Council of the European Union

Brussels, 7 March 2017
(OR. en)

6717/17

LIMITE

COSI 42
ASIM 18
ENFOPOL 90
SIRIS 39
DAPIX 65
CT 11
JAI 173
COMIX 177

NOTE

From:	Presidency
To:	JHA Counsellors / COSI Support Group Standing Committee on Operational Cooperation on Internal Security
Subject:	Security checks in case of irregular immigration - mapping exercise

Background

1. Following several terrorist attacks where the perpetrators were linked to irregular migratory movements, Member States should improve the detection of those who want to indiscriminately inflict harm to our communities and undermine our European values. While stressing that those opting for irregular movements are often eligible for international protection, Member States have a collective responsibility to protect our communities and those seeking protection themselves by deterring and preventing the entry of persons who are a threat to public security.

2. The Presidency submitted a discussion paper to the informal meeting of the Ministers of Justice and Home Affairs held on 26 January 2017 in Valletta, Malta, which was aimed at identifying both the challenges and opportunities to mitigate the risks emanating from the threat of having mala fide persons exploiting irregular movements, in particular with regard to IT systems which are an important tool to improve border management and security. At that meeting the Ministers expressed broad agreement to what was proposed in the discussion paper and the Standing Committee on the Operational Cooperation on Internal Security was tasked to further work on the proposals therein[1].

3. The purpose of the current paper is twofold: (i) to further detail the context in which security checks for persons having crossed the border illegally (hereinafter 'irregular migrants'[2]) are talking place, and (ii) to map the type of security checks Member States are currently undertaking regarding irregular migrants. The eventual aim is to identify good practices and to agree on a common standard as to which databases are consulted for security checks regarding irregular migrants that will be submitted to the Council in June 2017.

Legal framework for security checks

4. The procedures for the checks at external borders of the Union are regulated in a detailed manner in the Schengen Borders Code (SBC). The SBC lays down rules governing border control of persons crossing the external borders of the Member States of the Union. Article 8 of the Schengen Borders Code[3] provides that any cross-border movement at external borders shall be subject to checks by border guards. Such checks require, among others, a security check. Both regarding third country nationals (Article 8((3)(vi)) and regarding persons enjoying the right of free movement under Union law (Article 8(2)(b) SBC)), it requires a verification that the person concerned is not likely to jeopardise the public policy, internal security, public health or international relations of any of the Member States. Such verification shall include direct consultation of the SIS and other relevant Union databases, without prejudice to the consultation of national and Interpol databases.

---

1 The High Level Expert Group on Interoperability has also discussed issues related to irregular migrants, asylum seekers and security checks.

2 For the purpose of this note, the term 'irregular migrants' does not include those detected for illegal stay.

3 The amending Regulation as regards the intensification of checks against relevant databases at external borders is expected to enter into force by the end of March 2017.

5. The border checks are regularly conducted at border crossing points. However, the border guards are obliged to take measures against persons who have crossed the border illegally, also outside designated border crossings points. Article 13 SBC provides that, without prejudice to international protection, a person who has illegally crossed a border and who has no right to stay, shall be apprehended and be subject to the return Directive procedures. The Schengen Handbook provides that such persons shall be brought to the nearest border crossing point. There they are to be subjected to border checks in accordance with the Schengen Borders Code.

6. Under the conditions laid down in the SBC, Member States may also temporarily reintroduce border controls at internal borders, if there is a serious threat to their public policy or internal security. In such a case, they may conduct border checks, including security checks, provided for in the SBC. If security checks regarding persons who have crossed the border illegally are carried out on the basis of spot-checks within the territory of the Member States, and which do not have border control as an objective, these are not border checks but police checks performed under the national law (cf. Article 23 SBC).

7. Article 72 TFEU recalls the Member States' responsibilities for the maintenance of law and order and the safeguarding of internal security. Article 87 TFEU provides a legal basis allowing the Union to establish police cooperation involving all the Member States' competent authorities, including police, customs and other specialised law enforcement services in relation to the prevention, detection and investigation of criminal offences. As for the secondary law, Article 39(1) of the Convention implementing the Schengen Agreement of 14 June 1985 (CISA) provides that "the Contracting Parties undertake to ensure that their police authorities shall, in compliance with national law and within the scope of their powers, assist each other for the purposes of preventing and detecting criminal offences". Many Member States have in place various bilateral and multilateral arrangements concluded in accordance with those provisions.

Security checks in hotspots

8. The European response to the migration crisis included the so-called hotspot approach to managing exceptional migratory flows. The hotspots are designed to support Member States at the external borders of the EU, facing the disproportionate migratory pressures. Regulation 2016/1624 on the European Border and Coast Guard establishes the European integrated border management at external borders to tackle an existing or potential disproportionate migratory challenge characterised by a significant number of migrants arriving at external borders and defines the concept of "hotspot areas". The security checks taking place in these hotspots prove a good example of systematic approach regarding irregular migrants.

