Council of the European Union

Brussels, 21 February 2022
(OR. fr)

6246/22

LIMITE

CT 27
ENFOPOL 69
COTER 39
JAI 188
SIRIS 23
FRONT 67
IXIM 32
COSI 47
COMIX 76

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	5009/22
Subject:	Improving the post-hit procedure in the Schengen Information System (SIS) for alerts related to terrorism : answers to questions and next steps

Courtesy translation

At the TWP meeting on 12 January 2022, the Presidency proposed to improve the exchange of information between Member States on particular hits related to terrorist alerts in the Schengen Information System (SIS) and provided for this purpose an explanatory document. Following the comments made by the Member States at the meeting and received in writing, the Presidency wishes to provide additional information on this project.

Principles

- What is the current procedure when a Member State checks an individual listed for a terrorism-related motive in the SIS on its territory?

At present, when a Member State checks an individual for whom an alert has been issued in the SIS for a terrorist motive on its territory, it forwards the information to the Member State that registered the individual. The "issuing" State must then send this "hit" to Europol, in accordance with Article 48 of the SIS[1] Regulation. If, for example, a **foreign terrorist fighter (FTF) registered in the SIS** (Article 36) is checked, **only two Member States and Europol are informed of its presence on the European territory**, even though this individual represents a threat to all countries because of the absence of internal border controls within the Schengen area.

- What would be the changes induced by the Presidency's proposal on the post-hit procedure?

The revision of the post-hit procedure as proposed by the Presidency would allow **Member States, having previously volunteered, to receive alerts on** certain terrorist profiles (Islamist terrorists released from prison and linked to Syrian-Iraqi networks, Europeans who have left for the conflict zone, foreign terrorist fighters) registered in the SIS by other Member States. **Sending the relevant hits** to all voluntary Member States would be **mandatory and systematic for all Member States issuing alerts**.

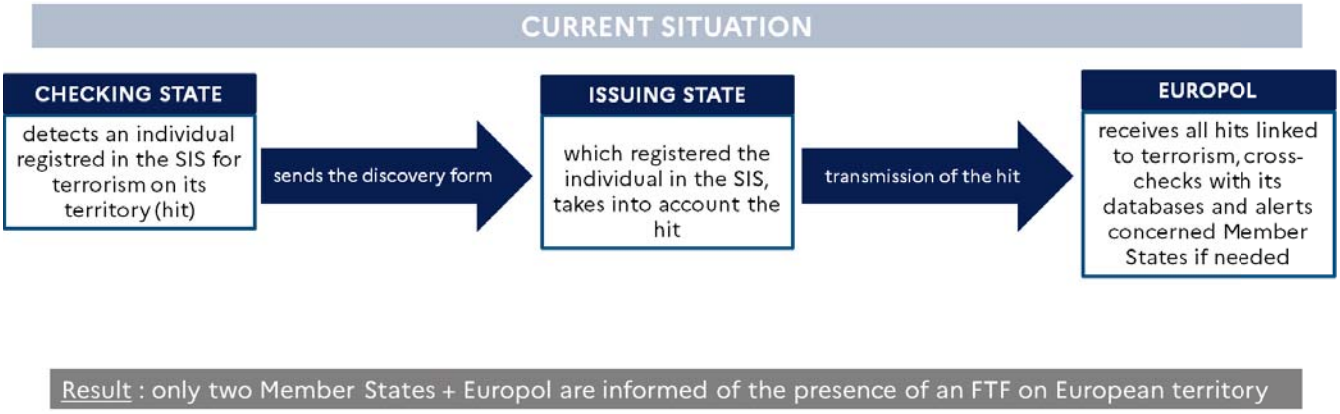
In this way, the "checking" Member States would **not have to take any additional action** compared to the current situation. The geographical position of the checking Member States would therefore not influence the additional workload of their SIRENE bureaux induced by the proposal. For example, a Member State which constitutes one of the **external borders of the European Union** and which checks more individuals due to migration flows, **would continue to send the discovery forms to the issuing States as it does now**.

