Council of the
European Union

Brussels, 31 December 2020
(OR. en)

12860/1/20
REV 1

LIMITE

ENFOPOL 310
COSI 212
IXIM 119
JAI 987

NOTE

From:	Presidency
To:	Delegations
Subject:	COVID-19 impact on internal security – follow up on the discussion in COSI on 13 July 2020: Secure Communication

Measures to prevent the spread of COVID-19 continue to significantly impact the cooperation of law enforcement authorities across the European Union. On 13 July 2020, the Standing Committee on Internal Security (COSI) discussed the impact of COVID-19 on EU internal security, following an initial discussion on 15 May 2020 under the Croatian Presidency. There was broad agreement that upholding internal security in the EU requires strong cooperation based on reliable and secure communication, as an alternative to physical meetings. COSI suggested that Europol (by making use of the Europol Innovation Lab) could map available solutions. As a first step, the Law Enforcement Working Party (LEWP) and the Working Party on JHA Information Exchange (IXIM) were asked to discuss the parameters for improving secure communications between law enforcement authorities in the EU, focusing on end-users and also on the actors involved in the development and governance of relevant tools.

I. Outcome of recent activities in the Council and at Europol

An initial discussion of the parameters for a short-term improvement in secure communications took place at the LEWP VTC meeting on 23 July 2020. The main findings identified in the discussion were summarised in doc. 10315/20 (see Annex), discussed and endorsed by the LEWP and IXIM at their meetings in September and October.

Also other Council fora discussed the need for action to improve secure communication for information exchange within the EU: On 11 September 2020, COREPER II underlined the necessity of secure communication, especially for items classified between EU-RESTRICTED and EU-SECRET. It was pointed out that communication tools at these levels already exist (e.g. secure telephone network), but only within a very restricted group of users. Another crucial point identified was secure video-conferencing with various aspects concerning certified commercial providers and unknown participants (10502/20 und 10503/20 - EU-RESTRICTED). The "Antici Group" was tasked to further discuss the proposals made and report back to COREPER in due time.

With the aim to map available solutions, Europol and the German Federal Criminal Police Office (Bundeskriminalamt), with the support by a number of Member States[1], founded a core group on secure communication. The group's first meeting took place on 16 September 2020 where experiences were exchanged in relation to the short-term communication solutions found to overcome some of the restrictions to physical operational meetings due to the impact of COVID-19. Furthermore, the group discussed the requirements for secure communications as identified by LEWP and IXIM, the challenges of interconnecting existing national solutions[2]. The group prepared an overview of existing tools for secure communication to address short term needs[3].

Furthermore, the group also prepared a Draft Roadmap regarding the Extension of Secure Communications for EU Law Enforcement[4] in the short-, medium- and long term containing proposals for the way forward.

[1] FR, NL, PT, SI, ES, and CH

[2] 12556/20.

[3] 12557/20.

[4] 12554/20.

The roadmap, already welcomed by the Member States during the LEWP videoconference on 9 November 2020, aims at three objectives: Enabling the rapid fulfilment of operational needs of law enforcement officers, identifying the areas where there is a need for common standards and conditions for secure law enforcement communication and defining them, as well as setting a joint direction for the development and implementation of business-oriented, secure and interoperable communication solutions.

The roadmap suggests the following actions:

short term (first half of 2021)

- Finalize and maintain an overview of existing and developing tools
- Draft use cases for the different types of operational needs
- Create a qualification of existing tools and the specification of gaps

mid-term (mid-2021 till end of 2022)

- Assess common standards for interoperability between tools / solutions
- Identify structural preconditions for a scalable extension of secure LE communications

long-term (from 2023 to 2025 or possibly longer).

- Complement existing resources to fulfil the structural needs for the anticipated growth and technological solution
- Develop new solutions/additions to existing tools to offer practical functionalities that are currently missing

The Presidency shares the observation of Europol that, compared to the situation in the beginning of the COVID-19 pandemic, remarkable progress has been made regarding the digital communication between law enforcement authorities in the EU.

