



EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR MIGRATION AND HOME AFFAIRS

Directorate E – HOME Affairs Funds
The Director

Brussels
HOME.E.3/AF

NOTE FOR THE ATTENTION OF THE MEMBERS OF THE COMMITTEE FOR THE HOME AFFAIRS FUNDS

Ref.: HOME-Funds/2023/53

Subject: Launch of the call for expression of interest for the “Specific Action Cybercrime - non-cash-payment fraud NCPF” under the Internal Security Fund (ISF) – Reference ISF/2024/SA/2.2.1

1. INTRODUCTION

Regulation (EU) 2021/1149 of the European Parliament and of the Council of 7 July 2021 establishing the Internal Security Fund provides that Member States may receive funding for specific actions in addition to their initial allocations in their respective programmes.

Specific actions aim to fund transnational or national projects that bring Union added value in accordance with the objectives of the Fund for which one, several or all Member States may receive an additional allocation to their programmes.

They will be implemented as one of the components of the Thematic Facility in line with Art. 8 of the above-mentioned Regulation and in accordance with the relevant financing decisions and work programmes for the Fund¹.

By the present note, the Commission launches a call for expression of interest for Specific Action “Cybercrime - non-cash-payment fraud NCPF”, in line with the actions listed in the above-mentioned Commission’s financing decision and work programme.

¹ [Internal Security Fund \(2021-2027\) \(europa.eu\)](https://eur-lex.europa.eu/eli/reg/2021/1149/oj)

2. GENERAL PRINCIPLES

Specific actions will be implemented by one or more Member States participating in the Internal Security Fund via funding received in addition to the allocation under their ISF programmes.

Funding for specific actions is added to the Member States' programme allocations by means of a programme amendment. That additional funding is earmarked for the specific action concerned and shall not be used for other actions in the Member State's programme, except in duly justified circumstances and as approved by the Commission through the amendment of the programme.

Whereas the regular EU co-financing rate under the Member States' programmes will not exceed 75% of total eligible expenditure, projects implemented under specific actions may benefit from an increased co-financing rate of up to 90% of total eligible expenditure.

The specific action must be implemented by the Member States in accordance with the ISF² Regulation and the Common Provisions Regulation (EU) 2021/1060 (CPR)³. This includes compliance with fundamental rights.

Your attention is drawn to one provision of the CPR. As regard the value added tax ("VAT") eligibility regime, Article 64 (1)(c) of the CPR provides that VAT is not eligible, except:

- (i) "for operations the total cost of which is below EUR 5 000 000 (including VAT);
- (ii) for operations the total cost of which is at least EUR 5 000 000 (including VAT) where it is non-recoverable under national VAT legislation".

3. CALL FOR EXPRESSION OF INTEREST

3.1. Indicative Budget available

The 2023-2025 Thematic Facility work programme indicates that for all specific actions under ISF EUR 16,5 million are available.

The indicative amount envisaged for this call ISF/2024/SA/2.2.1 is EUR 3,5 million.

The requested amount (i.e., the EU contribution to the Member State's ISF programme under the Specific Action):

- should ideally not be lower than EUR 300.000,00 per application,
- should ideally not be higher than EUR 1.000.000,00 per application.

² Regulation (EU) 2021/1149 of the European Parliament and of the Council of 7 July 2021 establishing the Internal Security Fund.

³ Regulation (EU) 2021/1060 of the European Parliament and of the Council of 24 June 2021 laying down common provisions on the European Regional Development Fund, the European Social Fund Plus, the Cohesion Fund, the Just Transition Fund and the European Maritime, Fisheries and Aquaculture Fund and financial rules for those and for the Asylum, Migration and Integration Fund, the Internal Security Fund and the Instrument for Financial Support for Border Management and Visa Policy.

Nonetheless, selection of a proposal requesting different amounts is feasible for very well justified instances.

Should a great number of applications be received and successful, the final amount to be allocated to a Member State's programme may be lowered.

The Commission encourages project proposals by groups of Member States in consideration of the potential transnational impact.

