EUROPEAN
COMMISSION

Strasbourg, 16.5.2017
COM(2017) 261 final

# COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL

## Seventh progress report towards an effective and genuine Security Union

## I. INTRODUCTION

This is the seventh monthly report on the progress made towards building an effective and genuine Security Union and covers developments under two main pillars: tackling terrorism and organised crime and the means that support them; and strengthening our defences and building resilience against those threats. This report focuses on the work towards the interoperability of information systems for security, border and migration management to make data management in the EU more effective and efficient, in full respect of data protection requirements, to better protect the external borders and enhance internal security for the benefit of all citizens. This report also provides an update on progress made on key legislative and non-legislative files.

The recent global cyberattack using ransomware to disable thousands of computer systems has again highlighted the urgent need to step up the EU's cyber resilience and security actions given the rapidly growing increase in cyber-enabled organised crime, as set out in the last Security Union Progress Report[1] and highlighted in Europol's Serious and Organised Crime Threat Assessment.[2] The Commission is accelerating its work on cybersecurity, in particular through its review of the 2013 EU Cybersecurity Strategy[3] as announced in the Digital Single Market mid-term review[4], to provide a current and effective response to address these threats.

President Juncker's State of the Union address in September 2016[5] and the European Council conclusions of December 2016[6] highlighted the importance of overcoming the current shortcomings in data management and of improving the interoperability of existing information systems. Recent terrorist attacks have brought this into even sharper focus, highlighting the urgent need for information systems to be interoperable, and to eliminate the current blind spots where terrorist suspects can be recorded in different, unconnected databases under different aliases. This report sets out the Commission's approach **on how to achieve the interoperability of information systems for security, border and migration management by 2020** to ensure that border guards, law enforcement officers including customs officials, immigration officials and judicial authorities have the necessary information at their disposal. This is a follow up to the April 2016 Commission Communication on stronger and smarter information systems for borders and security [7] and the work of the High-Level Expert Group on Information Systems and Interoperability that the Commission set up following that Communication.

## II. STRONGER AND SMARTER INFORMATION SYSTEMS

### *1. The Commission's Communication of April 2016 and steps taken so far*

The April 2016 Communication on stronger and smarter information systems for borders and security identified a number of structural shortcomings related to information systems:

---

1 COM(2016) 213 final (12.4.2017).

2 https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017.

3 JOIN(2013) 1 final (7.2.2013).

4 COM(2017) 228 final (10.5.2017). See also the Fourth Security Union Progress Report, COM(2017) 41 final (25.1.2017).

5 State of the Union 2016 (14.9.2016), https://ec.europa.eu/commission/state-union-2016_en.

6 European Council conclusions (15.12.2016), http://www.consilium.europa.eu/en/meetings/european-council/2016/12/20161215-euco-conclusions-final_pdf/.

7 COM(2016) 205 final (6.4.2016).

- sub-optimal functionalities in some of the existing information systems;
- information gaps in the EU's architecture of data management;
- a complex landscape of differently governed information systems; and
- a fragmented architecture of data management for borders and security where information is stored separately in unconnected systems, leading to blind spots.

To address these shortcomings, **the Commission proposed action in three areas**, underlining that the requirements of the Charter of Fundamental Rights and in particular the comprehensive framework for the protection of personal data in the EU will guide the Commission's work.

First, the Communication set out possible options for **maximising the benefits of existing information systems, stressing that Member States need to make full use of these systems**. Subsequently, the Commission presented in December 2016 legislative proposals to strengthen the Schengen Information System (SIS)[8] which is the most successful existing tool for cooperation of border guards, customs authorities, police officers and judicial authorities. The Commission also presented a legislative proposal in May 2016 to reinforce the asylum and irregular migration database Eurodac[9], facilitating returns and helping tackle irregular migration. In January 2016, the Commission presented a legislative proposal to facilitate the exchange of criminal records of third-country nationals in the EU by upgrading the European Criminal Records Information System (ECRIS).[10] As announced[11], and in the light of discussions with the co-legislators on the January 2016 proposal, the Commission will present in June 2017 a supplementary proposal to establish a centralised system[12] to identify convicted third-country nationals and to indicate which Member States are holding information on them.

