# Internal Security Fund

# National Programme 2021-2027

## Call for Proposals 2026

## Information and Guidance for Applicants

---

**Issued by the Finance Directorate, An Garda Síochána**

# Table of Contents

Contents

## 1. Overview of Call for Proposals

### *1.1 Introduction*

The Finance Directorate, An Garda Síochána is the Managing Authority of the Internal Security Fund ("ISF") for the 2021-2027 programming period and is issuing a Call for Proposals for projects suitable for funding.

Funding is available for actions that address one or more of the Specific Objectives set out in Article 3 of the ISF Regulation[1]. The three Specific Objectives of the ISF are detailed below:

**Specific Objective 1 (SO1)**
*'Improving and facilitating the **exchange of information** between and within competent authorities and relevant Union bodies, offices and agencies and, where relevant, with third countries and international organisations.'*

**Specific Objective 2 (SO2)**
*'Improving and intensifying **cross-border cooperation**, including joint operations, between competent authorities in relation to **terrorism and serious and organised crime** with a cross-border dimension.'*

**Specific Objective 3 (SO3)**
*'Supporting the strengthening of Member States' capabilities in relation to **preventing and combating crime**, terrorism and radicalisation, as well as managing security-related incidents, risks and crises, including through increased cooperation between public authorities, relevant Union bodies, offices or agencies, civil society and private partners in different Member States.'*

Applicants will be required to indicate on their applications the specific objective(s) addressed by the proposal for which they are applying for funds.

This information and guidance document is comprised of five sections:

**Section 1** – General information on call for proposal
**Section 2** – Detailed guidance on how to apply for funding
**Section 3** – Eligibility of expenditure
**Section 4** – Systems and records that must be in place and maintained
**Section 5** – Project monitoring, verification and reporting requirements.

This information and guidance document is accompanied by the Application Form.

Potential applicants should read all documentation associated with this call carefully before making an application for funding.

Applicants should note that any misleading statements or false information submitted during the application process may render the application invalid, irrespective of the cause.

[1] Regulation (EU) No 2021/1149.

Each successful organisation will be required to sign a Grant Agreement with the Managing Authority setting out the terms and conditions of the grant. Expenditure incurred prior to signing of the grant agreement will not be eligible for reimbursement.

Under section 42 of the Irish Human Rights and Equality Act, 2014, An Garda Síochána has a positive legal duty to have regard to the need to eliminate discrimination, promote equality and protect the human rights of staff and persons who avail of the services provided. In accordance with this duty, An Garda Síochana requires that the Grantee, in carrying out the project that is the subject of the Grant Agreement, have regard to the need to eliminate discrimination, promote equality and protect the human rights of staff and persons to whom services are provided. A condition in the Grant Agreement will reflect this requirement.

### *1.2 Background*

The overall objective of the Internal Security Fund is to contribute to high levels of security across the EU, in particular by preventing and combating terrorism, radicalisation, serious and organised crime and cybercrime, by assisting and protecting victims of crime, and by preparing for, protecting against and effectively managing security-related incidents, risks and crises. The ISF has three Specific Objectives as set out above.

The European Commission approved Ireland's ISF National Programme 2021-2027[2] on 28 November 2022.

This Call concerns all Specific Objectives.

The Finance Directorate, An Garda Síochána is designated as Ireland's Managing Authority for the ISF. The funding available to Ireland under the ISF will be used over the lifetime of the National Programme to support actions that will help to achieve the Specific Objectives set out in Article 3 of the ISF Regulation[1].

The applicant organisation will be required to source, either from own resources, or from a third party the 25% or 10% remaining co-funding necessary for the project. The arrangements for sourcing this co-funding must be confirmed at application stage. Co-funding cannot be sourced from any other EU Fund.

[2] The current version of the National Programme is available to view at the following address: https://www.garda.ie/garda/en/about-us/our-departments/finance-services/internal-security-fund-isf-2021-2027-national-programming-period.html

### *1.3 Application details*

| | |
|---|---|
| **Co-funding** | Selected projects will be co-funded on the basis of 75% or 90% by the European Union under the ISF (via the Finance Directorate, An Garda Síochána), and 25% or 10% by a funding arrangement to be put in place by the applicant prior to the application being made (*see section 2.3.4 for eligibility criteria for 90% funding.*<br><br>All applicants are required to provide evidence of this funding arrangement as part of their application.<br><br>The remaining 10% / 25% funding cannot be sourced from any other EU Fund. |
| **Method of Funding** | Subject to the availability of funds, ISF funding will be in the form of a grant issued subject to the terms of the Grant Agreement and ongoing conditions. |
| **Duration of Projects** | Projects must commence prior to 31 December 2027 and should end no later than 31st December 2029.<br><br>The Managing Authority reserves the right to vary the maximum duration in exceptional circumstances subject to EU legislation. |
| **Geographical Scope** | All interventions should be focused on activity in the State. The selection of projects to receive funding will have regard to the desirability of achieving a geographical spread of activities. |
| **Application Deadlines** | Application – deadline – See call as published. |
| **Selection of Projects** | All valid applications will be scored in line with the scoring system outlined at Section 1.7 of this document. |
| **Eligibility – Activities** | Proposals must only contain actions that are eligible for funding under Ireland's ISF National Programme.<br><br>All actions should address one or more of the Specific Objectives set out at Section 1.1 of this document.<br><br>The National Programme[2] includes examples of the types of actions that may be funded. Actions not specified in the National Programme[2] may still be eligible for funding provided they address one or more Specific Objective(s).<br><br>Actions should be specific and, where relevant, should be complementary to actions financed under other European Union Funds. |

| | |
|---|---|
| | All activities must be non-profit in nature. |
| **Applicants** | Applicants must be legally constituted at the point of signing a Grant Agreement and must be able to enter into a legally binding Grant Agreement, should their application be approved.<br><br>If more than one organisation is applying for funding, one organisation must be nominated as the Lead Applicant. If successful, the Lead Applicant will sign the Grant Agreement and will carry the liability for ensuring its terms and conditions are met both by them and by all delivery partners. It is acceptable for an organisation to make more than one application under this call. However, in these circumstances, the projects proposed must be clearly separate and distinct. |
| **Procurement** | All procurement must be undertaken in line the Office of Government Procurement's Public Procurement Guidelines and EU law.<br><br>Applicants are recommended to familiarise themselves with the procurement rules, as failure to comply with these rules could result in expenditure being disallowed. |
| **Publicity** | It is a core requirement for successful projects to ensure that all participants and staff are aware of the use of ISF funding on their programme.<br><br>Accordingly, there is a requirement for extensive publicity of ISF support on all documentation, publicity and project materials/web-site.<br><br>Failure to comply could result in grants being reduced or withdrawn. |
| **Audit / Compliance** | All expenditure and activities will be subject to rigorous audit. Non-compliance may lead to financial penalty. Where non-compliance is identified, the Managing Authority may take steps to recover funds already disbursed. |
| **Indicator Data** | All projects will be required to maintain records in respect of the achievement of output and result indicator targets as set out on the application form. This will require projects to obtain and maintain copies of documents which confirm eligibility and completion. This information will need to be reported regularly to the Managing Authority, and will be subject to verification checks. |
| **Application listing multiple activities** | Where a project consists of more than one activity, the applicant is required to list each activity they plan to deliver, |

| | |
|---|---|
| | supported by a clear breakdown of costs. Expected outputs and results for each activity should be provided. |

### *1.4 Applications*

Applicants must complete the Application Form in Microsoft Word.

Incomplete application forms will be deemed ineligible.