In case of a transnational project, the Commission recommends, for the sake of efficiency, the choice of Option 1 as presented in the Note HOME-Funds/2022/07(Ares(2022)1060102) of 14 February 2022 on *Transnational specific actions under the Asylum, Migration and Integration Fund (AMIF), the Instrument for Financial Support for Border Management and Visa Policy (BMVI), and the Internal Security Fund (ISF) – Arrangements between partners*.

Any proposal submitted by a single Member State still has to demonstrate its transnational impact by its transferability, as well as dissemination activities, trainings, or others.

3.2. Background for the specific action

In 2019, the European Parliament and Council adopted Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA (<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0713>).

Main features of the Directive

To make law enforcement action against fraud and counterfeiting of non-cash means of payment more effective, the Council and the European Parliament adopted Directive 2019/713 to update Framework Decision 2001/413/JHA, removing obstacles to operational cooperation and enhancing prevention and victims' assistance. The main novelties introduced by the Directive are:

1. An encompassing and robust definition of the payment instruments, which also includes non-corporeal payment instruments, as well as virtual currencies:

The inclusion of "record" in the definition of "payment instrument" is meant to extend the scope of the definition to data used for payments, therefore covering virtual payment instruments, which become tantamount to physical ones. The mention of "means of digital mediums of exchange" is meant to ensure that virtual currencies are included in the scope of the definition of "payment instrument".

2. Criminalising the possession, sale, procurement for use, import or distribution of stolen or counterfeited payment instruments, aside from using such instruments:

The Directive builds on the existing legal framework and covers all conducts that are currently criminalised. It also extends the scope of the offences in order to cover "preparatory acts":

- "Phishing" is covered by the Directive. In fact, phishing results in the "theft or unlawful appropriation of a payment instrument".

- "Carding" is covered by the Directive, which criminalises the sale, distribution or otherwise making available of a stolen or otherwise unlawfully appropriated payment instrument.

- "Pharming" is criminalised.

3. Setting a minimum level for maximum penalties across Member States

The Directive sets a maximum level of penalties.

Art 8(4) provides for a minimum maximum penalty of 5 years in presence of offences committed within the framework of a criminal organisation.

4. Strengthening the existing operational cooperation mechanisms

In order to shorten the delay for answering cross-border requests for information among law enforcement authorities, the Directive requires MS to (i) appoint an operational national point of contact and (ii) have procedures in place for urgent requests for assistance, to indicate, within eight hours of receipt, at least whether the request will be answered, and the form and estimated time of such an answer. In doing so, MS can make use of the existing network of operational points of contact available 24 hours a day and seven days a week.

5. Enhancing reporting of crime

In order to facilitate reporting of crime, the Directive requires Member States to take the necessary measures to ensure that appropriate reporting channels to the competent national authorities are available. In addition, the Directive requires MS to encourage reporting of crime.

6. Providing for victims to have access to information about their rights and about available assistance and support

The Directive sets out an obligation for Member States to ensure that support services addressing specific needs of victims are in place, in particular to the victims of identity theft. This provision covers both natural and legal persons, which are affected by the consequences of the offences.

The Directive requires Member States to take appropriate action, including through the Internet, such as information and awareness- raising campaigns, research and education programmes, where appropriate in cooperation with stakeholders, aimed at raising awareness and reducing the risk of becoming a victim of fraud.

Report assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive (EU) 2019/713

In July 2023, the European Commission issued the report (<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023DC0363>). It highlights that the Directive has led to substantive progress in criminalising fraud and counterfeiting of non-cash means of payment on a comparable level across the Member States, which facilitates the cross-border cooperation of law enforcement authorities investigating this type of offences. Member States have amended criminal codes and other relevant legislation, streamlined procedures, and set up or improved cooperation schemes. The Commission acknowledges the major efforts by the Member States to transpose the Directive.

However, the report points out that there is still scope for the Directive to reach its full potential if Member States were to fully implement all of its provisions. The analysis so far suggests that some of the main improvements to be achieved by the Member States include:

- offences related to the tools used for committing the offences,
- the provisions relating to ‘attempt’,
- exchange of information,
- assistance and support to victims.