In June 2017, the Commission will also present a legislative proposal to revise the legal mandate of eu-LISA[13], including a task for the agency on the development of interoperability of centralised EU information systems for security, border and migration management.

Second, the Communication set out possible options for **developing new and complementary actions to address gaps in the EU's architecture of data management**. In particular, the Commission identified significant information gaps regarding third-country nationals visiting the Schengen area and, within that same group, regarding visa-exempt third-country nationals entering the EU through land borders. Currently, the external border crossings of third-country nationals are not recorded, and no information is available for visa-exempt third-country nationals prior to their arrival at the external land border. As a follow-up the Commission presented legislative proposals to establish two new information systems to address these important gaps. In April 2016, the Commission proposed an EU Entry/Exit System to modernise external border management by improving the quality and efficiency of

---

8 COM(2016) 881 final (21.12.2016), COM(2016) 882 final (21.12.2016), COM(2016) 883 final (21.12.2016).

9 COM(2016) 272 final (4.5.2016).

10 COM(2016) 7 final (19.1.2016).

11 See the Fifth progress report towards an effective and genuine Security Union, COM(2017) 203 final (2.3.2017).

12 When Member States seek information about the conviction of a third-country national, the centralised system will direct them to those Member States where the criminal record details can be found.

13 European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

controls.[14] In November 2016, the Commission proposed a European Travel Information and Authorisation System (ETIAS) to gather information on all those travelling visa-free to the European Union so as to carry out irregular migration and security checks in advance.[15]

The third area underlined by the Communication highlighted the **need to improve the interoperability of information systems**. The Communication set out that with the comprehensive framework for the protection of personal data in the EU and significant developments in technology and IT security, there is a way to achieve the interoperability of information systems accompanied by the necessary strict rules on access and use without affecting the existing purpose limitation. The Communication presented **four options** to achieve interoperability:

- a **single-search interface** to query several information systems simultaneously and to produce combined results from the systems queried on one single screen;
- the **interconnectivity of information systems** where data registered in one system will automatically be consulted by another system;
- the establishment of a **shared biometric matching service** in support of various information systems; and
- a **common identity repository** with alphanumeric data for different information systems (including common biographical attributes such as name and date of birth).

The Commission initiated a discussion on how information systems in the European Union can better enhance border management and internal security and set up a High-Level Expert Group on Information Systems and Interoperability to take this work forward (see Section II.3 below).

*2. Progress on priority files on information systems*

Border guards, law enforcement officers, immigration officers and judicial authorities need access to accurate and complete data to do their jobs. **It is therefore essential that the European Parliament and the Council move forward on the priority proposals on information systems** under the first strand of the April 2016 Communication. As set out above, this is key to making existing information systems more effective for borders and security, and it will close important information gaps by establishing new systems necessary to secure the external border.

The most advanced proposal is the **EU Entry/Exit System**. This is in the trilogue phase and the target of concluding in June 2017, set by the European Council, is on track. Technical discussions continue to advance on the **European Travel Information and Authorisation System** (ETIAS), but the two institutions have yet to reach their negotiating positions. The adoption of the Council mandate is planned for June 2017, while the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) plans to adopt its negotiating mandate in September 2017. The Joint Declaration on the EU's legislative priorities for 2017[16] gave priority treatment to this file to ensure its delivery before the end of 2017. The Commission will continue to support the co-legislators to reach this goal. The two institutions

[14] COM(2016) 194 final (6.4.2016).
[15] COM(2016) 731 final (16.11.2016).
[16] Joint Declaration on the EU's legislative priorities for 2017 (13.12.2016), https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-legislative-priorities-2017-jan2017_en.pdf.

are also working on the Commission proposals to strengthen the **Schengen Information System** (SIS). The first round of discussions on the three proposals at Council working group level will be finalised under the Maltese Council Presidency. The European Parliament's rapporteur envisages to present a draft report in the Committee on Civil Liberties, Justice and Home Affairs (LIBE) by the end of June 2017. As regards the legislative proposal to reinforce **Eurodac**, the Council agreed on a partial general approach in December 2016 while the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) plans to vote on its report in May 2017. The trilogue phase should start right after.