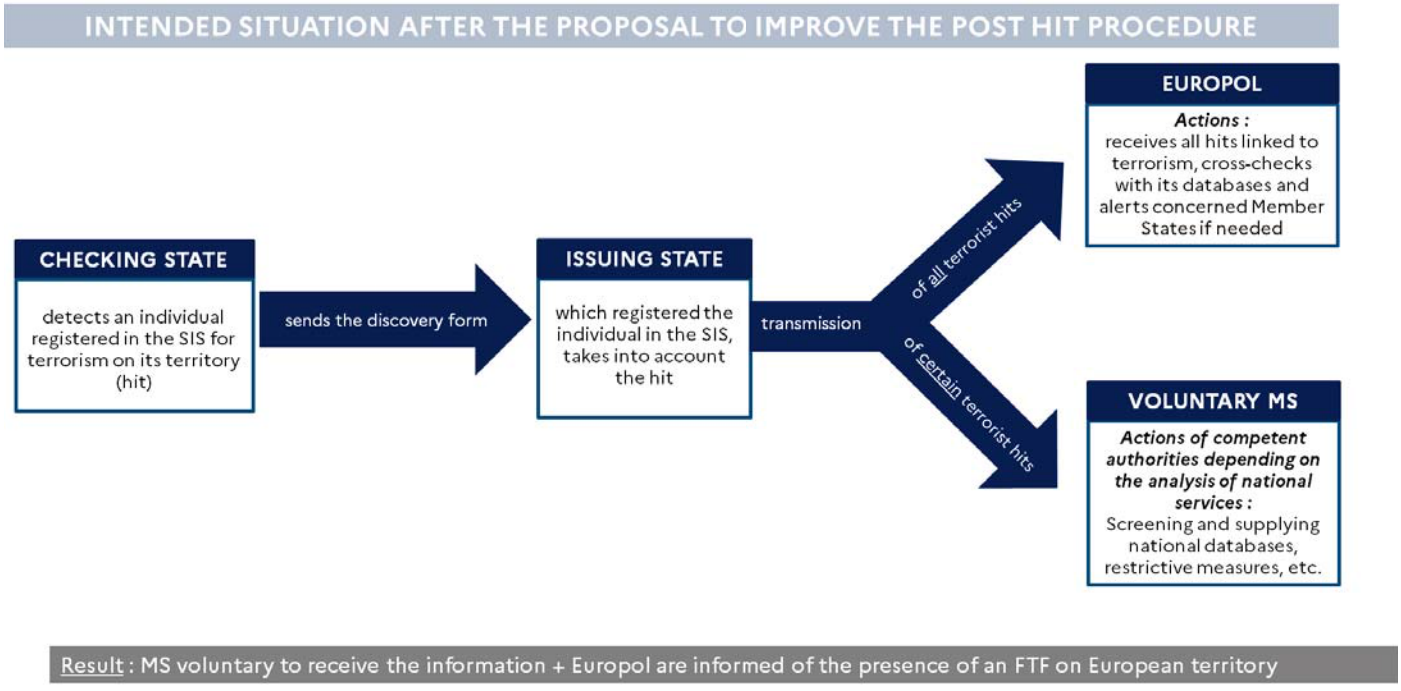
---

1 Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU.

With the proposed improved post-hit procedure, both Member States (the "issuing" State and the "checking" State) and Europol would **remain informed of the hit** triggered by the detection of the individual on European territory. However, **all other willing Member States would also receive this information**, thus promoting better communication between Member States.

Hence, the reform of the post-hit procedure could take the following form:





An important operational interest

- What is the added value for voluntary Member States in receiving the hits?

While the SIS Regulation **currently obliges Member States to transmit to Europol all hits related to terrorist offences**, except in special cases, it would be **legitimate for all other willing Member States to have access to this information** when it concerns certain dangerous profiles. The transmission of information between Member States would thus be enhanced in order to face the challenges posed by the absence of internal border controls within the Schengen area in a context of high terrorist threat.

This data could enable voluntary Member States to **issue restrictive or surveillance measures** where appropriate, **based on their own analysis** of the threat posed by these individuals. This data may also be used by the competent authorities of the Member States in **future investigations**.

- Why not limit ourselves to the analysis carried out by Europol?

Europol's analysis of terrorist hits sent by Member States, based on its information systems, is an undeniable and important step forward in the exchange and cross-checking of information at European level.