3.3. Scope and purpose of the specific action

The objective of this specific action is to provide financial support to Member States in reaping the full benefits from the implementation of Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment, with a focus on the areas of:

- **international cooperation and exchange of information,**
- **assistance to victims,**
- **prevention**

This call targets in particular a Member State or a group of Member States that:

- wish to cooperate more effectively with other Member States in tackling non-cash payment fraud,
- do not have authorities/organisations offering specific assistance to victims of non-cash payment fraud,
- have not yet implemented dedicated actions aiming at preventing non-cash payment fraud.

The call for expression of interest is open for both national and transnational project proposals:

- In case of **a group of Member States**, the following issue(s) should be addressed: international cooperation and exchange of information, and/or assistance to victims, and/or prevention in the area of non-cash payment fraud
- In case of **a single Member State**, the following issue(s) should be addressed: need to reinforce assistance to victims and/or prevention of non-cash payment fraud.

In case of a transnational project proposal, the lead Member State will have to make sure that the ISF Managing Authority of each participating Member States duly signs the “Partnership Declaration Form”. In the Application form, each Member State should be listed and the share that it will receive from the additional amount allocated, if the project proposal is successful, should be indicated. Based on this common agreement, each partner will have a role and resulting responsibilities in the implementation of the project and delivering on its objectives⁴.

This specific action falls specifically under points (c), (i) and (j) of Annex III of the ISF Regulation, regarding support to:

- (c) “EU policy cycle/EMPACT operational actions;
- (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, (...);
- (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”.

⁴ Please refer to the note HOME-Funds/2022/07 on the arrangements between partners to be sought when submitting proposals for transnational specific actions.

The specific action proposed may include, for instance, activities related to:

- reinforcing police and/or judicial cooperation among EU Member States for example through complementing EMPACT actions,
- reinforcing authorities and services aimed at assisting victims of non-cash payment fraud,
- preventing non-cash payment fraud for example through the establishment of public-private partnerships with financial institutions or other relevant entities.

Under this specific action the purchase of equipment, means of transport and security-related buildings is not eligible.

The specific action focuses on cybercrime and does not cover projects related to cybersecurity.

The Commission encourages Member States to submit project proposals with innovative approaches to non-cash payment fraud.

3.4. Expected results following the call

Member States can propose both projects implemented entirely at national level and projects implemented transnationally by a group of Member States. In the latter case, the proposing Member States should explain the specific added value of their transnational approach.

As outcome of the present call for expression of interest, three to ten projects are expected to be selected, targeting the three issues listed under Section 3.3 (international cooperation and exchange of information, assistance to victims, prevention).

Examples of actions:

- cross-border operational actions (possibly to support the EMPACT criminal topic of Online Fraud Schemes tackled through Operational Action Plans OAPs),
- mechanisms to exchange information across borders,
- reinforcing the capacity of the Points of Contact appointed under Directive 2019/713,
- mechanisms for victims to report non-cash payment fraud to law enforcement authorities,
- schemes to assist victims,
- awareness raising campaigns,
- cooperation with Service Providers/financial institutions/merchants to prevent fraud,
- increased public-private partnerships to prevent/investigate fraud or assist victims.

As a result, selected projects will:

- further enhance the capacity of law enforcement authorities to investigate and prosecute perpetrators, thus tackling the three aspects of prevention – prosecution – assistance to victims, which are complementary to each other,
- reduce the impact of non-cash payment fraud on victims,
- contribute to reducing the gains of organised crime groups responsible for fraud and increasing the risks for them to carry out this criminal activity.

The European Union will benefit from these projects, as citizens will feel better protected and their trust in the digital single market will not be impaired by the fear of fraud. Moreover, the projects will reduce the gains stemming from non-cash payment fraud for organised crime groups, thus enhancing the Internal Security of the EU.

4. PROCEDURE FOR APPLICATION

4.1. Admissibility and assessment aspects

All EU Member States participating in the ISF are eligible.