*3. The work of the High-Level Expert Group on Information Systems and Interoperability*

In June 2016, the Commission set up the High-Level Expert Group on Information Systems and Interoperability. The task of the Expert Group was to **address the legal, technical and operational challenges of the four options** to achieve interoperability, including their necessity, technical feasibility, proportionality and data protection implications.[17] The Expert Group was also asked to identify and address shortcomings and potential information gaps caused by the complexity and fragmentation of information systems.[18] It brought together experts from Member States and associated Schengen countries, and from the EU agencies eu-LISA, Europol, the European Asylum Support Office, the European Border and Coast Guard Agency and the Fundamental Rights Agency. The EU Counter-Terrorism Coordinator and the European Data Protection Supervisor participated as full members. Representatives of the Secretariat of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) and of the General Secretariat of the Council attended as observers.

The Commission welcomes the final report[19] of the High-Level Expert Group of 11 May 2017. The Expert Group concluded that **it is necessary and technically feasible to work towards the following three solutions for interoperability** and that they can, in principle, both **deliver operational gains** and be established **in compliance with data protection requirements**:

- a European search portal[20];
- a shared biometric matching service; and
- a common identity repository.

In the Expert Group's view, the option of interconnectivity of systems should only be considered on a case-by-case basis. One such case is the interconnection of the proposed EU Entry/Exit System and the Visa Information System.[21] The Commission proposal for the EU Entry/Exit System provides that data contained in the Visa Information System would be systematically and automatically consulted by the EU Entry/Exit System to store a small subset of data (visa sticker, number of entries, period of stay), enabling the EU Entry/Exit System to process data on visa holders correctly in compliance with the requirements of data

---

17 Commission Decision 2016/C 257/03 (17.6.2016).

18 See the scoping paper of the Expert Group (June 2016): http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=24081&no=2.

19 The final report of the Expert Group can be found at: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1. Its annexes include an executive summary of a report by the Fundamental Rights Agency as well as statements by the European Data Protection Supervisor and the EU Counter-Terrorism Coordinator.

20 The term ' single-search interface' was changed to 'European search portal' to avoid any confusion with national single-search interfaces that exist in Member States for national information systems.

21 Regulation (EC) No 767/2008 (9.7.2008).

minimisation and data consistency. The Expert Group considered that, provided sufficient progress is made on the other three solutions for interoperability, there is less need for interconnectivity between systems for the sole reason of improving the exchange of data.

The Expert Group's final report also highlighted the **importance of fully implementing and applying existing information systems**. It also looked at the decentralised **Prüm framework** for the exchange of data regarding DNA, fingerprints and vehicle registration,[22] recommending a feasibility study on moving towards a centralised routing component and possibly adding new functionalities. Concerning the decentralised system established by the **EU Passenger Name Record (PNR) Directive**[23], the Expert Group recommended a feasibility study on a centralised component for advance passenger information and passenger name record data as a technical support tool to facilitate the connectivity with air carriers. It considered that this would strengthen the effectiveness of Passenger Information Units once Member States have implemented the EU Passenger Name Record Directive.

The Commission will continue to focus on the **full implementation of existing information systems**. It is essential that the Member States make full use of existing systems, exploiting fully their potential. The Commission will continue to provide comprehensive support, in line with its implementation plan[24], to help ensure that all Member States implement the EU Passenger Name Record Directive by May 2018. It will work closely with all Member States on completing the full roll-out of the Prüm framework, in particular with the five Member States that still need to implement the Prüm Decisions. In the spirit of the recommendations of the Expert Group, the Commission will examine ways to strengthen the functioning and effectiveness of these systems when they are applied by Member States.

The Expert Group identified an **information gap related to external border crossings of EU citizens**. Its final report refers to the recent introduction of systematic checks against relevant databases of all persons, who enjoy the right to free movement under Union law, when they leave and enter the Schengen area.[25] It highlights that the time and place of these checks are not recorded and notes that this could provide useful information for law enforcement. The Expert Group therefore recommended further analysis of the proportionality and feasibility of a systematic recording of external border crossings of all EU citizens.[26]

The Commission notes that the Expert Group's report does not demonstrate the necessity and proportionality of recording the external border crossings of all EU citizens. Should further elements come to light demonstrating the necessity and proportionality of such recording, the Commission stands ready to assess the need for further action. Meanwhile, the Commission will look into the Expert Group's related recommendation to work towards the possible registration of 'hits' in the Schengen Information System of people under alert, as a possible way to register the travel movements of those EU citizens who have been identified as potentially involved in terrorism or other forms of serious crime.

