Council of the European Union

Brussels, 8 September 2020
(OR. en)

10315/20

LIMITE

ENFOPOL 195
JAI 654
COMIX 376

NOTE

From:	Presidency
To:	Delegations
Subject:	COVID-19 impact on law enforcement – follow up: Secure Communication

I. Introduction

On 15 May and 13 July 2020, the Standing Committee on Internal Security (COSI) discussed the impact of COVID-19 on EU internal security. Measures to prevent the spread of COVID-19 have a significant impact on law enforcement authorities across the European Union. Upholding internal security in the EU requires strong cooperation based on reliable communication and especially - as an alternative to physical meetings - secure communication tools. 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 WP) were asked to discuss the parameters for improving secure communications between law enforcement authorities in the EU, focusing on actors involved in its development and governance, and on users.

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 are identified below and will be submitted to the IXIM WP for further assessment. Meanwhile, Europol, in particular its Innovation Lab, is analysing existing solutions, operational requirements and possible gaps in secure communications, as tasked by the COSI at its meeting of 13 July 2020.

II. Priority needs

Generally, Member States are calling for:

- the improvement and extension of communication tools and solutions[1] 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

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 widely made available to all officers who need it.

General requirements

[1] Another communication tool addressed during the LEWP discussions was vRoom ('virtual Requests out of Mandate') within the Europol Platform for Experts (EPE). The EPE's vRoom makes it possible for competent authorities to swiftly communicate on issues regarding COVID-19, including those that might not fall directly under Europol's core activities. It is comparable to an internet forum which contains questions and answers that are visible to all registered users. However, as it does not allow for the exchange of operational information, it remains beyond the scope of this paper and further discussion on secure communication solutions.

- Secure/end-to-end encrypted; depending on the details of the solution, end-to-end encryption might be unnecessary if connections are limited to 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 standard, 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, and 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

III. Way forward

The LEWP and IXIM WP recognise the considerable efforts made in extending the options for virtual communication since the beginning of COVID-19 pandemic.

Subject to further consultation/discussion in the IXIM WP and progress to be reported by Europol on its analysis concerning secure communications as tasked by COSI, this document mainly aims to report on the outcome of the LEWP's discussions on 23 July 2020 (see above) and additionally to suggest a possible way forward to address the issues identified:

1. The Member States, the Council of the EU, the Commission, EU Agencies and all relevant stakeholders should be encouraged:

   - to swiftly extend the availability of video conference meetings (primarily) for essential cooperation fora at bi-/multilateral and EU level;
   - to devise solutions that allow for discussion of restricted/operational content at EU level (e.g. for Council Working Parties, other Council fora) as soon as possible.

2. Member States are encouraged to make full use of the existing secure communication possibilities, in particular the roll-out of SIENA to all relevant competent authorities, the integration of the SIENA Web Service within Member States' single points of contact (SPOCs) to ensure 24/7 monitoring and an integrated view on all law enforcement channels and, where operationally required, the implementation of SIENA CONFIDENTIAL to allow exchanges of information at the level of EU Confidential.

3. Europol should facilitate the extended implementation and operational use of its existing products and services by Member States and assess where, in accordance with the corporate prioritisation mechanisms, the delivery of additional services can be speeded up, especially where this would entail:

   - swiftly expanding its secure video conferencing tool, including bandwidth extension;
   - exploring ways of making progress on mobile solutions for investigators/field officers that enable swift and secure communication (or to interconnecting already existing solutions);
   - improving the roll-out and user-friendliness of SIENA.