However, **Member States' counter-terrorism services use their own specific databases, which are broader in scope** than the information exchanged with the Law Enforcement Agency. It seems therefore essential that the competent authorities of the Member States should also be able to compare the data from the hits with their national databases, in order to ensure that the threats posed by these individuals are assessed and dealt with.

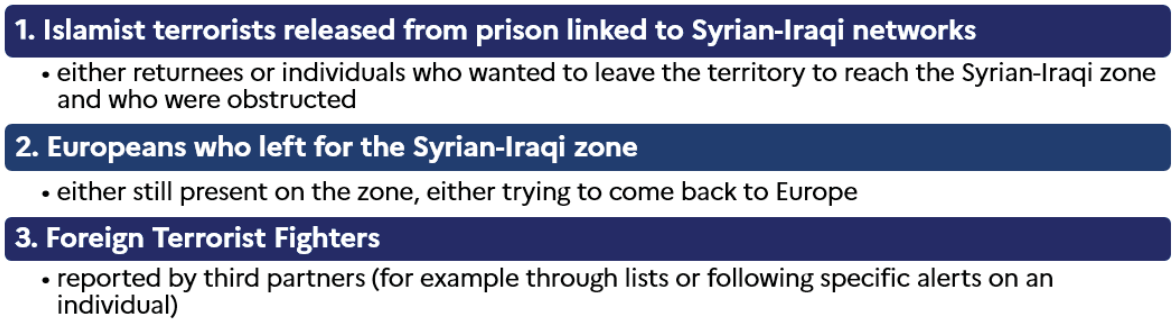
The current logic of disseminating analysis on hits only through Europol, although essential, does not currently allow to cover all Member States that could in fact be concerned by this information.

The proposal to improve the procedure is not intended to replace the existing mechanism with Europol, but to **complement it**, in order to ensure that the information has been cross-referenced more widely with national databases. Thus, both procedures would strengthen the European security architecture while reducing the blind spots related to the early detection of dangerous individuals on European soil.

Precise profiles and information targeted

- What kind of profiles are concerned by this proposal?

This proposal only concerns **certain types of terrorist profiles**, who have had **direct links with jihad zones, particularly in the Syrian-Iraqi region**, and who are considered the most dangerous. More specifically, it could apply to three types of individuals:



The number of individuals matching these profiles is small compared to all terrorist alerts in the SIS or to all alerts on all grounds in the SIS. Thus, the vast majority of alerts on terrorism would not be affected by the reform. For example, individuals monitored for home-grown[2] threats who have no specific European or international contacts with terrorist organisations, although they are registered in the SIS, are not intended to be covered by this mechanism.

- How can these individuals be singled out in the SIS?

At present, there is no way to single out these three types of profiles in the SIS: there is only a difference between individuals registered in connection with terrorism and those who are not. The implementation of this proposal would thus imply **a technical distinction between the different types of alerts concerned**. Several ways of doing this could be envisaged, such as:

- the creation of **sub-categories**, as in the diagram above*: "(1) prison leavers linked to terrorist networks, (2) Europeans who have left for the conflict zone (3) FTFs".*

- the creation of **a single sub-category of** "*terrorism linked to a terrorist network or terrorist fighter"*

[2] The home-grown threat comes from individuals who have been resident on national territory for a long period of time and who have not joined a jihad zone prior to their involvement.

This last approach has the advantage that it can evolve over time and thus adapt to **changes of the terrorist threat** (possible creation of new networks, new theatres of conflict, etc.)

How this distinction could be made in practice would be the **subject of discussions between Member States**, which could be held in IXIM to assess the technical possibilities and the implementation of the envisaged development.

Nevertheless, **technical considerations will be issues to be addressed at a later stage**, the objective of the Presidency being to agree on the findings and on the launch of an improvement of the post-hit procedure.

- What information is sent to voluntary Member States? Is there an exception to sending hits to voluntary Member States?

The issuing Member State would send to the voluntary Member States the **same information already sent by Member States to Europol,** i.e. information related to hits (hit information and discovery form).

