- attività di contrasto alla gestione illecita dei rifiuti, ivi incluse le rotte transnazionali dei relativi traffici;
- attività di formazione e aggiornamento della dirigenza delle FFPP, con particolare riferimento al coordinamento interforze e di cooperazione internazionale per investigazione e contrasto delle organizzazioni criminali.

Il risultato auspicato dall'Italia è il **miglioramento della cooperazione transnazionale tra FFPP**, in linea con le indicazioni comunitarie CEPOL e ENLETS, mediante la diffusione omogenea di competenze specialistiche (in materia di prevenzione e contrasto di fenomeni criminali transnazionali) e tecnologiche (attrezzature IT).

<b>Obiettivo nazionale</b>	4 - C - sostegno alle vittime
----------------------------	-------------------------------

Si prevedono interventi a supporto di **categorie vulnerabili**, quali ad esempio, in analogia con l'art.21, Capo V, della Direttiva 2013/33/UE, minori, MSNA e donne in stato di gravidanza vittime di reati quali la tratta di esseri umani, attraverso l'utilizzo di modalità operative e tecnologie in grado di tutelare lo stato di fragilità e debolezza delle stesse in fase di indagine.

<b>Obiettivo nazionale</b>	5 - C - valutazione dei rischi e delle minacce
----------------------------	--

<b>Obiettivo specifico</b>	<b>6 - Rischi e crisi</b>
----------------------------	---------------------------

La strategia per la prevenzione e il contrasto di situazioni di crisi ed emergenza si sviluppa su temi di preminente interesse quali terrorismo, attacchi CBRN-E, *cybercrime*, protezione di reti informatiche nonché prevenzione della catena alimentare (in continuità con BACCUS e SECUFOOD, finanziati con ISEC).

In materia di prevenzione delle minacce terroristiche interne e internazionali, si prevede la prosecuzione di attività preventive, anche per limitare proselitismo e radicalizzazione, quali ad esempio interventi volti ad incrementare le capacità professionali e l'addestramento per operazioni ad alto rischio, nonché sviluppare sistemi di intercettazione delle comunicazioni.

Attesa la positiva esperienza italiana si va ipotizzando la costituzione, presso Europol, di un analogo *fusion center* a livello europeo con particolare riferimento all'esigenza di contrastare il fenomeno dei *foreign fighters*.

Inoltre, è prioritario gestire e contrastare il fenomeno della propaganda via web, principale vettore delle minacce terroristiche, in relazione al quale si registra un trend crescente ad intraprendere percorsi radicali, anche di singoli individui (reducismo). L'azione di prevenzione e contrasto si attuerà mediante attività di intelligence e di sviluppo di sistemi IT in grado di operare in un tale contesto.

Da tale quadro emerge la necessità di prevedere azioni di prevenzione e gestione di attacchi CBNR-E, mediante:

- potenziamento di apparati di rilevazione della radioattività;
- acquisto di mezzi, eventualmente dotati di tecnologie avanzate (robot) per fornire risposte rapide in caso di attacchi;
- potenziamento delle dotazioni individuali e di reparto degli operatori destinati ad attività di prevenzione/contrasto;
- sviluppo sistemi IT e reti per il coordinamento in situazioni di crisi;
- formazione specialistica, anche per operatori sanitari.

Con riguardo alla protezione delle infrastrutture critiche informatiche, la strategia mira a rafforzare le architetture infrastrutturali mediante l'innalzamento degli standard di sicurezza di reti e la relativa resilienza. In particolare si prevede:

- sviluppo di piattaforme IT di esplorazione, ricerca, estrazione ed analisi di indicatori e segnali precursori della minaccia di attacchi informatici alle infrastrutture critiche del sistema Paese;
- piani di formazione per operatori preposti alla protezione delle infrastrutture, per incrementarne le capacità analitiche.

Con riferimento alla sicurezza alimentare la strategia mira a rafforzare le conoscenze e competenze degli operatori in materia di contaminazione deliberata della catena di fornitura alimentare europea al fine di prevenire l'introduzione sul mercato di alimenti e prodotti contraffatti.

In materia di protezione di vittime e testimoni (NO4) allo stato non si ritiene di chiederne co-finanziamento a valere su ISF. Si fa riserva di riprogrammare eventuali interventi, in considerazione di sopraggiunte necessità.

<b>Obiettivo nazionale</b>	1 - R - prevenzione e lotta
----------------------------	-----------------------------

Si prevede l'implementazione delle attività incluse nel *Policy Cycle* 2014-2017 in riferimento all'identificazione dei rischi e alla gestione delle crisi anche mediante l'acquisizione di tecnologie, sistemi ed attrezzature IT, al fine di prevenire in maniera efficace ed efficiente eventuali situazioni di crisi.

In tale contesto, facendo ricorso alle risorse di ISF si intende acquisire mezzi tattici e/o procedere alla personalizzazione di veicoli commerciali, dotati delle più evolute attrezzature e tecnologie per il monitoraggio a distanza di obiettivi sensibili (tra cui le infrastrutture nazionali ed i soggetti potenzialmente a rischio) da utilizzarsi in diversi scenari operativi al fine di prevenire situazioni di crisi e reati gravi, transfrontalieri e di criminalità organizzata. A tal proposito, per delineare le caratteristiche di tali mezzi, si rende con il supporto del Fondo ISF si procederà a:

- elaborare un'analisi dello stato dell'arte in materia di sistemi di monitoraggio a distanza, anche con il coinvolgimento delle *Law Enforcement Agencies*, ed individuazione delle criticità dei sistemi esistenti;
- produrre studi e disegni di piattaforme comuni per la condivisione tra le *Law Enforcement Agencies* delle attività di monitoraggio a distanza.

Al fine di incrementare il livello di efficienza della prevenzione del rischio nazionale, si prevede la condivisione e lo scambio delle *best practice* registrate tra le autorità istituzionali competenti, con particolare riferimento alle tecniche di riconoscimento biometrico ed al confronto fisionomico nell'ambito dell'analisi dei segnali audio e video.

Si prevede inoltre l'implementazione di sistemi di controllo e protezione, anche mediante la tecnologia SCEPYLT, con lo scopo di identificare le attività illegali di movimentazione, stoccaggio e trasporto di materiali esplosivi, anche nell'ambito della prevenzione e lotta al terrorismo e radicalizzazione.