Applications received by the closing date and time will be subject to an initial check by the Managing Authority to ensure that they are eligible for consideration. In order to be eligible, applications must:

- Be submitted on time;
- Be submitted by an eligible applicant organisation;
- Be complete (i.e., all relevant sections completed);
- Be signed by a person authorised to submit the application on behalf of the applicant organisation; and
- Provide evidence of remaining 10% / 25% funding required.

Applications that fail to meet this initial test will not be considered. Applications that pass this initial check will then go forward for further assessment.

### *1.5 Objectives of the Call*

| | |
|---|---|
| **Call Objectives** | Ireland's ISF National Programme contains a number of Specific Objectives to be achieved with the support of the ISF. This call is to select proposals for funding under the following Specific Objectives:<br>• Specific Objective 1,<br>• Specific Objective 2,<br>• Specific Objective 3. |
| **Indicative Actions** | Ireland's ISF National Programme 2021-2027[2] contains examples of the types of actions that may be funded under ISF. For some examples relevant to this call for proposals, please refer to the relevant subheadings for SO1, SO2 and SO3 in the National Programme[2].<br>Some actions will be the subject of direct awards to State bodies. |
| **Contribution to the Horizontal Principles** | Any actions selected for funding under this Call for Proposal shall be implemented with regard to the horizontal enabling conditions detailed in the National Programme[2]. |
| **Outputs and Results** | Proposals must include detailed outputs and results that applicants intend to achieve. Applicants are required to set out clear, measurable outcomes and targets for their project activities. |

### *1.6 Eligible expenditure*

Please refer to Section 3, which provides information on eligible expenditure.

Applicants must set out a budget showing total eligible cost, co-financing rate and requested EU contribution for the proposal. Separately eligible costs must be detailed by action dimension code (*see section 2.3.4 for details of available action dimension codes).* For all projects selected for funding, the Funds Administration Unit will, as part of its verification of expenditure, review backup documentation for all project expenditure.

Proof of direct expenditure incurred and paid will be required. Project staff costs must be supported by employment contracts and payroll documents, which have an explicit link to the project. Copies of invoices and receipts must be retained for all other direct and indirect costs incurred. Evidence of compliance with National and European Procurement Rules must be retained.

Where staff work part-time on the project and part-time on other activities, it is essential that detailed time-sheets are kept to enable the eligibility of staff costs to be determined.

Applicants must justify the salary levels proposed for project staff by reference to existing salary levels for similar positions in the labour market, and with due regard to the requirement for all activities funded to represent value-for-money.

### *1.7 Project selection criteria*

Applications which have passed the initial check will be assessed against the below selection criteria. The Evaluation Committee assesses all proposals by reference to the below criteria, with an individual weighting applied to each criterion. A proposal is required to receive an average passing mark for each criterion in order to be recommended for approval.

| Criterion | Total marks available |
|---|---|
| **Relevance** | 40% |
| **Organisation** | 30% |
| **Proposal Strength** | 15% |
| **Efficiency** | 15% |

| Criterion | Key question | Typical evaluation questions | Minimum passing score |
|---|---|---|---|
| **Relevance** | To what extent does the project address the Specific Objectives of the ISF and contribute to the selected eligible activity highlighted under the EU programming fiche? | Are project objectives clearly laid out and comply with the aims relating to the applicable Specific Objective (i.e., SO1/SO2/SO3)?<br><br>How relevant is the proposed project when compared to the requirements outlined in the ISF programming Fiche and its relevance to the applicable Specific | 30/40 (75%) |

| Criterion | Key question | Typical evaluation questions | Minimum passing score |
|---|---|---|---|
| | | Objective?<br><br>The extent to which the proposed activity fits with existing national policing policies. | |
| **Organisation** | Is it plausible on the basis of funding in the prior programming period, that the applicant will be able to successfully implement the project proposal and fulfil the obligations attached to the grant? | Is there evidence to support the capacity of the applicant to deliver on the proposed results.<br><br>Does the applicant have any prior experience of working with ISF requirements?<br><br>Evidence of the applicant to manage the proposed project in an appropriate manner.<br><br>Evidence of appropriate governance and financial viability of the organisation.<br><br>Previous delivery of ISF funded projects and meeting of reporting requirements. | 18/30 (60%) |
| **Proposal Strength** | Is the project proposal clear and concrete in all areas?<br><br>Are the anticipated activities and results to be achieved quantifiable and measurable? | How effective is the proposal and the outlay of the services that are to be made available?<br><br>How detailed and structured is the proposal?<br><br>How effective does the Proposal address the requirements of OGP Procurement guidelines.? | 9/15 (60%) |
| **Efficiency** | How clear and well-structured is the project budget and do the returns offer value for money? | How clear and well-structured is the project budget?<br><br>Are the Costs in line with Market norms?<br><br>Are the outlined overhead costs reasonable?<br><br>Are the overall project costs realistic and relevant? | 9/15 (60%) |

| Criterion | Key question | Typical evaluation questions | Minimum passing score |
|---|---|---|---|
| | | Does the overall project cost warrant the proposed returns from the project? | |

Proposing organisations should have regard to the above selection criteria and related evaluation questions when drafting a business case for a proposal, and consider whether the business case adequately addresses the criteria.

### *1.8 Notice of outcome*

All applicants will be informed of the outcome of their application.

### *1.9 Grant Agreement*

Successful applicants will be required to enter into a Grant Agreement with An Garda Síochána and to comply with all financial and other reporting requirements, including ongoing monitoring and evaluation in line with Article 74 of Regulation (EU) No 2021/1060.

The Grant Agreement is a legally binding document. Successful applicants will be subject to the terms and conditions contained in the Grant Agreement. Failure to meet any of the conditions of the Grant Agreement may result in the withdrawal of funding and, if necessary, recovery of some or all of funds issued.
The minimum requirements for ISF Grant Agreements are set out in Article 73(3) of Regulation (EU) No 2021/1060, according to which the Grant Agreement must include (but is not limited to):

- Specific requirements regarding the products or services to be delivered;
- The financing plan;
- The time limit for its execution;
- The method to be applied for determining the cost of the operation, and
- The conditions for payment of the support.

Funding is at all times conditional on the availability of resources in the relevant subheads of the An Garda Síochána Vote and this will be stipulated in the Grant Agreement.

Grant funding will be paid by electronic fund transfer (EFT) in accordance with the terms set out in the Grant Agreement, and subject to confirmation that a current Tax Clearance Certificate is in place.

### *1.10 Submission of applications*

Applications must be completed using the Application Form; no other form of application will be accepted.

When completed, all documents, together with any additional documentation requested must then be submitted via email to ISF@garda.ie, with the following subject line: 'ISF call for proposals 2026 – (*Project name*)'

It is the responsibility of the applicant to ensure that emails are clearly addressed and submitted in accordance with these directions.

### *1.11 Data protection.*

An Garda Síochána will treat all information and personal data you give us as confidential. An Garda Síochána is registered as a Data Controller under the General Data Protection Regulation.

### *1.12 Freedom of information*

An Garda Síochána is subject to the provisions of the Freedom of Information (FOI) Act 2014. The FOI Act imposes various duties on the An Garda Síochána and gives certain rights to individuals to access the records of An Garda Síochána, including those relating to reasons for decisions of An Garda Síochána. An Garda Síochána will hold records for all applications and these may be subject to FOI requests.

If, at the time of providing information to An Garda Síochána, your organisation considers certain information to be commercially sensitive, confidential or of a personal nature, and that there may therefore be reasons to consider it exempt from disclosure under FOI, you must identify the relevant information and specify the reasons for its sensitivity by email with submission of your application. However, An Garda Síochána can give no guarantee on the final outcome of any FOI request in any instance. An Garda Síochána may release all other information supplied by your organisation (without prior consultation), in response to an FOI request.