The Expert Group also identified an **information gap related to long-stay visas, residence permits and residence cards**. It observed that Member States have little means to check the

[22] Council Decision 2008/615/JHA (23.6.2008).
[23] Directive (EU) 2016/681 (27.4.2016).
[24] SWD(2016) 426 final (28.11.2016).
[25] Regulation (EU) 2017/458 of 15.3.2017.
[26] The Expert Group also discussed the options of extending the proposed EU Entry/Exit System to include EU citizens or extending the use of logs of the Schengen Information System. Both options were discarded.

validity of these documents in cases where they are issued by another Member State, and suggested that this could point to exploring a centralised EU repository containing information on long-stay visas, residence permits and residence cards. The Commission will assess the need for such a repository, including its necessity, technical feasibility and proportionality.

Finally, the Expert Group's report states that **customs authorities** are a crucial actor in the multi-agency cooperation at the external borders. Therefore, the Commission is exploring further the technical, operational and legal aspects of interoperability with customs systems.

## III. TOWARDS THE INTEROPERABILITY OF INFORMATION SYSTEMS

### *1. The Commission's objective for the interoperability of information systems by 2020*

The key objective is to ensure that border guards, law enforcement officers, immigration officials and judicial authorities have the necessary information at their disposal to better protect the external borders and enhance internal security for the benefit of all citizens. This is why the first step is that the various information systems in this field deliver effectively, and that the legislative proposals already on the table are swiftly adopted.

In line with the April 2016 Communication, and confirmed by the findings and recommendations of the Expert Group, the Commission sets out a **new approach to the management of data for borders and security** where all centralised EU information systems for security, border and migration management[27] are interoperable in full respect of fundamental rights so that:

- the systems can be searched simultaneously using a **European search portal**, in full compliance with purpose limitations and access rights, to make better use of existing information systems, possibly with more streamlined rules for law enforcement access[28];
- the systems use one **shared biometric matching service** to enable searches across different information systems holding biometric data, possibly with hit/no-hit flags indicating the connection with related biometric data found in another system[29];
- the systems share a **common identity repository** with alphanumeric identity data[30], to detect if a person is registered under multiple identities in different databases.

This new approach must ensure that the systems keep their **specific data protection provisions**, with specific rules on access for competent authorities, separate purpose

---

[27] The Schengen Information System, the Visa Information System, Eurodac, the proposed EU Entry/Exit System, the proposed European Travel Information and Authorisation System (ETIAS) and the proposed European Criminal Records Information System (ECRIS) for third-country nationals.

[28] The Council's Committee of Permanent Representatives (Coreper), upon giving the mandate to the Council Presidency to start interinstitutional negotiations on the EU Entry/Exit System on 2 March 2017, called on the Commission to propose a comprehensive framework for law enforcement access to the various databases in the area of justice and home affairs, with a view to greater simplification, consistency, effectiveness and attention to operational needs. The Expert Group recommends that the framework for law enforcement access would be based on a two-step approach where actual visualisation of data would only be envisaged once the existence of this data has been ascertained, thus improving effectiveness but reducing the number and extent of law enforcement accesses.

[29] Further technical analysis is needed on the potential inclusion of flagging functionalities in a shared biometric matching service and the data protection implications – see Section III.2 below.

[30] This would include common biographical attributes such as name, date of birth and gender.

limitation rules for each category of data and dedicated data retention rules. This approach on interoperability would not lead to the interconnectivity of all the individual systems.

This new approach would overcome the current weaknesses in the EU's architecture of data management, including eliminating identified blind spots. **eu-LISA** will play a crucial role in the work towards the interoperability of information systems, including with on-going and further technical analysis (see Section III.2 below). The legislative proposal that the Commission will present in June 2017 will strengthen eu-LISA's mandate, enabling it to ensure the implementation of this new approach. The Commission will also continue to involve the European Data Protection Supervisor and the Fundamental Rights Agency in the work on interoperability.