In tale ambito, i risultati auspicati dall'Italia sono:

- il **rafforzamento della cooperazione nel settore di law enforcement**, anche a livello transfrontaliero;
- il miglioramento delle **capacità di gestione delle situazioni di rischi e crisi**.

<b>Obiettivo nazionale</b>	2 - R - scambio di informazioni
----------------------------	---------------------------------

Al fine di garantire una gestione efficace di eventuali crisi ed emergenze sanitarie, anche legate ad attacchi CBRN-E sul territorio nazionale, mediante il supporto del Fondo ISF si prevede la realizzazione di una rete di collegamento tra una sala operativa/unità di crisi istituita a livello centrale e le sue articolazioni periferiche. Tale sistema, mediante acquisizione di attrezzature informatiche nonché mezzi di comunicazione multimediali, consentirà rapide e dirette comunicazioni di indirizzo e coordinamento.

Inoltre, sempre con il finanziamento di ISF si prevede l'implementazione di sistemi dedicati, anche mediante tecnologia EWS, per garantire rapide e dirette comunicazioni di indirizzo e coordinamento in caso di crisi e con riferimento al furto ed utilizzo di esplosivi, armi e materiali CBRN.

In tale ambito, i risultati auspicati dall'Italia sono:

- il **pieno utilizzo della tecnologia EWS** per lo scambio di informazioni connesse al furto, smarrimento, o cattivo uso di esplosivi, armi e materiali CBRN;
- lo **sviluppo ed il rafforzamento della capacità di contrastare gli incidenti CBRN**.

<b>Obiettivo nazionale</b>	3 - R - formazione
----------------------------	--------------------

In stretta correlazione con le attività da porre in essere per rendere più efficace lo scambio di informazioni tra gli operatori di sicurezza, mediante il supporto del Fondo ISF si prevedono attività di formazione specialistica per potenziare ed aggiornare le competenze degli operatori di polizia e di soccorso pubblico al fine di garantire la risposta rapida ad attacchi ed eventi chimici, biologici, radiologici, nucleari ed esplosivi (CBRN-E) sul territorio nazionale e la gestione di crisi ed emergenze sanitarie.

Inoltre, sempre mediante il Fondo ISF saranno realizzati corsi formativi ed attività seminariali su:

- scienze forensi per il miglioramento delle attività di ricerca e sviluppo, per il personale operante nei laboratori e sui mezzi tattici;
- tecniche di riconoscimento biometrico e confronto fisionomico nell'ambito dell'analisi dei segnali audio e video;
- rischi di contaminazione deliberata della catena di fornitura alimentare europea, ad esempio con riferimento ad etichette che richiamano in modo fraudolento al “*Made in Italy*”.

Nell’ambito della prevenzione dei rischi di radicalizzazione e terrorismo, sono anche previsti corsi di formazione (comprensivi della relativa attrezzatura tecnica necessaria) su strumenti e tecniche investigative e simulazioni di scenari operativi ad alto rischio, anche in presenza di ostaggi, per l’addestramento dei gruppi speciali.

Il risultato auspicato dall’Italia è la creazione di una cultura europea in materia di prevenzione e gestione delle situazioni di crisi da attuarsi mediante la diffusione omogenea di competenze specialistiche (in materia di CBRN-E, contaminazione alimentare, e lotta alla radicalizzazione e terrorismo) e tecnologiche (attrezzature IT d’avanguardia).

<b>Obiettivo nazionale</b>	4 - R - sostegno alle vittime
----------------------------	-------------------------------

L’attenzione delle Forze di Polizia italiane nell’approccio con le vittime dei reati è da sempre particolarmente approfondita ed efficace, essendo oggetto di specifica formazione per gli operatori di tutti i livelli.

Tale **formazione** si basa sulle buone prassi ricavate fin dal 2007 nell’ambito del Progetto Europeo DAPHNE II AVICRI (*Attention for victims of crimes*), avente come obiettivo specifico la creazione e l’elaborazione di pacchetti educativi, condivisibili con gli addetti ai lavori a livello europeo, volti alla Formazione di Funzionari ed Ufficiali delle Forze di Polizia addetti all’accoglienza delle vittime dei crimini. A tal scopo, è stato elaborato il manuale “*Costruzione della sicurezza tra incontro ed interazione – Forze di polizia e Vittime dei reati – approccio alla vittima: linee guida e buone prassi*”, distribuito in tutti gli Uffici operativi delle FFPP sull’intero territorio nazionale.

All’occorrenza viene fornita anche adeguata **assistenza sanitaria e psicologica**, soprattutto in presenza di vittime particolarmente vulnerabili (minori, donne, anziani, persone con disabilità), per i quali esistono presso gli uffici operativi delle FFPP italiane sezioni e personale specializzato.

Per quanto attiene alla **tutela dei testimoni dei reati**, è operativa in Italia una legislazione *ad hoc* (legge 13 febbraio 2001 n. 45 che ha modificato la precedente disciplina relativa ai collaboratori di giustizia di cui alla legge 15 marzo 1991 n. 82) con la quale vengono garantite particolari misure di protezione a quanto rendono dichiarazioni all’autorità giudiziaria su fatti criminali particolarmente gravi. I testimoni e i loro familiari godono di uno speciale

programma di protezione, un ‘pacchetto’ di misure di sicurezza, assistenza e recupero sociale, la cui ammissione viene decisa da una Commissione costituita presso il Ministero dell’interno. Le principali misure contenute nel programma sono:

- misure di tutela dell’incolumità;
- misure di assistenza;
- cambiamento delle generalità (una completa ricostruzione, a tutti i fini, dell’identità anagrafica del collaboratore, formalizzata da appositi decreti dei Ministeri dell’interno e della giustizia);
- misure di reinserimento sociale.

Naturalmente si tratta di Fondi di bilancio coperti da assoluta riservatezza e pertanto, allo stato, non si ritiene possibile richiederne alcuna compartecipazione al Fondo Sicurezza Interna ISF.

<b>Obiettivo nazionale</b>	5 - R - infrastrutture
----------------------------	------------------------

In linea con quanto previsto nella Obiettivo Nazionale “1. R - prevenzione e lotta” in merito all’acquisizione di attrezzature e tecnologie finalizzate alla protezione di infrastrutture critiche (fisse o mobili), al monitoraggio a distanza di obiettivi sensibili e alla protezione di spazi pubblici (*soft target*) in linea con quanto previsto dall’Agenda sulla Sicurezza COM(2015)185 *final*.