## **2.** Guidance on making an application

Please review this guidance in full before completing the application form.

### *2.1 Preliminary questions*

Queries regarding this call for proposals may be submitted to ISF@garda.ie with the subject heading: 'ISF call for proposals 2026 query' on or before 26/06/2026.

### *2.2 Section A: Administration*

In section A of the form, you will be asked to provide some information in respect of your organisation.

Where there are multiple organisations involved in the application, please provide details of a lead applicant, as well as details of additional applicants.

### *2.3 Section B: Presentation of the funding proposal*

#### 2.3.1 **Section B1: Description of the project**

Please provide a summary, detailed project plan and outline the proposed benefits of the project. You should also describe the intended delivery model, as well as how the project will comply with the Office of Government Procurement's Public Procurement Guidelines for Goods and Services.

#### 2.3.2 **Section B2: Identification of specific objectives and policy aims**

Please indicate which Specific Objective your proposal addresses, as well as the policy aims that the proposal seeks to address.

Article 3 of the ISF Regulation[1] sets out three 'Specific Objectives' of the ISF. Every project proposal submitted must fulfil at least one of the three Specific Objectives. It is therefore important to explain how the proposal will address the Specific Objective.

*Scope of support – Annex III to the ISF Regulation*

Annex III to the ISF Regulation[1] provides a list of 12 types of action that the ISF may support. This list is not exhaustive; however, it is useful to assess whether the proposal will correspond with any of these actions and explain such in the business case. It is also useful to explain the current state of play regarding the relevant action, as well as particular challenges being faced. These actions are as follows:

a. Setting up, adapting and maintaining ICT systems that contribute to the achievement of the objectives of this Regulation, training on the use of such systems, and testing and improving the interoperability components and data quality of such systems,
b. Monitoring of the implementation of Union law and Union policy objectives in the Member States in the area of security-relevant information systems, including data protection, privacy and data security,
c. EU policy cycle/EMPACT operational actions,
d. Actions supporting an effective and coordinated response to crises and linking up existing sector-specific capabilities, expertise centres and situational awareness centres, including those for health, civil protection, terrorism and cybercrime,
e. Actions developing innovative methods or deploying new technologies with a potential for transferability to other Member States, in particular projects aimed at testing and validating the outcome of Union-funded security research projects,

f. Actions that improve resilience as regards emerging threats, including trafficking via online channels, hybrid threats, the malicious use of unmanned aerial systems and chemical, biological, radiological and nuclear threats,
g. Providing support to thematic or cross-theme networks of specialised national units and national contact points to improve mutual confidence, the exchange and dissemination of know-how, information, experience and best practices, the pooling of resources and expertise in joint centres of excellence,
h. Education and training for staff and experts in relevant law enforcement and judicial authorities and administrative agencies, taking into account operational needs and risk analyses, in cooperation with CEPOL and, when applicable, the European Judicial Training Network, including education and training on prevention policies, with special emphasis on fundamental rights and non-discrimination,
i. Cooperation with the private sector, for example in the fight against cybercrime, in order to build trust and improve coordination, contingency planning and the exchange and dissemination of information and best practices among public and private actors, including in the protection of public spaces and critical infrastructure,
j. Actions empowering communities to develop local approaches and prevention policies, and awareness-raising and communication activities among stakeholders and the general public on Union security policies,
k. Financing of equipment, means of transport, communication systems and security-relevant facilities, and
l. Financing the cost of staff involved in the actions that are supported by the Fund or actions requiring involvement of staff for technical or security-related reasons.

Reference to programming *fiche*
The EU has developed a programming fiche (see Appendix I), which outlines various policy areas of focus that should be addressed by ISF projects. Prospective applicants should review the programming fiche and outline which policy aims will be addressed by the proposed project.

It is also useful to explain the current state of play regarding the relevant policy aims, as well as particular challenges being faced.

Please contact the ISF section mailbox (ISF@Garda.ie) with any queries relating to demonstrating how a project will address the policy aims outlined in the programming fiche.

### 2.3.3 **Section B3: Project performance indicators**

Please outline which output and result indicators the project will address in the requested format per the application form.

*Output and Result indicators*

Article 27 of the ISF Regulation[1] explains that Fund progress is communicated to the Commission by way of output and result indicators, with specific indicators relevant to each Specific Objective. Annex VIII to the ISF Regulation[1] outlines the indicators as follows:

| Specific Objective 1 |
|---|
| *Output Indicators* |
| Number of participants in training activities |
| Number of expert meetings / workshops / study visits |
| Number of ICT systems set up / adapted / maintained |
| Number of equipment items purchased |
| *Result Indicators* |
| Number of ICT systems made interoperable in the Member States / with security-relevant EU and decentralised information systems / with international databases |
| Number of administrative units that have set up new, or adapted existing, information exchange mechanisms / procedures / tools / guidance for exchange of information with other Member States / Union bodies, offices or agencies / third countries / international organisations. |
| Number of participants who consider the training useful for their work |
| Number of participants who report three months after the training activity that they are using the skills and competences acquired during that training activity |

| Specific Objective 2 |
|---|
| *Output Indicators* |
| Number of cross-border operations, separately specifying:<br>- The number of joint investigation teams<br>- The number of EU policy cycle / EMPACT operational activities |
| Number of expert meetings / workshops / study visits / common exercises |
| Number of equipment items purchased |
| Number of transport means purchased for cross-border operations |
| *Result Indicators* |
| The estimated value of assets frozen in the context of cross-border operations |
| Quantity of illicit drugs seized in the context of cross-border operations, by type of product<br>- cannabis;<br>- opioids, including heroin;<br>- cocaine;<br>- synthetic drugs, including amphetamine-type stimulants (including amphetamine and methamphetamine) and MDMA;<br>- new psychoactive substances;<br>- other illicit drugs. |
| Quantity of weapons seized in the context of cross-border operations, by type of weapon<br>- weapons of war: automatic firearms and heavy firearms (anti-tank, rocket launcher, mortar, etc.);<br>- other short firearms: revolvers and pistols (including salute and acoustic weapons);<br>- other long firearms: rifles and shotguns (including salute and acoustic weapons). |
| Number of administrative units that have developed / adapted existing mechanisms / procedures / tools / guidance for cooperation with other Member States / Union bodies, offices or agencies / third countries / international organisations. |
| Number of staff involved in cross-border operations |
| Number of Schengen evaluation recommendations addressed |

| Specific Objective 3 |
|---|
| *Output Indicators* |
| Number of participants in training activities |
| Number of exchange programmes / workshops / study visits |
| Number of equipment items purchased |
| Number of transport means purchased |
| Number of items of infrastructure / security-relevant facilities / tools / mechanisms constructed / purchased / upgraded |
| Number of projects to prevent crime |
| Number of projects to assist victims of crime |
| Number of victims of crime assisted |
| *Result Indicators* |
| Number of initiatives developed / expanded to prevent radicalisation |
| Number of initiatives developed / expanded to protect / support witnesses and whistle-blowers |
| Number of critical infrastructure / public spaces with new adapted facilities protecting against security-related risks |
| Number of participants who consider the training activity useful for their work |
| Number of participants who report three months after the training activity that they are using the skills and competences acquired during that training activity |

### 2.3.4 **Section B4: Budget and costing**

Please provide the requested budgetary information in questions 19 – 22.