If the Member State issuing the alert considers that the data should not be transmitted to Europol (under the exception provided for in Article 48 of the SIS Regulation), **it may also decide not to transmit the data to the voluntary Member States.**

If, after receiving information from a hit, a voluntary Member State wishes to obtain further details on the reasons for the individual's registration in the SIS or information on his or her check, **it may contact the issuing or checking Member State through the appropriate existing cooperation channels**.

Voluntary action by Member States

- What is the difference between a voluntary State and a non-voluntary State?

A Member State, whether voluntary or not, would be obliged to transmit the terrorist hits of the targeted profiles to the voluntary Member States. It would send the same data that it already sends to Europol. However, only a voluntary Member State would receive the hits mentioned above.

- How can a Member State express interest in volunteering?

While **no procedure is currently favoured by the Presidency**, it could be envisaged that Member States wishing to volunteer could do so **within the TWP.**

For example, the Presidency could draw up **a list of volunteer Member States each year for a one year period.** This would allow Member States to be added to the scheme over time, or to withdraw from the procedure if they wish so.

This is a proposal that may be subject to **exchanges of views between Member States.**

Legal effects

- Will legal changes be needed to implement the reform?

Today, **there is no legal basis for the transmission of hits between all Member States**. Therefore, legal changes are **necessary.** Before launching an in-depth legal assessment on how to modify the texts in force, the Presidency would first like to **consolidate a common understanding and consult all Member States on the operational interest of such a measure**.

Subject to further analysis in IXIM and in cooperation with the Commission, it will be necessary to determine whether a modification of the SIRENE Manual is sufficient to incorporate the technical changes or whether a legislative amendment of the SIS Regulation is necessary.

- Is there a legal problem with the ownership of the information?

The issuing State, **which owns the information of the registration** of an individual in the SIS, transmits the hit information to all the other voluntary Member States. Thus, there are **no legal problems relating to the ownership of the information**. In any case, these data are already transmitted to Europol, without this creating any legal difficulties.

A low impact on SIRENE bureaux

- What will be the additional workload for the SIRENE bureaux? For the competent services?

A quantified estimation was transmitted on 5 January 2022 by the Presidency in document 5009/22. This estimation is based on French data, which accounts for 66% of the registration of individuals in the SIS under Article 36. Other estimations may be made in the course of future work between Member States.

a) Sending hits to volunteer Member States

The revision of the post-hit procedure should not create significant additional work for the SIRENE Bureaux, which **already have to transmit all hits on terrorist offences to Europol**. Thus, a transmission process identical to the one currently in place in this case could be envisaged, depending on the internal organisation of the national SIRENE bureaux. In concrete terms, this could mean **adding additional recipients** when sending hits to Europol, which would correspond to the Member States that volunteer to receive the hits. The aim is to create a **simple and time-saving process** based on what already exists in order to minimise the actions to be taken by the SIRENE Bureaux.

b) The reception of hits by voluntary Member States

The reception of hits by voluntary Member States **would not imply any particular additional mandatory action** than what is already foreseen in the classical case of reception of a hit. **The voluntary Member State will be solely responsible** for the way in which this information is processed at its level. It will designate the service responsible for handling the hit, which will then determine the actions it deems necessary to process the information (obstruction of the individual, surveillance, data collection, etc.).

Next steps

The Presidency proposes the following next steps to delegations:

1) Continue the assessment of the operational need *(February and March 2022)*

The Member States are invited to **take into account the answers** given by the Presidency in this document and **to make any additional remarks.** The Presidency will try to answer the questions of the Member States at the TWP meeting on 28 February.

2) Develop Council conclusions *(March and April 2022)*

The Presidency recalls that its main objective is to **include the operational need and the lines of reflection linked to this proposal in Council conclusions**. A first version of these conclusions will be examined at the TWP meetings of March and April.

The **technical and legal details** mentioned in this document will be **studied at a later stage** after confirmation that the operational need is shared by Member States and will not be included in the draft conclusions.

3) Work on the concrete terms of the reform *(from the second half of 2022)*

The Member States, in cooperation with the Commission, will then have to consolidate **the technical and legal details of the revision** induced by this proposal, which will then be sent to IXIM in coordination with the TWP to assess their feasibility and concrete impact.

Delegations are invited to consider the next steps proposed by the Presidency before ***4 March 2022***.