Nell’ambito della protezione delle infrastrutture critiche di rete, inoltre, si rende opportuno, sempre mediante le risorse di SIF, procedere con lo sviluppo di una piattaforma automatizzata di esplorazione, ricerca, estrazione ed analisi, sia in tempo reale che off-line, degli indicatori (*threat signature*) e dei segnali precursori, anche di natura comportamentale, per la rilevazione di potenziali attività *cyber* ostili a danno di reti informatiche sensibili, pubbliche e private.

In tale ambito, il risultato auspicato è garantire il **potenziamento delle infrastrutture nazionali** per la raccolta e l’analisi dei dati.

<b>Obiettivo nazionale</b>	6 - R - allarme rapido e crisi
----------------------------	--------------------------------

Per la gestione operativa delle situazioni di crisi in caso di allarme, si prevede di potenziare tramite il Fondo ISF le capacità di gestione degli incidenti CBRN-E attraverso l’acquisizione di mezzi di soccorso sanitario, forniti delle più avanzate attrezzature IT, e comprensivi di sale operative per i necessari collegamenti atti a gestire gli eventi di crisi sul territorio. Tali mezzi saranno dotati di particolari attrezzature per fronteggiare le delicate situazioni di operatività e soccorso tra cui, ad esempio, barelle a pressione negativa e positiva per il trasporto di pazienti bio-contaminati ad alto rischio di contagio ed irradiati con lesioni gravi, vittime di attacchi aggressivi CBRN-E.

Per la prevenzione delle medesime situazioni di crisi, e nell’ottica di ridurre i tempi di reazione agli allarmi, si prevede di ricorrere al finanziamento di ISF per:

- la realizzazione di un sistema IT che, utilizzando sofisticati modelli matematici per la predizione di scenari di fenomeni criminali complessi, crei una simulazione di scenari futuri di fenomeni terroristici e di criminalità organizzata attraverso sistemi di analisi integrata di dati storici di carattere investigativo;

- l'adeguamento tecnologico delle sale operative ed aggiornamento di n. 1300 stazioni preposte alla rilevazione della radioattività attraverso la modifica parziale di HW e SW delle stazioni e l'integrazione delle stesse con dispositivi aggiuntivi in grado di monitorare altre sostanze pericolose (in particolare chimiche).
- interventi per la **gestione e il contenimento dell'emergenza epidemiologica da COVID 19**, volti al contrasto della crisi e al rafforzamento della capacità operativa, in condizioni di sicurezza, delle forze di polizia e dei vigili del fuoco, impegnati in prima linea su questa emergenza.

In tale ambito, i risultati attesi dall'Italia sono:

- il rafforzamento delle **capacità di *targeting*, individuazione, identificazione e intervento** in caso di attacco CBRN-E;
- il potenziamento delle capacità di far fronte a situazione di crisi mediante lo **sviluppo di soluzioni IT altamente performanti**.

<b>Obiettivo nazionale</b>	7 - R - valutazione dei rischi e delle minacce
----------------------------	--

Mediante le risorse del Fondo ISF si intende:

- rendere maggiormente efficienti il sistema di indagine per il contrasto della criminalità informatica attraverso la realizzazione di una piattaforma integrata per l'analisi ed il "*reverse engineering*" dei *malware* integrata con un modulo per la correlazione di dati di log provenienti da dispositivi di sicurezza delle reti informatiche;
- realizzare un sistema di prevenzione dei rischi di contaminazione deliberata della catena di fornitura alimentare europea, nonché predisporre contromisure rapide ed efficaci per proteggere la filiera degli alimenti da possibili attacchi e contaminazioni intenzionali.

I risultati attesi dall'Italia in tale ambito sono:

- l'**incremento della capacità di valutazione dei rischi** nell'ambito della criminalità informatica
- il **miglioramento delle capacità di rilevazione e contenimento delle minacce** la sicurezza nazionale ed UE, in ambiti quali ad esempio la catena alimentare.