*Proposed budget*

Table 2 in Annex VI to the ISF Regulation[1] provides a list of 11 'codes for the type of action dimension.' These are codes by which project expenditure will be categorised when successful applicants report periodically to the Managing Authority and when a payment application is prepared for submission to the European Commission.

| | |
|---|---|
| **001** | ICT systems, interoperability, data quality (excluding equipment) |
| **002** | Networks, centres of excellence, cooperation structures, joint actions and operations |
| **003** | Joint Investigation Teams (JITs) or other joint operations |
| **004** | Secondment or deployment of experts |
| **005** | Training |
| **006** | Exchange of best practices, workshops, conferences, events, awareness-raising campaigns, communication activities |
| **007** | Studies, pilot projects, risk assessments |
| **008** | Equipment |
| **009** | Means of transport |
| **010** | Buildings, facilities |
| **011** | Deployment or other follow-up of research projects |

Proposals should categorise projected project expenditure in line with the 11 above codes. Prospective applicants should also be cognisant of the fact that, per Article 13(7) of the ISF Regulation[1], a maximum of 35% of the total allocation for project expenditure for the National Programme may be spent on equipment (action dimension code 008). Should the requested budget of successful applications under action dimension code 008 cumulatively exceed 35% of the budgeted expenditure, the final amount to be allocated to an applicant's proposal under action dimension code 008 may be lowered.

It is important that the components of the budget are laid out in a clear and understandable manner, as the Evaluation Committee comprises individuals from non-financial backgrounds. The budget should map each project deliverable to one of the 11 codes above. An example of a completed budget is detailed below:

| Activities | Total eligible cost | Action dimension code |
|---|---|---|
| Software System 1 | €250,000.00 | 001 ICT systems, interoperability, data quality (excluding equipment) |
| Software System 2 | €50,000.00 | 001 ICT systems, interoperability, data quality (excluding equipment) |
| Laptops | €200,000.00 | 008 Equipment |
| Total | €500,000.00 | |

*Value for money*

In addition to a clear and well-structured budget, proposals should also include an explanation as to how the proposed costs are in line with market norms and that value for money will be sought throughout the project.

*Actions in Annex IV to the ISF Regulation*

As outlined above, proposals that address actions listed in Annex IV to the ISF Regulation[1] may qualify for co-funding of 90% from the EU. If this applies to the proposal, please explain which action will be addressed and how the project will address the action.

The actions listed in Annex IV are as follows:

(1) Projects which aim to prevent and counter radicalisation,
(2) Projects which aim to improve the interoperability of EU information systems and national ICT systems, insofar as provided for by Union or Member State law,
(3) Projects which aim to fight the most important threats posed by serious and organised crime, in the framework of EU policy cycle/EMPACT operational actions,

(4) Projects which aim to prevent and fight cybercrime, in particular child sexual exploitation online, and crimes where the internet is the primary platform for evidence collection, and
(5) Projects which aim to improve the security and resilience of critical infrastructure.

Please contact the ISF section mailbox (ISF@Garda.ie) with any queries in relation to whether a project may address one of the actions listed in Annex IV.

**3.** Eligibility of expenditure

Articles 63-68 of Regulation (EU) No 2021/1060[3] set out the conditions for determining the eligibility of expenditure. A brief outline of eligibility of expenditure rules is provided below.

- The expenditure must have been incurred by a beneficiary during the term of the contract.
- The expenditure must have been for operations set out in the Grant Agreement. All expenditure must be actually incurred and paid, recorded in the beneficiary's accounts and supported by appropriate documents to ensure an adequate audit trail. The supporting documents must be retained until the 31st December 2038 unless otherwise notified by the Managing Authority.
- All expenditure must be provided for in the Grant Agreement and/or the agreed project budget.
- All expenditure must be necessary for implementation of the project activities covered by the Grant Agreement.
- All expenditure must be reasonable and justified and in line with the principles of sound financial management, in particular in terms of value for money and cost-effectiveness.
- All EU publicity and information requirements must be adhered to.
- All EU and National Procurement Rules must be adhered to.
- Staff costs must be supported by contracts of employment, payroll records (including salary slips, Revenue payment verification) and detailed timesheets (for employees working part time on the project and part time on other activities) completed according to a prescribed template. This will apply both for employees in the project organisation and any contract staff working on the project.

In addition, Article 5(5) of Regulation (EU) No 2021/1149 provides that projects which support the following actions are **ineligible** for funding under the ISF:

(a) Actions limited to the maintenance of public order at national level,
(b) Actions with a military or defence purpose,
(c) Equipment of which the primary purpose is customs control,
(d) Coercive equipment, including weapons, ammunition, explosives and riot batons, except for training purposes, and

[3] Regulation (EU) No 2021/1160

(e) Informant rewards and flash money outside the framework of an EU policy cycle / EMPACT operational action.

**4.** Systems and records

**Governance**
All procedures and systems required in managing public funds must be applied, monitored and reviewed by the board of each grant funded organisation. The quality of your corporate governance and decision-making is fundamental to your contract compliance. Where there is more than one organisation responsible for delivering the project, the lead Organisation has the responsibility of reporting to the Funds Administration Unit all project financial expenditure, activities, outputs and indicator data for the project being funded.

**Internal Financial Procedures**
Each organisation receiving funding must have in place an internal financial procedures document specifying the practices and procedures in place, as well as who has responsibility for them.

**Financial Information and Accounts**
The beneficiary must maintain proper books of account to record the day-to-day transactions of the organisation. The books and records should record all income received and all payments made; these form the basis of the financial accounts.

**Recording Monitoring Data**
The beneficiary must maintain records to support the achievement of indicator targets and be in a position to provide requested information on these to the relevant National and EU Authorities. This will require projects to review such documentation as is necessary to confirm that activities are eligible to an ISF project, and to retain a copy of such document(s) for verification purposes.

**Apportionment Policy**
It is acknowledged that ISF funding provided may represent only one element of the funding for the organisation's activities. Apportionment of shared costs of administration, management costs and overheads is allowed provided it can be supported by a fair apportionment policy that allocates costs pro rata.

**Travel & Subsistence**
You are recommended to have a Travel & Subsistence policy that limits the amounts payable for travel and subsistence to the Civil Service travel and subsistence rates, or lower.

## 5. Project monitoring, verification and reporting requirements

### *5.1 Project Monitoring*

Monitoring is the process which involves the regular recording and reporting of information about participants and activities in order to:

- Indicate how each Beneficiary is progressing in delivering the project or service described in the Grant Agreement;
- Ensure allocated funds are used for their intended purpose; and
- Provide data that the Managing Authority can aggregate and analyse to generate information on the overall size, value and impact of the programme.

All projects are required to submit regular returns to the Managing Authority per the grant agreement and are expected to record data via an IT software system called "EPPM":

- Financial information, detailing expenditure on the project, using template worksheets that will be provided;
- Operational information, setting out achievements against plan for the project, using template worksheets that will be provided;
- Annual Audited Accounts or in cases where an audit exemption applies, an Income and Expenditure Account and Statement of Assets and Liabilities must be provided upon request.

### *5.2 Common Monitoring and Evaluation Reports*

You will be asked to provide information for evaluation report(s) during the 2021-2027 programming cycle.

### *5.3 Management Verifications*

Desk-based verifications and on-the spot (both announced and un-announced) verifications of operations will be carried out in respect of funded projects.

#### 5.3.1 **Desk-Based Administrative verifications/controls**

Administrative verifications will be carried out in respect of all quarterly financial reports submitted to the Managing Authority. Desk-based verifications comprise a complete review of the scanned supporting documents (such as invoices, proofs of payment, receipts, payslips, timesheets, and proofs of delivery and recruitment/procurement details).

#### 5.3.2 **On-the-spot verifications**

On-the-spot verifications are intended to verify the implementation and progress of the project on site. On-the-spot checks ensure that the delivery of the product or service is in compliance with the terms and conditions of the Grant Agreement, and that the beneficiary is providing accurate information regarding the physical and financial implementation of the operation. They are also used to ensure that the Beneficiary is complying with the ISF publicity requirements.