9. One of the Actions of the Roadmap to enhance information exchange and information management including interoperability solutions in the JHA area[4], namely Action 44, refers to the need of enhancing of the security checks in hotspots. Progress regarding this Action was reported to the Council on 18 November 2016[5]. Action 44, specifies that "access should be provided to the relevant databases SIS, EU VIS, Eurodac, Interpol databases and Europol databases, in particular to facilitate information exchange on security concerns in relocation cases including exchange of fingerprints before relocation".

10. The main means of running security checks upon the migrants' arrival is fingerprinting, which allows for checks against both national fingerprints criminal record databases and the SIS II (manually, pending the roll-out of the AFIS), VIS and Europol.

[4] 9368/1/16 REV 1
[5] 13554/1/16 REV 1

Security challenges in case of irregular border crossings

11. When faced with hundreds, if not thousands, of arrivals and/or rescues per day, Member State authorities are confronted with complex security challenges. Illegal border-crossings outside designated border-crossing points take place between authorised border crossing points and are often undocumented, which means that it is impossible to run a check against any security database unless biometrics are utilised. However, today, only the VIS and Eurodac are fully biometric databases. The AFIS of the SIS II is being developed, but not yet rolled out. The AFIS for Europol can be used by Europol staff only.

12. There is also a risk that returning, fleeing and/or transiting foreign terrorist fighters (FTFs) could mingle with irregular movements, and could moreover resort to document fraud, as they are likely to surmise that their names are on watch lists or because they want to travel undetected[6]. Other FTFs are known to have used their relatives' travel document/s or other third-party passports as impostors often because their own travel document/s have been either withheld by the issuing authorities or else by the organisations they were linked with. Only the systematic use of biometrics', especially fingerprints, can assist in identifying mala fide persons.

13. It is submitted that an area of freedom and security necessitates that 'security checks' are systematically carried out when migrants who have irregularly crossed a border are apprehended, including migrants who are seeking asylum or other forms of international protection. Extending 'security checks' to persons applying for asylum should not be taken with a negative connotation. Actually, it protects and secures bona fide asylum seekers from stigmatisation. Furthermore, such additional 'security checks' enhance territorial control, which forms part of the four-tiers access model – an integral notion within the Integrated Border Management concept.

14. Without any prejudice to Member States' national legislations and procedures, EU agencies could support the Member States' competent authorities in line with their respective mandates, as is currently happening in the hotspots.

---

6 See draft Council conclusions on the Action plan to strengthen the European response to travel document fraud

15. The 'hotspot approach' also demonstrates that effective security checks necessitate the systematic use of biometrics in order to deal with large flows and conduct ‘security checks’ as early as possible after arrival. Member States should ensure that such ‘security checks’ are uniformly replicated all along the external borders of the EU. The aim is to replicate the good practices that Member States could already have in place regarding the use of biometrics and to agree on a common standard as to which databases are consulted.

Mapping the current situation regarding Member State practices for consulting databases

16. Member States are invited to indicate:

1) based on existing good practices, which of the below databases should be consulted when crosschecking all irregular migrants;
2) whether such databases’ consultation already takes place in a systematic manner; and
3) whether irregular migrants are systematically fingerprinted (in addition to the requirements flowing from the Eurodac Regulation).

- **National databases**
  - National police databases, including fingerprint databases
  - Missing persons’ lists and other watch lists
  - Other relevant databases

- **European databases**
  - SIS II *(Schengen Information System)*
  - EIS *(Europol Information System)*
  - VIS
  - Eurodac

- **Interpol databases**[7]
  - Interpol's I-24/7 network *(Connects all Interpol's National Central Bureaus)*
    - AFIS[8] *(Automatic fingerprint identification system)*
    - SLTD *(Stolen and Lost Travel Document database)*
    - TDAWN *(Travel Documents Associated with Notices)*
    - NOTICES *(International alerts or requests for cooperation)*
    - FTF project *(currently 14,188 profiles as of February 2017)*

17. Obviously, the successful consultation of databases depends on the extent to which they are fed, in particular with biometric data. A case in point is the current gap between Interpol databases and the US SRTP (Secure Real-Time Platform), which enables the automatic comparison of fingerprints against US data, including battlefield data from Syria and Iraq and other conflict zones. The US offer to provide Member States with access to this data could bridge the gaps, by providing access an additional database against which irregular migrants can be checked.

18. Facial recognition technology could also be considered as an additional tool, especially to identify those whose facial details are known but there are no available fingerprints to crosscheck with. Again, the effectiveness of such databases' consultation depends on the population of such facial details databanks, which arguably are still in their early stages.

---

7 https://www.interpol.int/INTERPOL-expertise/Databases

8 Includes biometrics found and/or seized in conflict zones shared with Interpol via Notices.