The Specific Action proposed should not start before 1 January 2024 and should ideally be completed by 31 December 2026 at the latest.

DG HOME will assess the proposals submitted by the Member States.

To be considered admissible a proposal must:

1. be submitted within the deadline (see below) to the ISF specific actions functional mailbox HOME-ISF-SPECIFIC-ACTIONS@ec.europa.eu
2. consist of the official ISF/2024/SA/2.2.1 Application form attached to this note together with its annexes, which must be readable and complete (all fields necessary for assessment are filled in),
3. be submitted by the Managing Authority on behalf of the entity in the Member State that will be responsible for the implementation of the specific action,
4. identify a project beneficiary (an entity) that will be responsible for the implementation of the specific action in the Member State (in the lead for the action),
5. in case of a transnational project: include partnership declaration forms signed by the Managing Authorities of all participating Member States⁵.

DG HOME will assess admissible proposals based on the following criteria⁶:

A. Relevance (20 points – minimum score 10 points):

1. **Clarity and consistency** of the objectives and scope of the project proposal against the objectives and expected results identified in this call.

B. Quality and content (50 points – minimum score 25 points):

1. **Maturity of the proposal; appropriateness of the design** and planned implementation, considering the envisaged activities; methodology (including operational and financial management); **organisation of work and strategy for project management and monitoring**, evaluation; **innovative aspects**; measures undertaken or envisaged to mitigate the identified risks.
2. **Cost-effectiveness and complementarity with other EU funding sources**: the Member State(s) should present the amount of financial support requested and its appropriateness in relation to the scale and type of activities (personnel, travel, etc.) and the (long-term) expected results, as well as the

⁵ Please refer to the note HOME-Funds/2022/07 on the arrangements between partners to be sought when submitting proposals for transnational specific actions.

⁶ Only proposals scoring at least the 'pass scores' defined for each category (A, B and C) of the assessment criteria can be proposed for funding, depending on their overall ranking and budget availability. Proposals not meeting the 'pass score' of criterion A (10 points) will not be further assessed.

overall cost-effectiveness and value for money. The Member State(s) should also explain the complementarity with other EU funding sources (Member States' ISF programmes, ISF calls for proposals under Union Actions, Europol EMPACT grants, etc.).

3. **Level of involvement of and cooperation with relevant EU entities** (Institutions, Bodies and Agencies – e. g. Europol and CEPOL) whenever appropriate, and explanations on how this will be achieved. **Links to the EMPACT criminal topic Online Fraud Scheme** should be demonstrated, if appropriate.

C. Impact (30 points – minimum score 15 points):

1. **Impact or effect for the EU** of the project in relation to the objective of the call for expression of interest (**Union added value**).
2. The Member State(s) should demonstrate that extra funding available under the programme financed from the ISF may effectively **contribute to achieving the priorities and expected outcomes of this Call, notably regarding the output and results indicators** listed in Annex VIII of the ISF regulation (see Annex 4).
3. **Level of involvement of competent authorities from EU Member States:** law enforcement authorities, private and public entities (e.g. financial institutions, merchants, relevant internet service providers, etc.) involved in tackling non-cash payment fraud, organisations involved in assistance of victims, etc.
4. **Level of transnationality** of the project proposal:
 - proposals submitted by groups of Member States are encouraged,
 - proposals submitted by a single Member State should demonstrate **transnational impact** (e.g. dissemination activities, trainings, **transferability** of the project results, etc.).
5. **Efforts to disseminate and communicate** the results of the project.
6. **Sustainability** of the project: continuation of the project after the implementation period is over (e.g. inclusion of the created procedures/networks into the institutional setting; involvement of the trained staff in related areas of activity; sustainable public-private partnerships; feeding project deliverables into the work of existing EU agencies (Europol, CEPOL) or relevant existing organisations (e.g. European Cybercrime Training and Education Group ECTEG), etc.).

Member State(s) must ensure respect for the horizontal principles described in Article 9 of Regulation (EU) 2021/1060, including respect for fundamental rights and compliance with the Charter of Fundamental Rights of the European Union.