## 6. Appendix I



**Programming Fiche**
**Ireland**

**Internal Security Fund (ISF)**

## Future priorities

| **Specific objective 1 - to increase the exchange of information among and within the Union law enforcement and other competent authorities and other relevant Union bodies as well as with third countries and international organisations** |
|---|
| **Current priorities or types of actions in the National Programme that could be continued under this specific objective**<br>• Create effective systems for the exchange of information between all relevant national actors, neighbouring countries, other EU Member states, EU agencies and international organisations.<br>**Policy issues (in priority order) that should be addressed in the future under this specific objective**<br><br>**Information Systems**<br>• Ensure the full and uniform implementation of the Union acquis on security supporting information exchange (e.g. Prüm, PNR, SIS II (police) or in relation to Europol data.<br>• Set up a SPOC (Single Point of Contact) for international police cooperation in the exchange and management of criminal intelligence linked to cross-border crime.<br>• Set up and adapt national IT systems or devices in order to ensure the effective connection to security relevant Union information systems and communication networks, including their interoperability.<br>• Acquire, adjust or develop appropriate tools to address identified gaps in the EU information architecture, for instance with the objective of extending the access to Europol's secure operational network to all relevant competent authorities at the confidentiality level required by the nature of the cooperation, and enhancing connectivity infrastructure so that Europol products and services SIENA, EIS, QUEST could be rolled out beyond Europol National Units, in particular to AROs and PIUs;<br>• Set up and adapt the relevant IT systems to address relevant and future Union priorities, (for example: single window approach for the collection of API and PNR data, adoption of artificial intelligence tools for the processing of PNR, development of communication networks for the exchange of PNR at EU level and the interoperability with and connection to the various European (and international) systems and databases relevant for the processing of PNR)<br>• Create a UMF-based workflow interface with national processing systems to allow automated information exchange and follow up to hits and making UMF as the European standard for data exchanges;<br>• Introduce/update EIS Data Loaders, incl. New Generation Data Loaders (based on UMF, with a possibility of providing data also for analysis);<br>• QUEST integration with national single search system with a view to facilitating access/searching Europol data, including the forthcoming pilot project on QUEST+ and automation of searching (QUEST) and hit-follow up processes (SIENA web service);<br>• Upgrade to SIENA CONFIDENTIAL especially (but not only) for CT Units;<br>• Support SIENA web service integration with national case management/messaging systems and in particular the integration into 24/7 SPOC where also SIRENE bureaux and INTERPOL NCB reside;<br>• Implement and upgrade the law enforcement access to European Search Portal (ESP) and the large-scale European Information Systems (SIS, VIS, Eurodac, EES, ETIAS, ECRIS-TCN), noting that it will possible to make QUEST+ available via ESP (according to Interoperability Regulation);<br>• Upgrade MS' capabilities for Identity & Access Management, especially since Europol provides multi-level security (BPL, EU-REST and EU-CONF). |

**Cybercrime**

- Develop capabilities to deal with encrypted evidence through the development and sharing of solutions and good practices through participation in Europol's network of points of encryption expertise.
- Foster the involvement of law enforcement in 5G standardization bodies and develop close cooperation between law enforcement and relevant technology providers/telecommunication operators, to enable timely implementation of lawful interception mechanisms in 5G networks.
- Ensure that systems are in place for the recording, production and provision of statistical data measuring the reporting, investigative and judicial phases of cybercrime, in conformity with Article 18 of Directive (EU) 2019/713 and Article 14 of Directive 2013/40/EU.
- Ensure that the necessary laws, regulations and administrative provisions are in force to comply with Directive 2013/40/EU on attacks against information systems.
- Ensure that the necessary laws, administrative provisions and technical processes are in place to allow for an effective fight against child sexual abuse. In particular, the necessary measures must be in place to enable the transmission of information concerning the existence of criminal convictions for any offences referred to in Articles 3-7 of the Directive 2011/93/EU on combating child sexual abuse and sexual exploitation, or of any disqualification from exercising activities involving regular and direct contact with children arising from such criminal convictions. The transmission must be carried out in accordance with the procedures set out in the Council Framework Decision 2009/315/JHA on the organisation and content of the exchange of information extracted from the criminal record between Member States when requested under Article 6 of that Framework Decision with the consent of the person concerned.

**Organised Crime**

- Ensure the full implementation of **Directive 2019/1153 on law enforcement access to financial information to combat serious crimes**. Pursuant to the Directive, Ireland has to provide the designated national competent authorities and the Asset Recovery Office with **direct access** to the centralised bank account registry or electronic data retrieval system by **1 August 2021**. It is worth noting that there is currently no operational registry or system in Ireland.
- Strengthen the operational capacity of the national Asset Recovery Offices, in particular by providing them with direct access to the relevant national databases (e.g. criminal records, company registries, vehicle registries, land registries, maritime registries).
- Improve the operational capacity to manage frozen and confiscated assets by, for example, setting up an Asset Management Office, or by strengthening the capabilities of the existing Asset Management Office, or equivalent mechanism.
- Set up or strengthen national databases for the registration of frozen assets.

**Anti-Corruption**

- Facilitate and streamline the flow of information between institutional actors in Member States (law enforcement, audit and control bodies, Financial Intelligence Unit - FIUs, tax authorities, competition authorities, prosecution bodies) in order to facilitate the detection and investigation of complex corruption and economic crime cases.

**Firearms**

- Support the establishment of a national focal point on firearms to produce better analysis of all information available in the area of illicit firearms, ensure full participation in the exchange of information with Europol in the area of firearms trafficking, act as a repository for firearms-related intelligence both criminal and ballistic, and as a repository for all lost, stolen and recovered firearms.

**Migrant smuggling**

- Training activities in the area of migrant smuggling at national level for LE and judiciary officers.
- Ensure resources to further make use of opportunities offered by EU Agencies and partners participating in the EMPACT Policy Cycle.

**Suggestions for desired outcomes**

- Ensure the uniform application of the Union acquis on security supporting information exchange (e.g. Prüm, PNR, SIS II). Increased use of EU security relevant information systems and communication networks.

- Provide the competent authorities with swifter access to financial and other relevant information and improve the effectiveness of financial investigations into serious crime.
- Address, if applicable, as a result of the European Semester, those country-specific recommendations (CSRs) which concern key security policy priorities, in particular the fight against corruption and money laundering.

**Specific objective 2 - to intensify cross-border joint operations among and within the Union law enforcement and other competent authorities in relation to serious and organised crime with a cross-border dimension**

**Current priorities or types of actions in the National Programme that could be continued under this specific objective**

- Participate in joint cross-border actions at international level.

**Policy issues (in priority order) that should be addressed in the future under this specific objective**

**Law Enforcement Cooperation**

- Facilitate and improve the use of joint investigation teams, joint operations and other operational cooperation mechanisms in the context of the EU Policy Cycle (EMPACT), with special emphasis on cross-border operations.
- Develop joint threat / risk analyses to better target joint operations or patrols, and the including for the querying of information systems with alphanumeric and biometric data.
- Develop training and awareness raising activities in order to enhance the capabilities of the personnel working in Passenger Information Units (PIUs) responsible for the processing of PNR data to conduct joint analysis and joint targeting activities.
- Support participation in the Joint Cybercrime Taskforce (J-CAT), through the secondment of dedicated cybercrime liaison officers at Europol.

**Child sexual abuse**

- Enable efficient cross-border cooperation in the fight against child sexual abuse, including in investigations and the exchange of best practices. Cross-border cooperation should also be enabled at a global level, in coherence with Member States' commitments as part of the We Protect Global Alliance to End Child Sexual Exploitation Online.