Europol is currently upgrading the number of virtual rooms and the number of users who can be simultanously connected via OpsTalk, the Agency's classified videoconferencing system, which is accessible to Member States‘ Liaison Bureaux. Europol has expanded the number of Virtual Command Post licences from 300 to 500, as well as engaging with the vendor to increase user experience and improve functionalities, including secure voice and video communication. Concerning the call for improving the roll-out and user-friendliness of SIENA, SIENA now has 2,200 active competent authorities connected (this figure excludes Liaison Bureaux/Europol National Units and National Contact points and inactive/obsolete mailboxes). In terms of usability improvements, several minor improvements have been implemented since 2019 (e.g. announcements on the landing page and simplification of some fields) while the first batch of major usability improvements is about to be deployed in production.

However, currently communication mostly still relies on commercial tools, often not suitable for communication and information exchange on sensitive issues. Therefore, in the opinion of the Presidency it remains urgent to achieve further progress in establishing secure communication solutions for EU law enforcement.

II. Next steps

COSI recognises the considerable efforts made in extending the possibilities for secure communication between law enforcement authorities in the EU since the beginning of the COVID-19 pandemic.

Subject to further progress to be reported by Europol on the core group's analysis and possible solutions concerning secure communication, COSI (...) **endorsed** the following next steps **at its meeting on 19 November 2020 and in the subsequent written consultation during which no substantial remarks have been raised by the delegations**:

1. COSI suggests that the core group on secure communication would invite experts from all Member States to participate and to continue its work and achieve the short term aims set out in the Roadmap for the first half of 2021 and, on the basis of results achieved, draft a proposal for the financing and monitoring of the Roadmap's implementation for discussion in COSI.

2. COSI will pursue the topic as a matter of high priority (follow-up by incoming Presidencies)

LEWP/IXIM Key findings for secure communication (short term)

Priority needs

Generally, Member States are calling for:

- the improvement and extension of communication tools and solutions that already exist (rather than creating new ones);
- the complementarity of solutions at EU level with national information management structures.

1. Secure Video Conferencing

The need for a secure video conferencing solution was stated.

General requirements

- Secure for exchange of operational data and classified information
- Availability for field officers and investigators
- Availability for policy [decision] makers/Council fora

Possible solutions

- Extending Europol's secure video conferencing application (Ops Talk) to law enforcement authorities
- Establishing secure videoconferencing for policy [decision] makers at Council level, or extending / upgrading the recently established PEXIP solution

2. Swift communication for operational purposes from mobile devices (“WhatsApp for law enforcement officers”)

To ensure effective cooperation between Member States’ law enforcement authorities, mobile instant messaging software for operational purposes (“WhatsApp for Law Enforcement Officers”) has to be established and made widely available to all officers who need it.

General requirements

- Secure/end-to-end encrypted; depending on the exact parameters of the solution, end-to-end encryption might be unnecessary if connections are established only via secure servers under full control of Member States’ governments and/or EU institutions
- User friendly (e.g. availability in different languages)
- Easy installation on different mobile devices/platforms
- Chatroom/group chat function
- Use of secure networks, no direct connection to the Internet, continuous state-of-the-art transport encryption
- Implementations should occur as open source solutions if possible; existing open source projects should be (re-)used

Possible solutions

- Extending Europol’s Virtual Command Post (VPC)
- Federation of different interoperable solutions based on a common open communication protocol, rather than the definition of one mandatory single product
- Quick Response for Operational Centres (QROC) project by the EU Agency for Large-Scale IT Systems (eu-LISA) and the European Network of Law Enforcement Technology Services (ENLETS)

3. SIENA Roll-Out

General requirements

- 24/7 availability (currently information exchange is monitored 24/7 at Europol and in several but not all Member States)
- Broader access to SIENA, e.g. for customs authorities, Police Customs Cooperation Centres (PCCCs) and also decentralised law enforcement authorities
- Establishing “SIENA-direct exchange” as a new workflow, complementing the conventional workflow through central agencies
- SIENA as the preferred channel of choice in Europe

Possible solutions

- Improving SIENA in terms of usability and integration of smart services, such as entity extraction, translation tool
- Promoting the SIENA web service as the key instrument to ensure that when information is exchanged directly, central agencies remain fully informed by integrated automated processes