Ensuring a high level of **data quality is essential for information systems to be effective**. Interoperability can only work if information systems are fed with accurate and complete data. The Commission already identified data quality as a matter requiring further EU action.[31] It will, as a matter of urgency and together with eu-LISA, implement the recommendations made by the Expert Group to improve the quality of data in EU information systems.

The Commission will take forward the Expert Group's recommendations on automated quality control, a 'data warehouse' capable of analysing anonymised data extracted from relevant information systems for statistical and reporting purposes, and training modules on data quality for staff responsible for providing input to the systems at national level. The important role of eu-LISA in ensuring high data quality in centralised EU information systems will also be reflected in the upcoming legislative proposal.

Interoperability requires technical interaction between existing information systems. Facilitating this interaction is the objective of the **Universal Message Format** (UMF) at EU level. The Commission, together with eu-LISA, will take forward the recommendations of the Expert Group to enhance the Universal Message Format in line with ongoing work, with the aim to ensure that the development of the format is reflected in EU centralised information systems.

*2. The way forward to achieve the interoperability of information systems by 2020*

In parallel to the work on delivery of the priority files on information systems, the Commission invites the European Parliament and the Council to hold a **joint discussion on the way forward** on interoperability as set out in this Communication. To this end, the Commission will present and discuss these ideas with the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) on 29 May 2017 and with the Member States at the 8 June 2017 Justice and Home Affairs Council. Building on those discussions, the three institutions should hold tripartite technical level meetings[32] in autumn 2017 further to discuss the way forward on interoperability as set out in this Communication, including the operational needs for borders and security and how to ensure proportionality and full compliance with fundamental rights. The goal is to reach as soon as possible, and at the latest before the end of 2017, a **common understanding on the way forward** and on the necessary steps to be taken to achieve the interoperability of information systems by 2020.

[31] Fourth progress report towards an effective and genuine Security Union, COM(2017) 41 final (25.1.2017).

[32] These technical meetings could follow the example of the meeting on Smart Borders held in February 2015.

In parallel to the joint discussion between the three institutions, and without anticipating its outcome, the Commission and eu-LISA will continue to conduct **further technical analysis on the identified solutions for interoperability** in the course of 2017, through a series of technical studies and proofs of concept. The Commission will regularly update the European Parliament and the Council on progress made in this technical analysis.

Taking advantage of the exchanges with the European Parliament and the Council, as well as the outcome of the ongoing legislative work on information systems and further technical analysis, the **Commission is working intensively to present, as soon as possible**[33]**, a legislative proposal on interoperability**. In line with better regulation principles, the preparation of the legislative proposal will include a public consultation and an impact assessment, including on fundamental rights and in particular the right to the protection of personal data. Together with the legislative proposal on interoperability, the Commission will also present a legislative proposal to revise the legal basis of the Visa Information System[34] following up on the evaluation report presented in October 2016.[35] The Visa Information System is one of the centralised information systems that should be part of the new approach to the management of data for borders and security.

The **joint discussion between the three institutions on the way forward to achieve interoperability by 2020 should not delay the work on legislative proposals** on information systems currently under discussion by the co-legislators. Most of these proposals have already been identified by the Joint Declaration as urgent and key priorities, and they all address important information gaps requiring urgent action, also in line with Expert Group's recommendations. The supplementary legislative proposal for a European Criminal Records Information System (ECRIS) for third-country nationals that the Commission will present in June 2017 will also be fully compatible with the Expert Group's recommendations on interoperability and the approach set out in this Communication. In order to implement this new approach in a way that is manageable, it is essential that the legal bases of all affected information systems are stable. This is why agreement on the legislative proposals currently under discussion must come first.

## IV. IMPLEMENTATION OF OTHER PRIORITY FILES ON SECURITY

### *1. Legislative initiatives*

On 1 May 2017, the new **Europol Regulation**[36] entered into application. It constitutes a turning point for Europol and introduces a number of new elements that will allow the EU law enforcement agency to become a genuine EU hub for information exchange on serious cross-border crime and terrorism. Europol will have the tools to become more effective, efficient and accountable. In particular, a changed framework for data processing will enhance the agency's capacity to develop criminal analyses at the service of Member States, and a more robust data protection regime will ensure independent and effective data protection supervision.