## CALENDARIO INDICATIVO

Obiettivo specifico	ON/AS	Azione principale	Nome dell'azione	Inizio della fase di pianificazione	Inizio della fase di attuazione	Inizio della fase di chiusura
OS1 - Sostegno per una politica comune in materia di visti	ON1 - Capacità nazionale	1	Adeguamento infrastruttura IT e rafforzamento rete di scambio dei Server delle Sedi consolari	2015	2017	2020
OS1 - Sostegno per una politica comune in materia di visti	ON1 - Capacità nazionale	2	Potenziamento connettività Sedi Consolari per ottimizzare i tempi di processing emissione dei visti	2015	2017	2020
OS1 - Sostegno per una politica comune in materia di visti	ON1 - Capacità nazionale	3	Aggiornamento IT Sistemi I-VIS - Centrale e livello periferico	2015	2016	2020
OS1 - Sostegno per una politica comune in materia di visti	ON2 - Acquis dell'Unione	1	Formazione per operatori delle Sedi Consolari	2015	2019	2020
OS2 - Frontiere	ON1 - EUROSUR	1	Acquisizione HW e SW per potenziamento operativo dei sistemi di NCC e nodo EUROSUR	2015	2019	2020
OS2 - Frontiere	ON1 - EUROSUR	2	Potenziamento dispositivi di sorveglianza marittima per il controllo delle frontiere	2015	2018	2020
OS2 - Frontiere	ON1 - EUROSUR	3	Tecnologie per scoperta/tracciamento assetti aeronavali per classificazione/identificazione	2015	2018	2020
OS2 - Frontiere	ON2 - Scambio di informazioni	1	Evoluzione apparecchiature di NCC e sistemi informativi per scambio informazioni real time	2015	2019	2020
OS2 - Frontiere	ON2 - Scambio di informazioni	2	Consolidamento e securizzazione dei sistemi a bordo delle UU.NN. e dei connessi sistemi terrestri	2015	2019	2020
OS2 - Frontiere	ON2 - Scambio di informazioni	3	Adeguamento della componente TDL per UU.NN. impiegate per il controllo flussi migratori e S.A.R.	2015	2019	2020
OS2 - Frontiere	ON3 - Norme comuni dell'Unione	1	Potenziamento ed estensione dei sistemi ABC	2015	2019	2020
OS2 - Frontiere	ON4 - Acquis dell'Unione	1	Formazione specialistica del personale impiegato negli uffici di frontiera	2015	2018	2020
OS2 - Frontiere	ON4 - Acquis dell'Unione	2	Recurrent Training personale impiegato nel controllo delle frontiere aeree, terrestri e marittime	2015	2018	2020
OS2 - Frontiere	ON4 - Acquis dell'Unione	3	Formazione specialistica ICT e linguistica del personale impiegato negli uffici di frontiera	2015	2016	2020
OS2 - Frontiere	ON5 - Sfide future	1	Sviluppo di nuovi e innovativi strumenti e sistemi per la gestione e controllo frontiere	2018	2019	2020
OS2 - Frontiere	ON6 - Capacità nazionale	1	Acquisto mezzi aerei marittimi e terrestri per individuare persone in mare e pattugliare frontiere	2015	2015	2021
OS2 - Frontiere	ON6 - Capacità nazionale	2	Adeguamento sistemi a bordo delle UU.NN. ed estensione della capacità su ulteriori UU.NN.	2015	2016	2020
OS2 - Frontiere	ON6 - Capacità nazionale	3	Acquisto di Uffici mobili e apparati per le verifiche biometriche e documentali e foto-segnalamento	2015	2016	2020
OS2 - Frontiere	AS2 - Strumenti FRONTEX	1	Acquisto mezzi aerei	2015	2017	2020
OS2 - Frontiere	AS2 - Strumenti FRONTEX	2	Acquisto mezzi marittimi	2015	2017	2021
OS3 - Sostegno operativo	ON1 - Sostegno operativo per i visti	1	Manutenzione SW applicazione visti ed introduzione nuove funzionalità	2015	2017	2020
OS3 - Sostegno operativo	ON1 - Sostegno operativo per i visti	2	Manutenzione piattaforma integrata test e validazione	2015	2019	2020
OS3 - Sostegno operativo	ON2 - Sostegno operativo alle frontiere	1	Manutenzione di infrastrutture ICT utilizzate per la gestione integrata delle frontiere	2015	2016	2020
OS3 - Sostegno operativo	ON2 - Sostegno operativo alle frontiere	2	Ristrutturazione delle principali scuole di formazione e del NCC	2015	2019	2020
OS3 - Sostegno operativo	ON2 - Sostegno operativo alle frontiere	3	Manutenzione e supporto logistico integrato di mezzi	2015	2018	2020
OS5 - Prevenzione e	ON1 - C -	1	Predisposizione sistemi elettronici per la	2015	2018	2020

Obiettivo specifico	ON/AS	Azione principale	Nome dell'azione	Inizio della fase di pianificazione	Inizio della fase di attuazione	Inizio della fase di chiusura
lotta alla criminalità	prevenzione e lotta		rilevazione di utenze mobili (GSM/UMTS/LTE)			
OS5 - Prevenzione e lotta alla criminalità	ON1 - C - prevenzione e lotta	2	Potenziamento delle capacità di disinnesco di ordigni	2015	2017	2020
OS5 - Prevenzione e lotta alla criminalità	ON1 - C - prevenzione e lotta	3	Laboratori forensi dotati di tecnologie evolute per le analisi chimiche	2015	2017	2020
OS5 - Prevenzione e lotta alla criminalità	ON2 - C - scambio di informazioni	1	Potenziamento dei sistemi AFIS eAPIS	2015	2018	2020
OS5 - Prevenzione e lotta alla criminalità	ON2 - C - scambio di informazioni	2	Network integrato in campo balistico e miglioramento degli attuali sistemi 3D	2015	2018	2020
OS5 - Prevenzione e lotta alla criminalità	ON2 - C - scambio di informazioni	3	Progetto sviluppo PNR	2017	2018	2020
OS5 - Prevenzione e lotta alla criminalità	ON3 - C - formazione	1	Formazione sul rafforzamento della protezione interna ed esterna delle reti informatiche	2015	2019	2020
OS5 - Prevenzione e lotta alla criminalità	ON3 - C - formazione	2	Formazione su indagini finanziarie, traffico droga, corruzione, patrimoni illeciti	2015	2018	2020
OS5 - Prevenzione e lotta alla criminalità	ON3 - C - formazione	3	Formazione in materia giudiziaria e polizia (ETS)	2015	2019	2020
OS5 - Prevenzione e lotta alla criminalità	ON4 - C - sostegno alle vittime	1	Infrastrutture per il sostegno alle categorie vulnerabili	2018	2019	2020
OS6 - Rischi e crisi	ON1 - R - prevenzione e lotta	1	Mezzi tattici per monitoraggio a distanza di obiettivi sensibili	2015	2019	2020
OS6 - Rischi e crisi	ON2 - R - scambio di informazioni	1	Reti di collegamento tra sala operativa e articolazioni periferiche sanitarie	2015	2019	2020
OS6 - Rischi e crisi	ON3 - R - formazione	1	Formazione specialistica in materia di attacchi CBRN	2015	2019	2020
OS6 - Rischi e crisi	ON3 - R - formazione	2	Formazione specialistica nell'ambito delle Scienze forensi	2015	2019	2020
OS6 - Rischi e crisi	ON3 - R - formazione	3	Tecniche investigative ed operazioni antiterrorismo ad alto rischio	2015	2019	2020
OS6 - Rischi e crisi	ON5 - R - infrastrutture	1	Sviluppo piattaforma automatizzata per rilevare potenziali attività cyber ostili	2015	2018	2020
OS6 - Rischi e crisi	ON5 - R - infrastrutture	2	Sviluppo soluzioni tecnologiche innovative per la protezione di infrastrutture critiche	2015	2018	2020
OS6 - Rischi e crisi	ON6 - R - allarme rapido e crisi	1	Potenziamento del sistema di rilevamento della radioattività	2015	2019	2020
OS6 - Rischi e crisi	ON6 - R - allarme rapido e crisi	2	Mezzi sanitari con attrezzature per fronteggiare emergenze nel settore CBRN	2015	2016	2020
OS6 - Rischi e crisi	ON6 - R - allarme rapido e crisi	3	Sistemi informatici di simulazione di scenari futuri di fenomeni terroristici	2015	2016	2020
OS6 - Rischi e crisi	ON7 - R - valutazione dei rischi e delle minacce	1	Realizzazione piattaforma integrata con moduli per la correlazione di dati di log	2015	2019	2020
OS6 - Rischi e crisi	ON7 - R - valutazione dei rischi e delle minacce	2	Sistema di prevenzione dei rischi di contaminazione della catena di fornitura alimentare	2015	2019	2020