Member States must also ensure that the envisaged actions are not affected by a reasoned opinion delivered by the Commission in respect of infringement proceedings under Article 258 of the Treaty on the Functioning of the European Union (TFEU) that put in doubt the legality and regularity of expenditure or the performance of the actions (Article 8(5) of Regulation (EU) 2021/1149).

4.2. Application procedure

Deadline for the application: Member States are invited to submit their proposals by 26 April 2024 at the latest, using the official ISF/2024/SA/2.2.1 Application form attached to this Note, together with its annexes. The applicant may submit an application in any

official EU language (project abstract/summary should however always be in English). For reasons of efficiency, it is strongly advised to use English for the entire application package.

To ensure equal and fair treatment of the proposals and allow the Commission to allocate at the same date all the available funding, DG HOME will assess all proposals simultaneously. Therefore, proposals submitted after the deadline will not be admissible.

The Members of the Committee for the Home Affairs Funds will be informed at the latest 10 working days before the deadline for the submission of the proposals in case the deadline for the submission of proposals is extended.

E-mail address for the application: The proposals should be submitted to the ISF specific actions functional mailbox HOME-ISF-SPECIFIC-ACTIONS@ec.europa.eu. Member States may submit additional documentation, if necessary.

No modification to the application is allowed once the deadline for submission has elapsed. However, if there is a need to clarify certain aspects or to correct clerical mistakes, the Commission may contact the applicant/ lead Member State during the assessment process. A reply should be provided by the Member State within 3 working days from the request date.

Any requests for clarification from Member States on this call for expression of interest may be sent by 10 April 2024 at the latest, to the same ISF specific actions functional mailbox HOME-ISF-SPECIFIC-ACTIONS@ec.europa.eu.

Requests for clarifications should be sent only **by the Managing Authority**. The Managing Authority has an important role to play in explaining to potential beneficiaries the applicable rules and specificities of the ISF programme and the Specific Actions scheme, as well as helping them to prepare their applications. The Managing Authority should be their sole contact point and has the responsibility to review and reply to any questions received from applicants. It may, however, address these questions to the Commission services if further clarification is needed. As projects under specific actions are managed at national level, according to national rules, specific questions on eligibility of costs should be addressed first to the Managing Authority.

To respect the equal treatment and transparency, the replies to the written requests for clarification received will be sent to all Member States, via HOME-AFFAIRS-FUNDS-COMMITTEE@ec.europa.eu

DG HOME will inform Member States of the outcome of the assessment of the proposals towards July 2024.

5. AMENDMENT OF THE ISF PROGRAMMES AND ELIGIBILITY OF EXPENDITURE

After having been informed of the outcome of the call for expression of interest, each successful Member State shall submit to the Commission a request to amend its ISF programme via SFC. The amended programme should include a short description of the specific action, adjust the output and result indicators, and include the costs and codes linked to this specific action (respectively in the description and under tables 1, 2 and 3 of the Specific Objective 2, as well as table 6 and appendix 3 of the programme).

When amending an ISF programme of a Member State, two situations may arise regarding the eligibility of expenditure⁷:

1. For Member States that have included all the types of interventions listed in Annex VI table 2 of the ISF Regulation that are relevant for the Specific Action “Cybercrime - non-cash-payment fraud NCPF” in table(s) 2.1.3 of Specific Objective 2 in their *initially approved* ISF programme: expenditure for the specific action will be eligible as of 1st January 2024.
2. For Member States that have *not* included all the types of interventions listed in Annex VI table 2 of the ISF Regulation that are relevant for the Specific Action “Cybercrime - non-cash-payment fraud NCPF” in the tables in the table(s) 2.1.3 of the Specific Objective 2 in their *initially approved* ISF programme: expenditure for the specific action will be eligible from the date of submission by the Member State of its request for amendment of the ISF programme that will add the respective types of interventions in the programme.

Yours faithfully,

Silvia MICHELINI

⁷ Art. 63(7) of Regulation (EU) 2021/1060.