---

[33] This will require agreement by the co-legislators on the related legislative files currently under discussion – see Section II.2 above.

[34] Regulation (EC) No 767/2008 (9.7.2008).

[35] COM(2016) 655 final (14.10.2016).

[36] Regulation (EU) 2016/794 (11.5.2016).

As required by the Treaty, Europol's activities will be further scrutinised by the European Parliament, together with national Parliaments, which will further increase the agency's transparency and legitimacy in the eyes of citizens.

To minimise the negative effects of the Danish departure from Europol following the results of the referendum in Denmark on 3 December 2016, an **operational cooperation agreement between Europol and Denmark** was signed on 30 April 2017. As agreed in the joint declaration of President Juncker, Council President Tusk and the Danish Prime Minister Rasmussen of 15 December 2016[37], the agreement lays down special operational arrangements providing for a sufficient level of operational cooperation between Denmark and Europol, including the exchange of operational data and exchanges of liaison officers, subject to adequate safeguards. Although this agreement does not replace full membership of Denmark at Europol, i.e. access to Europol's data repositories or full membership in Europol's governance fora, Denmark has accepted the jurisdiction of the European Court of Justice and the competence of the European Data Protection Supervisor, and has implemented in Danish law the relevant EU data protection rules[38]. As set out in the joint declaration, these arrangements are conditioned on Denmark's continuing membership of the EU and the Schengen area.

On 28 April 2017, the Commission adopted an implementing decision on the common protocols and data formats to be used by air carriers when transferring **passenger name record (PNR)** data to Passenger Information Units (PIUs) pursuant to the EU Passenger Name Record Directive[39]. This implementing decision harmonises the technical aspects of the transmission of passenger name record data by air carriers. The agreed data formats and transmission protocols will be mandatory for all transfers of passenger name record data by air carriers to the Passenger Information Units as of 28 April 2018.

On 25 April 2017, the Council formally adopted the new **Firearms Directive**.[40] Member States now have 15 months to put in place the required controls on the acquisition and possession of firearms to ensure that criminal groups or terrorists do not exploit fragmented rules across the Union. On 28 April 2017, the Expert Group on Deactivation Standards reached an agreement on the new deactivation standards with a view to adopting a revised Commission Regulation (EU) 2015/2403 before July 2017. The current revised version aims to clarify some technical standards to ensure the correct application of all technical proceedings for the deactivation of a weapon.

*2. Implementation of non-legislative actions*

The large scale global ransomware attack on 12 May 2017 has highlighted the urgent need for the EU and its agencies and Member States to step up their actions to combat the growing threat of **cybercrime**, focussing also on detection and deterrence. The European Cybercrime Centre at Europol (EC3) has played a leading role in the law enforcement response to the latest attack, building on the work it has done previously in this area notably through the 'no more ransom' campaign. The EU Computer Emergency Response Team has also been in close contact with the European Cybercrime Centre, affected countries' Computer Security

---

37 Declaration by the President of the European Commission, Jean-Claude Juncker, the President of the European Council, Donald Tusk and the Prime Minister of Denmark, Lars Løkke Rasmussen (15.12.2016), http://europa.eu/rapid/press-release_IP-16-4398_en.htm.

38 Directive (EU) 2016/680 (27.4.2016).

39 Directive (EU) 2016/681 (27.4.2016).

40 http://www.consilium.europa.eu/en/press/press-releases/2017/04/25-control-acquisition-possession-weapons/

Incident Response Teams, cybercrime units and key industry partners to mitigate the threat and assist victims. The Commission announced in the Digital Single Market mid-term review on 10 May 2017 its intention to review the 2013 EU Cybersecurity Strategy by September 2017. This work is being accelerated to ensure that the existing focus on prevention is broadened to include a greater emphasis on detection and deterrence. The aim should be both to reduce the likelihood of cyber-attacks and also their impact by strengthening resilience and further developing the work of Member States in building their national capacities and implementing fully the Network Information Security Directive[41]. The potential for cybercrime (and cyber-enabled crime) stems not only from flaws in systems and software but also from behaviours which lead to poor cyber-hygiene. The Commission will not only strengthen the mandate of the EU Network and Information Security Agency (ENISA) but also bring forward proposals to develop cyber security standards, certification and labelling to make systems and devices more cyber secure. It will also focus on building cyber skills and technical capacity within the Union.