**Fraud and counterfeiting of non-cash means of payment**

- Create dedicated points of contact for fraud and counterfeiting of non-cash means of payment, with a view to preparing the implementation of Article 14(1) of Directive (EU)2019/713.

**Organised Crime**

- Increase coordination and cooperation of law enforcement authorities and other competent authorities dealing with organised crime, for example through networks of specialised national units, Union networks and cooperation structures, or Union centres of excellence.
- Provide financing for operational support in complex high profile investigations requiring highly specialised criminal expertise, in particular support to Member States' participation in Operational Task Forces (OTF) to identify High Value Targets (HVT) posing the highest risk to the internal security of the EU.
- Increase exchange on EU crime statistics in harmonised manner with a possibility to create EU CRIM statistic date base (database on a number of phenomena could help us to define the threats and risks better).
- Extend assistance to state-of-the-art forensic expertise, for example deployment of digital forensic tactical advisers; large-scale technically demanding support on the ground; network acquisition/cloud forensics/live forensics, etc. deployment of technologies such as ANPR, UAVs or mobile communication devices,

**Trafficking in human beings**

- Focus on preventing trafficking in human beings, by countering the impunity that fosters the crime, enhancing national and transnational efforts to step up investigations, prosecution and convictions of all perpetrators.

**Anti-Corruption**

- Facilitate operational cooperation and coordination among law enforcement authorities and other relevant authorities in and among the EU Member States and with relevant agencies and third country authorities for a more effective investigation of cross border corruption cases.
- Facilitate information exchange and training on best practices in investigating crossborder corruption cases.

**Drugs**

- Enhance operational cooperation between MS and with Europol and the EMCDDA to disrupt the illicit drugs market, taking into account current trends.
- Improve and harmonise national data collection mechanisms on drug supply indicators and drug production sites.
- Improve monitoring and operational resources in cooperation with EUROPOL and the EMCDDA against drug trafficking and distribution using online platforms such as social media, websites, Darknet markets, including developing new responses to tackle the threat posed by trafficking through postal and parcel deliveries, including through informal parcel delivery entities.
- Better respond to a globalised drug market by strengthening partnerships between Member States' authorities, international organisations, third countries and with industry, as well as operational actions identified under EU dialogues on drugs with third countries.
- Contribute to a measurable reduction of the demand for drugs on what concerns prevention.

**Firearms**

- Enhance operational cooperation to fight against firearms trafficking along firearms trafficking routes, notably by strengthening the operational cooperation among law enforcement authorities and improving knowledge, detection, investigation and prosecution in using dedicated investigative tools (i.e. controlled deliveries, hot pursuit, tapping etc.).

**Migrant smuggling**

- Ensure resources to allow efficient cooperation between EU MS LEAs and Third Countries' LEAs, including through JITs/COPs.
- Ensure resources to allow increased use of Eurojust support for Joint Investigation Teams (both with EU and non-EU countries) in the area of migrant smuggling.

**Suggestions for desired outcomes**

- Increased number of joint cross-border actions supported by the Fund. Enhanced operational cooperation of LE authorities through transnational networks.
- Address, if applicable, as a result of the European Semester, those country-specific recommendations (CSRs) which concern key security policy priorities, in particular the fight against corruption and money laundering.

**Specific objective 3 - to support effort at strengthening the capabilities in relation to combatting and preventing crime including terrorism in particular through increased cooperation between public authorities, civil society and private partners across the Member States**

**Current priorities or types of actions in the National Programme that could be continued under this specific objective**

- Anti-radicalisation actions.
- Develop the capabilities of the competent authorities to detect and combat crime.
- Training programmes.

**Policy issues (in priority order) that should be addressed in the future under this specific Objective**

**Law Enforcement Cooperation / Training**

- To increase law enforcement (joint) trainings, exercises, mutual learning, specialised exchange programmes and sharing of best practice including in and with third countries and other relevant actors, in cooperation with CEPOL and in line with the Strategic Training Needs Analysis when applicable.
- To increase training, exchange of best practices (including the Unions agencies, such as CEPOL and Europol, as well as air carriers' industry and other relevant actors) on the development of PNR systems and the exchange of PNR data.
- To focus training projects on the following policy priorities under each crime area: open source intelligence, data collection, analysis and application; financial investigations, money flows, alternative banking, etc.; elements of cyber investigations, darknet and e-evidence; document fraud; fundamental and human rights; crime prevention; respective areas of forensics; links between different crime areas; and English language, specific professional terminology.
- To support the development of CEPOL National Units with adequate resources to ensure Law Enforcement training reaches all relevant Law Enforcement bodies.
- To exploit synergies by pooling resources and knowledge among Member States and other relevant actors, including civil society through, for instance, the creation of joint centres of excellence, the development of joint risk assessments, or common operational support centres for jointly conducted operations.
- To increase analytical capacities especially from mobile devices (UFED).
- To ensure adequate multidisciplinary counter-crime structures to deal with increasing poly-criminal organised crime groups often posing a mafia style threat. This multidisciplinary nature should also go beyond solely law enforcement aspects to include cooperation with the private sector, third countries and be carried forward along the whole penal chain. The multidisciplinary approach should also be reflected in the provision of resources to ensure timely data collection on criminal justice statistics collected by Eurostat (e.g. migrant smuggling) - including cross-cutting collection from various authorities such as police, prosecution, courts, prisons.
- To establish a list of trusted interpreters and translators at national/regional level to support investigative and judicial follow-up of cross-border crimes.

**Prevention of radicalisation**

- Rehabilitation, reintegration and deradicalisation: Multi-agency cooperation between relevant partner organisations, with a view to rehabilitation, reintegration and risk management of radicalised individuals (including after release), with a focus also on returning foreign terrorist fighters and their families. This includes exit programmes and specialised training programmes for professionals and community partners.
    - Countering online extremist and terrorist propaganda by strengthening capabilities to detect and refer terrorist content and coordinate with Europol; support the development of alternative and counter narratives as well as strategic communication capabilities.
    - Local and multi-agency approach: Support to local and regional administrations and initiatives, in particular to develop local prevention strategies, action plans, collaborations among relevant stakeholders and other capacity building actions.
- Ideology and polarization: Address all forms of violent extremism, including right wing extremism. Work with communities (training and civic education for religious leaders), support local authorities to develop an action plan for dealing with presence of local extremist groups, support information and awareness raising campaigns on how to report hate speech and threats online and in local communities, encourage dialogue with media on a common understanding of responsible reporting on extremist violence and extremist groups.
    - Early detection, recognizing signs of radicalisation, strengthening resilience, community focus, multi-agency approach.

**Protection of citizens and infrastructure**

- Protection of public spaces: the actions could cover: enhanced public-private cooperation; enhanced protection against threats posed by Unmanned Aerial Vehicles and other emerging threats; acquisition and use of detection equipment, including mobile, regarding chemical, biological, radiological, nuclear and explosives (CBRN-E) threats.
- CBRN-E: the actions could include: 1) effective implementation and enforcement of the new Explosives precursors Regulation, including online mystery shopping; different tools to raise awareness in the supply chain of the obligations of the Regulation and evaluate their effectiveness;

2) pooling of resources and knowledge among Member States, sharing of good practices, and conducting trainings and exercises; 3) measures to enhance the security of radioactive sources, including upgrade in physical protection and awareness raising activities.