## 5. INDICATORI COMUNI E INDICATORI SPECIFICI PER PROGRAMMA:

<b>Obiettivo specifico</b>	<b>1 - Sostegno per una politica comune in materia di visti</b>			
<b>Indicator</b>	<b>Unità di misura</b>	<b>Valore di riferimento</b>	<b>Valore obiettivo</b>	<b>Fonte di dati</b>
C1 - Numero di attività di cooperazione consolare sviluppate con l'aiuto del Fondo	Numero	0,00	0,00	Projects
C2.1 - Numero di unità del personale formato in aspetti legati alla politica comune dei visti con l'aiuto del Fondo	Numero	0,00	400,00	Projects
C2.2 - Numero di corsi di formazione (ore effettuate)	Numero	0,00	3.000,00	Projects
C3 - Numero di posti specializzati in paesi terzi sostenuti dal Fondo	Numero	0,00	40,00	Projects
C4.1 - Numero di consolati sviluppati o aggiornati con l'aiuto del Fondo rispetto al numero totale dei consolati	Numero	0,00	172,00	Projects
C4.2 - Percentuale di consolati sviluppati o potenziati con l'aiuto del Fondo rispetto al numero totale dei consolati	%	0,00	97,60	Projects

<b>Obiettivo specifico</b>	<b>2 - Frontiere</b>			
<b>Indicator</b>	<b>Unità di misura</b>	<b>Valore di riferimento</b>	<b>Valore obiettivo</b>	<b>Fonte di dati</b>
C1.1 - Numero di unità del personale formato in aspetti legati alla gestione delle frontiere con l'aiuto del Fondo	Numero	0,00	3.275,00	Projects
C1.2 - Numero di corsi di formazione in aspetti legati alla gestione delle frontiere con l'aiuto del Fondo	Numero	0,00	185,00	Projects
C2 - Numero di controlli di frontiera (controlli e sorveglianza), infrastrutture e mezzi sviluppati o aggiornati con l'aiuto del Fondo	Numero	0,00	840,00	Projects
C3.1 - Numero di valichi di frontiera lungo le frontiere esterne attraverso porte di controllo automatizzato con il sostegno del Fondo	Numero	0,00	151.200.000,00	Projects
C3.2 - Numero totale di valichi di frontiera	Numero	0,00	315.950.000,00	Projects
C4 - Numero di infrastrutture nazionali di sorveglianza delle frontiere istituite/perfezionate nel quadro di EUROSUR	Numero	0,00	10,00	Projects
C5 - Numero di incidenti segnalati dallo Stato membro al quadro situazionale europeo	Numero	0,00	5.813,00	Projects
C6 - Ore erogate per il servizio di mediazione/interpretariato permanente e/o a chiamata	Ore	0,00	446.000,00	Projects
C7 - Numero di sistemi aerei a pilotaggio remoto finanziati con l'aiuto del Fondo	Numero	0,00	7,00	Projects
C8 - Numero di progetti per la costituzione della National Uniform Interface (NUI) nel quadro dell'Entry Exit System	numero	0,00	1,00	Projects

<b>Obiettivo specifico</b>	<b>5 - Prevenzione e lotta alla criminalità</b>			
<b>Indicator</b>	<b>Unità di misura</b>	<b>Valore di riferimento</b>	<b>Valore obiettivo</b>	<b>Fonte di dati</b>
C1 - Numero di squadre investigative comuni e di progetti operativi di EMPACT finanziati dal Fondo, compresa la partecipazione di Stati membri e autorità	Numero	0,00	3,00	Projects
C2.1 - Numero di funzionari delle autorità di contrasto formati su tematiche inerenti alla dimensione transfrontaliera con l'aiuto del Fondo	Numero	0,00	8.000,00	Projects
C2.2 - Durata della formazione (realizzata) su tematiche inerenti alla dimensione transfrontaliera con l'aiuto del Fondo	Giorni/persona	0,00	350,00	Projects
C3.1 - Numero di progetti nel campo della prevenzione dei reati	Numero	0,00	31,00	Projects
C3.2 - Valore finanziario dei progetti nel campo della prevenzione dei reati	EUR	0,00	50.370.447,95	Projects
C4 - Numero di progetti finanziati dal Fondo e finalizzati a migliorare gli scambi d'informazioni tra autorità di polizia concernenti i sistemi di dati, archivi o strumenti di comunicazione di Europol (ad es. caricatori di dati, estensione dell'accesso a SIENA, progetti finalizzati a migliorare i contributi agli archivi di lavoro a fini di analisi ecc.)	Numero	0,00	8,00	Projects
C5 - Numero di sale d'ascolto finanziate dal Fondo a sostegno delle categorie più deboli vittime di reati	Numero	0,00	30,00	Projects

<b>Obiettivo specifico</b>	<b>6 - Rischi e crisi</b>			
<b>Indicator</b>	<b>Unità di misura</b>	<b>Valore di riferimento</b>	<b>Valore obiettivo</b>	<b>Fonte di dati</b>
C1 - Numero di strumenti messi a punto o potenziati con l'aiuto del Fondo per agevolare la protezione di infrastrutture critiche da parte degli Stati membri in tutti i settori dell'economia	Numero	0,00	3,00	Projects
C2 - Numero di progetti relativi alla valutazione e alla gestione dei rischi nel settore della sicurezza interna finanziati dal Fondo	Numero	0,00	5,00	Projects
C3 - Numero di riunioni di esperti, di workshop, seminari, conferenze, pubblicazioni, siti web e consultazioni (online) organizzati con l'aiuto del Fondo	Numero	0,00	25,00	Projects

## 6. QUADRO PER LA PREPARAZIONE E L'ATTUAZIONE DEL PROGRAMMA DA PARTE DELLO STATO MEMBRO

### 6.1 Coinvolgimento dei partner alla preparazione del programma

Il processo di programmazione 2014-2020 è stato avviato in data 18.10.2013 con il c.d. Dialogo Politico tra i rappresentanti della CE e dello SM.