- Addressing insider threat: the actions could include background checks (in particular in aviation, but also in relation to protection of major public events and for personnel with access to CBRN materials).
- Critical Infrastructure Protection: the actions could include: 1) analysis of interdependencies, vulnerabilities and possible cascading effects on critical infrastructure networks, possibly in conjunction with neighbouring Member States. 2) measures to improve cooperation and support to critical infrastructure operators, e.g. establishing mechanisms for regular dialogue between authorities and operators, facilitating the exchange of threat and incident information, providing training to operators' security staff, disseminating guidance or best practice on security standards, establishing common criteria for risk assessments, or conducting exercises to test critical infrastructure protection and resilience. 3) A review of the state of play and future trends in application of the Directive 2008/114 on European Critical Infrastructures (ECI) and especially of the part on identification of ECIs.

**Combating terrorist financing**

- Strengthen capabilities in relation to counter-terrorism financial investigations, by improving financial investigation techniques and applying them more comprehensively, developing means to deal with emerging financial products and services, and intensifying cross-border joint operations among and within the Union law enforcement and in cooperation with Europol, and private entities. Particular emphasis might be placed on improving capabilities to conduct financial investigations into cryptocurrencies or other virtual assets.

**Drugs**

- Reduce vulnerabilities at external borders by enhancing risk analysis and profiling, intelligence sharing and implementation of proven approaches at maritime ports and airports.
- Enhance forensic capacity at national level to determine and address the threats posed by innovations in drug production and trafficking methods.

**Encryption**

- Support LE officers to allow their participation in the training courses developed by ECTEG (European Cybercrime Training and Education Group) and (in most cases) delivered by CEPOL.

**Cybercrime**

- Support LE officers to allow their participation in the training courses developed by ECTEG (European Cybercrime Training and Education Group) and (in most cases) delivered by CEPOL including the CEPOL Cybercrime Academy.
- Reinforce/develop training programmes based on competencies described in the EU Training Competencies Framework and on the training priorities identified in the CEPOL Operational Training Needs Analysis (OTNA) on Cybercrime. Use of available materials (e.g. ECTEG courses) is recommended.
- Cyber-crime centre of excellence: foster close cooperation between law enforcement authorities and academia, with a view to better preventing and investigating cybercrime, developing investigative tools, administrating trainings and developing dedicated courses and accreditation of experts.
- Cyber-crime centre of excellence: foster close cooperation between law enforcement authorities and academia, with a view to better preventing and investigating cybercrime, developing investigative tools, administrating trainings and developing dedicated courses and accreditation of experts.
- Ensure/develop/improve platforms for online reporting of crimes committed online, especially with regard to fraud and counterfeiting of non-cash means of payment.
- Develop/set up entities able to assist victims of cybercrime and online fraud, especially with regard to identity theft, with a view to preparing the implementation of Article 16 of Directive (EU) 2019/713.
- Enable the development and implementation of measures to prevent the sexual abuse and sexual exploitation of children, including through public-private partnerships and cooperation with civil society and academia. Of particular relevance are prevention programmes to prevent recidivism and programmes for persons who fear that they might sexually offend against children, and, in general,

the measures referred to in Articles 21 to 24 of Directive 2011/93/EU on combatting child sexual abuse and sexual exploitation.

**Organised Crime**

- Strengthen capabilities in investigating organised crime with a focus on High Value Targets.
- Increase application of the administrative approach to tackle serious and organised crime and provide for legal framework to allow for better exchange of administrative information across borders.
- Strengthen capacities to develop and make use of special investigative techniques relevant to the fight against organised crime.

**Anti-Corruption**

- Enhance the capacity of the national authorities, in particular the dedicated anticorruption unit in An Garda Síochána in order to improve the investigation and prosecution of corruption via training, specialised exchange programmes and sharing of good practices with a view to achieving a better prevention, detection and repression of corruption in the public and private sector.
- Support civil society actions in the area of preventing and detecting corruption.
- Facilitate improvement of national statistical data collections on the treatment of corruption cases in the criminal justice system in Member States in order to achieve a better and comparable evidence-base for policy making.

**Trafficking in Human Beings (THB)**

- The priorities related to the fight against THB include: preventing that trafficking in human beings happens; addressing the culture of impunity via national and transnational efforts to increase investigations, prosecution and convictions of traffickers; victims of trafficking in human beings should be treated as rights holders to effectively exercise their rights when it comes to their assistance, support and protection. For this their early identification is important.

**Migrant smuggling**

- Ensure adequate multidisciplinary counter-crime structures to deal with increasing polycriminal organised crime groups often posing a mafia style threat. This multidisciplinary nature should also go beyond solely law enforcement aspects to include cooperation with the private sector, third countries and be carried forward along the whole penal chain.
- Assign the necessary resources at national level (e.g. specialised units) in order to enhance smooth cross-border cooperation with counterparts in other Union Member States
- Enhance cooperation with the private sector in the prevention and follow-up to cross-border crimes e.g. financial sector, social media outlet, courier service providers, information sharing with haulage sector / carriers, etc.
- This should also be reflected in the provision of resources to ensure timely data collection on criminal justice statistics collected by Eurostat (e.g. migrant smuggling) – includes crosscutting collection from various authorities such as police, prosecution, courts, prisons.
- Increase national capacities to detect document fraud (in particular at the air border).
- Vulnerabilities identified in the two latest cycles of vulnerability assessments carried out by the EBCGA require a focus on ensuring availability of sufficient number of appropriately trained staff (document experts), appropriate technical equipment to detect sophisticated document fraud and forensic expertise.
- Training activities in the area of migrant smuggling at national level for law enforcement and judiciary (including related to documentary fraud, financial and online investigations and cooperation with third countries). Through the CEPOL Strategic Training Needs Analysis, Member States identified training related to the Facilitation of Illegal Immigration as the highest priority out of 21 criminal areas. This combined with the more specific Training Needs Analysis focusing specifically on cross-border cooperation to address migrant smuggling, pointed to the following training priorities at national level focusing on law enforcement and judicial officials to:
    - Enhance English foreign language skills to allow cross-border cooperation, which is to be supplemented at European level by specific professional terminology training activities
    - Knowledge of opportunities working with non-EU countries
    - Awareness of the role of social media in migrant smuggling and the relevant procedures (take-down request of pages, or their preservation for investigative purposes).

**Security Research**

- Developing innovative methods or deploying new technologies in close cooperation with the European Network of Law Enforcement Technology Services (ENLETS): testing, validating and exploiting the outcome of Union funded security research projects in developing and procuring state of the art tools and instruments for LEAs

**Suggestions for desired outcomes**

- More training programmes organised for LE officials on cross-border related topics. Providing or short, medium and long-term solutions for the challenges posed in the investigation of cybercrime. Encouraging initiatives to prevent radicalisation.
- Ireland transposed the Directive 2008/114 on European Critical Infrastructures but did not identify or register any ECIs. Furthermore, Ireland has not participated regularly in the meetings of Critical Infrastructure Protection Points of Contact (CIP POC); regular participation would be welcomed. An improvement of reporting on CIP prescribed by the Directive 2008/114 would also be useful.
- In Critical Infrastructure Protection (CIP) also develop a strong capacity to conduct risk assessments and engage with private operators, especially in order to provide security advice
- Address, if applicable, as a result of the European Semester, those country-specific recommendations (CSRs) which concern key security policy priorities, in particular the fight against corruption and money laundering.
- Improved capabilities to fight cybercrime, e.g. through training, the development or adaptation of tools, collaboration (between LEAs and with other stakeholders), and the use of capabilities available at Europol (which might require training and technical connections).

**Other comments**

**External dimension**
Cooperation with third countries on anti-terrorism and anti-radicalisation activities, cooperation between law enforcement authorities in the fight against terrorism, drugs and criminality as well as operational cooperation to tackle trafficking in human beings and migrant smuggling. Where needed implementation could be envisaged via several channels e.g. ad hoc projects/programmes, liaison officers, special investigation teams.

**Synergies with other Funds**

| **Asylum and Migration Fund** |
|---|
| There could be complementarities between ISF and AMF on legal migration regarding actions related to the fight against trafficking in human beings and migrant smuggling, protection of victims of trafficking in human beings and prevention of and countering radicalisation.<br><br>Financing of EURODAC/security part. |
| **Border Management and Visa Instrument** |
| No participation of Ireland in BMVI. |
| **Cohesion Funds (ESF+, ERDF, etc.)** |
| **European Social Fund+: actions to counter radicalisation, victim protection, drugs**<br><br>In the Multiannual Financial Framework 2014-2020, drug policy issues were addressed mainly by the anti-drugs chapter of the Justice Programme (mainly on what concerns drug demand/public health) and by the Internal Security Fund – Police (mainly on what concerns drug supply/law enforcement and security), in line with the two pillars of drugs policy: security and public health. It was decided that the successor of the |

current Justice programme will not address any drug policy topics. The future Internal Security Fund 2021-2027 will address mainly security aspects of drugs policy; however, the public health aspects of drugs policy are envisaged to be addressed by the successor of the current Health Programme – the European Social Fund Plus (ESF+), including on health services to patients in the area of drugs, harm reduction and prevention of drugs related deaths and research on the epidemiology aspects of the use and abuse of drugs. These measures focused on public health challenges related to illicit drug should be covered not only by the health strand of the ESF+, but also by the shared management/national programmes co-funded by ESF+. ESF+ may also support actions aimed at addressing radicalisation through fostering active inclusion and promoting equal access to and completion of quality and inclusive education and training for disadvantaged groups and through improving access to employment of, in particular, long-term unemployed and inactive people. Victims of crime could benefit from measures aiming to improve access to long-term care. In view of addressing root causes of radicalisation, the ESF may also support actions of social innovation and social experimentations designing and implementing community-led local development strategies.

**European Regional Development Fund: protection/design of public spaces, cybersecurity, actions to counter radicalisation, Critical Infrastructure**

ERDF could finance actions related to the protection of public spaces. ISF can finance small-scale projects, such as the innovative integration of security into the design of new buildings/public space and the purchase of closed circuit television systems, concrete bollards and other preventive equipment, such as cyber-attack resilient information and communications security systems. However, the ERDF is better placed for making such investments at regional and local level and contributing to infrastructure investments where security is a key element in the design of the public space.

ERDF will also address cybersecurity concerns when promoting digitalisation of SMEs, large enterprises and promoting government ICT solutions and IT services (cyber threats and cybercrime) under ERDF specific objective Reaping the benefits of digitisation for citizens, companies and governments (PO1). Cyber threats are increasing. They can disrupt the supply of essential services (critical infrastructure) such as water, healthcare, electricity, mobile services or generate substantial financial losses, undermine user confidence and cause major damage to the economy. Cybercrime is one of the fastest growing forms of crime and the risks are increasing exponentially. Unless we substantially improve cybersecurity, the risk will increase in line with digital transformation.

ERDF can also address protection of critical infrastructure (e.g. transport infrastructure, power plants, data centres, security and safety at airport and of air traffic management systems etc.) under i.a. specific objective Developing smart energy systems (PO2) or specific objective Developing a sustainable, climate resilient, intelligent, secure and intermodal TEN-T (PO3). Under PO 5 ERDF can also address security in the urban and other areas through the following specific objectives Fostering the integrated social, economic and environmental development, cultural heritage and security in urban areas and Fostering the integrated social, economic and environmental local development, cultural heritage and security, including for rural and coastal areas, etc. It can cover e.g. prevention of radicalisation under social integration measures and protection of public spaces.

**External Instruments (NDICI and IPA)**

The external actions will continue to be implemented in complementarity to the NDICI and IPA that are and will remain the primary tools to support the external dimension of the Union's migration and security policy. Member States through their national programmes are more adequate to promote and deliver on cooperation initiatives that complement and reinforce actions taken at the EU level. For example, when Member States have good bilateral relations with third countries, specific interests and expertise or networks in a given third country, or when the nature of a specific policy has a direct impact on the MS and might require bilateral cooperation.

**Neighbourhood, Development and International Cooperation Instrument (NDICI): fighting THB and migrant smuggling, support to regional and international initiatives contributing to security, preventing and countering radicalisation**

NDICI can support actions in third countries to address the root causes of irregular migration and forced displacement and to supporting migration management and governance. The ISF on the other hand will provide for an external dimension that will essentially represent an extension of the EU's security policies. It will focus on actions that serve primarily the EU's security related priorities.

NDICI will allow for making best use of geographic programmes, supplemented by the Global Challenges thematic programme and the rapid reaction response pillar. Additional financing may also be mobilised in case of need from the unallocated funds of the emerging challenges and priorities cushion, which identifies migratory pressure as one of the key grounds for its mobilisation. The measures supported aim at addressing all aspects of migration and forced displacement. This includes for instance addressing root causes of irregular migration and forced displacement, fighting trafficking in human beings and smuggling of migrants, supporting sustainable reintegration of returning migrants, promoting conditions for facilitating legal migration, stepping up cooperation on integrated border management, ensuring protection and development-based solutions for forcibly displaced persons and their host communities, supporting regional and international initiatives contributing to security, stability and peace and preventing and countering radicalisation leading to violent extremism and terrorism.

The Internal Security Fund will continue supporting cooperation with third countries on anti-terrorism and anti-radicalisation activities, cooperation of law enforcement authorities in the fight against terrorism as well as serious and organised crime, trafficking in human beings and migrant smuggling, including through joint investigation teams.

**Instrument for Pre-Accession Assistance (IPA): fight against organised crime/corruption/ THB and migrant smuggling, strengthening law enforcement**

The Instrument for Pre-Accession Assistance will support enlargement countries in preventing and tackling organised crime and corruption and in strengthening their law enforcement and migration management capabilities, including border management. It will support cooperation on migration, including border management, ensuring access to international protection, sharing relevant information, strengthening the development benefits of migration, facilitating legal and labour migration, enhancing border control and pursuing our effort in the fight against irregular migration, trafficking in human beings and migrant smuggling.

**Other Funds**

**Digital Europe: cybersecurity**

The Digital Europe Programme is about digital transformation of public services and businesses. Amongst several other issues it will address cybersecurity, as it is of key importance to ensure trust in digital products and services, especially given the wide spread of cyber-attacks. ISF will deal with cyber-dependent crimes, i.e. crimes that can be committed only through the use of information and communications technology devices and systems, and cyber-enabled crimes, i.e. traditional crimes, such as child sexual exploitation, which can be increased in scale or reach by the use of computers, computer networks or other forms of information and communications technology.

**Horizon Europe: security related research projects leading to innovative technologies**

There are complementarities between ISF and the Horizon Europe Programme. Actions related to the testing, validating, exploiting and deploying the outcomes, including innovative new technologies, developing from security research projects funded under the cluster "Civil Security for Society" of Horizon Europe, can be supported by ISF.

**Customs Control Equipment Instrument: customs control equipment to be used also for police cooperation and fight against serious and cross border crime**

Multi-purpose equipment, e.g. container scanner purchase, also other equipment could fall into the grey zone. Need to coordinate with TAXUD on gap assessment / needs.

**EU civil protection mechanism:** Exploit synergies regarding disaster risk management, prevention and preparedness.

**EU Defence Fund:** Multi-purpose equipment (e.g. UAVs)

**SRSP:** potential overlap/synergies in several areas such as radicalisation, money laundering, financial crime, OSINT to counter terrorism, disaster management, cybercrime, anti-corruption, etc.