In data 17.01.2014 il Capo della Polizia - Direttore Generale della Pubblica Sicurezza ha istituito il Tavolo Tecnico di Programmazione Congiunta allo scopo di consultare i potenziali beneficiari del Fondo ed avviare la concertazione volta alla definizione della strategia nazionale in materia di controllo delle frontiere, gestione dei visti e contrasto al crimine per il periodo 2014-2020. Alla prima riunione del Tavolo, che si è tenuta in data 30.01.2014, hanno partecipato le Amministrazioni istituzionalmente competenti, ovvero:

- MI: DDCC del DPS e DLCI
- MI: VVF
- MD: CGAC e MM
- MEF: GdF
- MG: PP
- MIPAAF: CFS
- PCM: DIS
- MAECI
- MIT: CdP-GC

Durante la riunione sono stati illustrati obiettivi, finalità e linee di finanziamento e è stato presentato lo Strumento Operativo di Programmazione, elaborato dalla STA sotto forma di scheda di rilevazione, con lo scopo di agevolare le Amministrazioni nella presentazione dei contributi e raccogliere in maniera uniforme. Ciò ha consentito di trasmettere il PN via SFC in data 2.12.2014.

A seguito delle osservazioni della CE del 6.02.2015 e del 16.03.2015 ed in considerazione dei contingenti fatti di cronaca in materia di emergenza frontiere, *smuggling*, *foreign fighters* e anti-terrorismo, l'AR ha convocato ulteriori riunioni volte a condividere con le Amministrazioni le misure da intraprendere. In particolare, tali incontri sono valsi ad approfondire e focalizzare le linee di intervento strategiche su cui l'Italia intende focalizzarsi nei prossimi anni. Gli incontri inoltre hanno permesso di implementare e dettagliare alcune sezioni del Programma.

### 6.2 Comitato di sorveglianza

Il CdS è presieduto dall'AR o in caso di assenza/impedimenti, dal Direttore della STA.

A seguito dell'approvazione del PN verrà formalizzato un regolamento interno che definisce: composizione, ruoli e modalità di funzionamento del CdS.

Il CdS ha il compito precipuo di accertare la verifica dell'efficacia e della qualità dell'attuazione del PN attraverso:

- il monitoraggio e la valutazione periodica dei progressi compiuti nel conseguimento degli obiettivi specifici, fissati per Priorità nazionale
- la condivisione del *reporting* annuale da inviare alla CE
- il monitoraggio delle iniziative di informazione, comunicazione e pubblicità
- la concertazione nella fase di revisione del PN, al fine di conseguire gli obiettivi del Fondo.

Il CdS è informato in merito ad eventuali *audit* di organismi nazionali e comunitari.

Indicativamente fanno parte del CdS:

- i partner coinvolti durante la programmazione e l'attuazione del PN
- i rappresentanti della CE – DG HOME
- il Direttore della STA e i funzionari responsabili degli uffici
- l'Autorità di Audit
- valutatore esterno (non appena individuato)

Possono altresì partecipare su esplicito invito: esponenti nazionali, regionali e locali del settore pubblico e privato, nonché rappresentanti del partenariato economico e sociale e del terzo settore.

### 6.3 Quadro comune di monitoraggio e valutazione

L'attività di monitoraggio e valutazione, che assicura la corretta attuazione e gestione del Programma, viene effettuata tramite l'utilizzo di un sistema informativo gestionale in grado di raccogliere dati e documenti, verificarne l'affidabilità e l'omogeneità, elaborare report di sintesi sullo stato di attuazione e dialogare con SFC 2014.

In particolare il sistema, le cui specifiche tecniche sono disegnate sulla base delle procedure del SiGeCo, prevede le seguenti funzionalità:

- trasmissione *application form* dei progetti;
- istruttoria per ammissione a finanziamento;
- monitoraggio delle attività di *procurement*;
- verifica avanzamento fisico e finanziario;
- controlli di I livello;
- monitoraggio degli indicatori di programma e di progetto;
- accesso protetto di utenti profilati;
- protocollo di colloquio con SFC 2014.

Il sistema prevede meccanismi di controllo multilivello per rilevare anomalie e generare alert agli utenti interessati.

Per le attività di valutazione, che potrebbero essere affidate a valutatori esterni, il sistema informativo costituisce la base dati su cui effettuare elaborazioni ed aggregazioni che consentono di implementare report

sulla qualità dei progetti, i risultati raggiunti e le migliori pratiche sviluppate.

#### **6.4 Coinvolgimento del partenariato nell'esecuzione, nel monitoraggio e nella valutazione del programma nazionale**

I Partner titolari di progetti per l'attuazione del PN sono le Amministrazioni pubbliche centrali responsabili dell'implementazione delle politiche per la gestione delle frontiere e visti, la prevenzione e il contrasto della criminalità e la gestione delle situazioni di rischio e crisi.

Tali Beneficiari supportano costantemente l'AR nel perseguire l'efficacia e l'efficienza nell'attuazione del PN, in termini sia di corretto avanzamento finanziario, procedurale e fisico che di raggiungimento degli obiettivi specifici.

Ciascuna Amministrazione Beneficiaria Partner dovrà dotarsi di un'adeguata struttura di *governance* in modo da garantire l'implementazione dei progetti in linea con la pianificazione e il raggiungimento degli indicatori. A tale riguardo, ogni Beneficiario dovrà identificare un Referente, membro ordinario del CdS, con il ruolo di:

- trasmettere le *application form*;
- sottoscrivere le Convenzioni di Sovvenzione con l'AR;
- assicurare la sana gestione finanziaria dei progetti;
- fornire i dati di monitoraggio all'AR;
- istituire un sistema di contabilità separata per consentire la tracciabilità dei flussi finanziari;
- attivare iniziative per la disseminazione dei risultati;
- conservare e rendere disponibile la documentazione di progetto per controlli futuri di organismi nazionali e comunitari.

La struttura del Beneficiario sarà accompagnata dalla STA nel corso di tutta la programmazione mediante la diffusione di procedure e strumenti operativi omogenei per la gestione e il controllo dei progetti. A tal fine, saranno convocati tavoli tecnici bilaterali, implementati *focus group* tematici (per le diverse componenti di ISF1 e ISF2), e organizzati seminari informativi rivolti a tutti i soggetti coinvolti nella gestione e controllo dei progetti, volti ad armonizzare procedure e modalità operative definite per il Fondo.

#### **6.5 Informazione e pubblicità**

Il Sistema Informativo di Monitoraggio e Valutazione prevede, oltre ad una profilatura protetta per i soli utenti registrati, un'interfaccia *open data* (portale web) che rappresenta il principale canale d'informazione per le diverse categorie di utenti.

Il portale web conterrà i principali dati relativi al Fondo:

- base legale (Regolamenti UE, rapporti Frontex, normativa nazionale, comunicazioni *AMIF-ISF Committee*,...);
- informazioni generali (PN e eventuali revisione);
- pubblicazione *call for proposal* del PN;
- informativa sulle *call for proposal* dell'UE (*Union Actions*);

- descrizione del modello organizzativo e di gestione del Fondo;
- news ed eventi pubblicati costantemente e in tempo reale;
- rassegna stampa;
- *open data* con report periodici di avanzamento della spesa;
- sezione multimediale con gallerie audiovisive e album fotografici.

Il portale conterrà inoltre un forum aperto di discussione, un servizio dedicato alle FAQ, una casella di posta elettronica a cui rivolgersi per l'invio di informazioni e una pagina con *link* a siti web di interesse tematico.

La trasparenza delle informazioni sarà garantita dalla pubblicazione dell'elenco dei beneficiari e della lista dei progetti ammessi al finanziamento per ISF1 e ISF2.

Il sito verrà inoltre costantemente monitorato relativamente ai dati di accesso e gradimento.

Ulteriori azioni di informazione, pubblicità e eventi di disseminazione dei risultati e *best practices* saranno poste in essere in corso di attuazione del programma.

## 6.6. Coordinamento e complementarità con altri strumenti

Il MI, per la programmazione 2014-2020, è titolare di Programmi e progetti cofinanziati da fondi europei, la cui gestione è demandata ai Dipartimenti competenti per materia; il **DPS** in linea di continuità con EBF e PON Sicurezza 2007-2013, è responsabile dell'attuazione di ISF e del PON Legalità 2014-2020.

Per garantire un'efficace implementazione di ciascuno strumento finanziario il DPS si è dotato di una struttura operativa: la *Segreteria Tecnica-Amministrativa dei Fondi Europei e Programmi Operativi Nazionali*. La STA opera sotto il coordinamento dell'AR, che riveste altresì il ruolo di AdG del PON Sicurezza 2007-2013 e del PON Legalità 2014-2020. La STA ha implementato procedure volte ad assicurare la complementarità delle strategie ricadenti nella gestione concorrente con quelle gestite direttamente dalla CE ed attuate dallo SM (Azioni dell'Unione e Azioni Specifiche).

In fase di programmazione, si sono tenuti incontri con i Partner per condividere la strategia generale del 2014-2020 ed indirizzarli verso lo strumento finanziario più coerente con i loro fabbisogni. In particolare, in data 9.06.2014 si è tenuto un incontro, presieduto dall'AR/AdG, nell'ambito del quale le DDCC del DPS si sono confrontate con la STA per procedere congiuntamente alla definizione degli interventi da attuarsi rispettivamente con ISF e PON Legalità in un'ottica integrata ed efficiente. Date le strategie e i rispettivi obiettivi dei due Fondi, l'AR definirà dei criteri *ad hoc* per valutare, in alcuni casi limitati, l'ammissibilità dei progetti a valere su ISF e PON Legalità per assicurare il corretto utilizzo dei fondi UE.

Tali momenti di condivisione hanno consentito alla STA di arginare il rischio di incorrere in duplicazioni di interventi analoghi.

Durante la fase di attuazione, inoltre, grazie al Sistema Informativo di Monitoraggio e Valutazione (contenente i dati sia di ISF sia di PON) sarà possibile rilevare duplicazioni di progetti a valere sugli strumenti finanziari mediante la generazione automatica di *alert* di sistema che prevengano il rischio di doppio finanziamento.

Presso il **DLCI** è incardinata l'AR di AMIF 2014-2020. La STA, anche in questo caso, ha instaurato una proficua collaborazione con i referenti di AMIF, al fine di attuare progettualità integrate sul tema dell'immigrazione e della sicurezza interna, per l'individuazione delle appropriate fonti di finanziamento.

Infine, con riguardo alla complementarità con strumenti finanziari diversi da quelli citati (es. FSE in riferimento ad attività in materia di rafforzamento della capacità istituzionale, EuropeAid, IPA, Horizon 2020) la STA assicurerà un costante scambio di informazioni con i referenti ed i rappresentanti (capi di gabinetto, unità di coordinamento, ecc.) per garantire coerenza e complementarità degli interventi proposti, nonché assenza di duplicazioni.

La STA inoltre garantirà un periodico flusso informativo con le agenzie europee interessate: FRONTEX, eu-LISA, EASO, EMCDDA, CEPOL, EUROPOL.

## 6.7 Beneficiari

### 6.7.1. Elenco dei principali tipi di beneficiari del programma

I Beneficiari del Fondo sono le Amministrazioni pubbliche centrali responsabili dell'implementazione delle politiche per la gestione delle frontiere e visti, la prevenzione e il contrasto della criminalità e la gestione delle situazioni di rischio e crisi.

### 6.7.2 Aggiudicazione diretta (se del caso)

L'AR ha individuato specifiche procedure per la selezione dei progetti che saranno attuate in modalità *awarding body* e *executing body*.

Per quanto riguarda la modalità ***awarding body*** verranno attivate:

- *call for proposal ristrette*, tramite inviti ristretti a presentare proposte destinati a tutti i Beneficiari del Fondo o solo ad alcuni di essi;
- *assegnazioni dirette*, in casi debitamente giustificati, ad es.: prosecuzione di progetti pluriennali, situazioni di emergenza o se la natura specifica del progetto o la competenza tecnica degli organismi competenti non permetta alternative (situazioni di monopolio legale o di fatto).

Per quanto riguarda la modalità ***executing body***, l'AR, nell'esercizio delle sue funzioni, individua le tipologie di servizi, lavori e forniture da acquisire all'interno della linea di finanziamento "Assistenza Tecnica" e incarica la STA all'espletamento delle procedure ad evidenza pubblica da attuarsi conformemente alla normativa nazionale e comunitaria vigente.

## 7. PIANO DI FINANZIAMENTO DEL PROGRAMMA

**Tabella 1: Piano di finanziamento ISF-Frontiere**

<b>Obiettivo specifico/obiettivo nazionale</b>	<b>Totale</b>
OS1.ON1 Capacità nazionale	8.917.835,32
OS1.ON2 Acquis dell'Unione	523.000,00
OS1.ON3 Cooperazione consolare	0,00
<b>TOTALE ON OS1 Sostegno per una politica comune in materia di visti</b>	<b>9.440.835,32</b>
OS1.AS1 Cooperazione consolare	
<b>TOTALE OS1 Sostegno per una politica comune in materia di visti</b>	<b>9.440.835,32</b>
OS2.ON1 EUROSUR	23.052.171,00
OS2.ON2 Scambio di informazioni	6.551.860,70
OS2.ON3 Norme comuni dell'Unione	7.726.281,44
OS2.ON4 Acquis dell'Unione	6.637.844,62
OS2.ON5 Sfide future	10.556.994,50
OS2.ON6 Capacità nazionale	96.908.662,62
<b>TOTALE ON OS2 Frontiere</b>	<b>151.433.814,88</b>
OS2.AS2 Strumenti FRONTEX	74.565.000,00
<b>TOTALE OS2 Frontiere</b>	<b>225.998.814,88</b>
OS3.ON1 Sostegno operativo per i visti	105.684,10
OS3.ON2 Sostegno operativo alle frontiere	41.197.554,01
<b>TOTALE OS3 Sostegno operativo</b>	<b>41.303.238,11</b>
Assistenza tecnica alle frontiere	8.315.344,00
<b>TOTALE</b>	<b>285.058.232,31</b>

(1) L'importo riferito agli obiettivi OS2 / ON6 comprende una dotazione di 6 412 600 EUR da impiegare ai sensi dell'articolo 64, paragrafi 1 e 2, del regolamento (UE) 2017/2226. Questa specifica dotazione può sostenere il 100% di tali spese (comprese le spese per la gestione operativa del sistema) ed è prevista esclusivamente a tale scopo. Non può essere utilizzata per coprire altre esigenze o altre spese, ivi comprese le spese di cui all'articolo 64, paragrafo 2, dalla lettera a) alla lettera g), e articolo 64, paragrafo 3. Di tale dotazione specifica non occorre tener conto nel calcolo che determina la percentuale di finanziamento che può essere impiegata per finanziare il sostegno operativo, in conformità dell'articolo 10, paragrafo 1 del regolamento (UE) n. 515/2014.

(2) The amount under SO2 / NO6 includes an envelope of EUR 3 216 666,66 that shall be used to support exclusively the costs incurred by Member States in accordance with Article 85(1) of Regulation (EU) 2018/1240. Such costs can be fully supported (up to 100%) by this extra allocation. This extra allocation cannot be used to cover other costs, including those referred to in Article 85(2) points a) to d) of Regulation (EU) 2018/1240, as well as ETIAS' operating costs.

(3) The amount under SO2 / NO6 includes an envelope of EUR 1 227 000 that shall be used to support the costs incurred by Member States for the quick and effective upgrading of the national components of the SIS, in line with the requirements of Regulation (EU) 2018/1861. Such costs can be fully supported (up to 100%) by this extra allocation.

(4) The amount under SO2 / NO6 includes the amount awarded for the new Specific Action(s) added to Annex II to Regulation (EU) No. 515/2014, as set out in Commission Delegated Regulation (EU) 2020/446.



**Tabella 2: Piano di finanziamento ISF-Polizia**

<b>Obiettivo specifico/obiettivo nazionale</b>	<b>Totale</b>
OS5.ON1 C - prevenzione e lotta	24.321.117,09
OS5.ON2 C - scambio di informazioni	21.932.643,25
OS5.ON3 C - formazione	3.654.084,53
OS5.ON4 C - sostegno alle vittime	462.603,08
OS5.ON5 C - valutazione dei rischi e delle minacce	0,00
<b>TOTALE OS5 Prevenzione e lotta alla criminalità</b>	<b>50.370.447,95</b>
OS6.ON1 R - prevenzione e lotta	500.000,00
OS6.ON2 R - scambio di informazioni	100.000,00
OS6.ON3 R - formazione	500.000,00
OS6.ON4 R - sostegno alle vittime	0,00
OS6.ON5 R - infrastrutture	2.553.000,00
OS6.ON6 R - allarme rapido e crisi	5.997.000,00
OS6.ON7 R - valutazione dei rischi e delle minacce	1.450.000,00
<b>TOTALE OS6 Rischi e crisi</b>	<b>11.100.000,00</b>
Assistenza tecnica - polizia	3.031.587,05
<b>TOTALE</b>	<b>64.502.035,00</b>

**Tabella 3: Impegni annuali complessivi dell'UE (in EUR)**

	<b>2014</b>	<b>2015</b>	<b>2016</b>	<b>2017</b>	<b>2018</b>	<b>2019</b>	<b>2020</b>	<b>TOTALE</b>
ISF-Frontiere	0,00	43.957.988,00	41.105.893,00	43.716.553,00	73.799.162,99	42.617.345,42	39.861.289,90	285.058.232,31
ISF-Polizia	0,00	12.770.465,00	10.878.961,00	17.067.271,00	7.928.446,00	7.928.446,00	7.928.446,00	64.502.035,00

**Motivazione di eventuali scostamenti dalle quote minime fissate nei regolamenti specifici**

--

## DOCUMENTI

Titolo del documento	Tipo di documento	Data documento	Riferimento locale	Riferimento della Commissione	File	Data di invio	Inviato da
----------------------	-------------------	----------------	--------------------	-------------------------------	------	---------------	------------

## RISULTATI DI CONVALIDA PIÙ RECENTI

Gravità	Codice	Messaggio
Info		La versione del programma è stata convalidata.
Attenzione	2.15	È necessaria una nuova decisione della CE per le versioni > 1. È necessaria una nuova decisione della CE quando vengono modificati/aggiunti/eliminati campi appartenenti alla decisione della CE. Questi campi sono tutti i campi, ad eccezione di quelli utilizzati nella sezione Autorità e del campo Sistema di gestione e di controllo. Per il piano finanziario, gli importi nell'ambito di un obiettivo specifico possono essere modificati senza che sia necessaria una nuova decisione della CE, purché il totale per obiettivo specifico rimanga invariato.