In the current circumstances of threats related to public policy or internal security, **intensified police checks** in the territory of Member States, including in border areas, may be both necessary and justified to enhance security within the Schengen area. This is why, on 2 May 2017, the Commission presented a Recommendation on proportionate police checks and police cooperation in the Schengen area.[42] The recommendation sets out measures Schengen States should take to provide for a more effective use of existing police powers to address threats to public policy or internal security. When needed and justified, Member States should intensify police checks in border areas and on main transport routes. The decision on such checks as well as their location and intensity remains fully in the hands of the Member States and should always be proportionate to the identified threats. In addition, the Commission recommends that all Member States strengthen cross-border police cooperation to address threats to public policy or internal security.

In the area of **aviation security**, there have been developments in recent weeks with new security measures imposed by the United States and the United Kingdom on incoming flights from a number of countries in the Middle East, North Africa and Turkey, requiring that large electronics are placed in checked-in baggage. On the EU side, work has advanced on the risk assessment on threats and vulnerabilities for incoming flights coming from third countries. Following information that the United States may be planning to introduce similar measures for flights from EU airports, the Commission has facilitated contacts at political level to ensure coordinated actions between the United States and the EU. A meeting between the United States and the EU side will take place in Brussels on 17 May 2017, in order to jointly assess the potential risks and work towards a common approach to address the developing threat.

Work is ongoing in the Council's Standing Committee on Operational Cooperation on Internal Security (COSI) on the next **EU Policy Cycle for serious international and organised crime** for the years 2018-2021, taking into account the eight crime threat priorities

[41] Directive (EU) 2016/1148 (6.7.2016).

[42] On 2 May 2017, the Commission approved in principle the Recommendation on proportionate police checks and police cooperation in the Schengen area (C(2017) 2923). Formal adoption took place on 12 May 2017.

identified by the Commission in the last Security Union Progress Report.[43] The Council is expected to adopt Council Conclusions on the new EU Policy Cycle on 18 May 2017.

Following the Commission's progress report to the Justice and Home Affairs Council in December 2016 on the ongoing work to improve criminal investigators' cross-border access to **electronic evidence**[44], the Commission is currently finalising its assessment and will propose a way forward for discussions at the Justice and Home Affairs Council on 8 June 2017.

The Commission has supported the work that at this stage a group of Member States undertakes to maintain e-CODEX, a system for cross border judicial cooperation and digital access to legal procedures. The Commission has taken note that these Member States consider that this is not a sustainable solution. At Council working group level, the Member States have examined different options and concluded that the best place to ensure maintenance and operability of the e-CODEX system would be eu-LISA. To explore the best solution, the Commission has launched an assessment of the impact of various options for the maintenance of e-CODEX. The result of this impact assessment will be available by autumn 2017.

The above-mentioned adoption of the Firearms Directive is an important step forward to enforce the rules on legal acquisition and possession of firearms. The Commission is also addressing **illicit trafficking of firearms** both within the EU and outside its borders. On 16 March 2017, an EU-Ukrainian technical roundtable on illicit trafficking of firearms took place in Kiev. This was the first meeting of its kind between the EU and Ukraine to improve the exchange of information related to illicit trafficking of firearms. The second EU-Tunisian technical roundtable on illicit trafficking of firearms was held in Tunis on 28 March 2017. For both Ukraine and Tunisia, an action plan was agreed that includes EU expert missions to evaluate each country's administrative framework, to organise a high-level conference on related legislation, and to propose training, study visits and workshops on practical data management as well as operational cooperation.

The Commission and the European External Action Service submitted to the Council a **joint non-paper on EU external action on counter-terrorism** on 12 May 2017 outlining the priority countries, areas and instruments for EU action in this field. This joint paper contributes to the discussion on the revision of the February 2015 Council Conclusions on EU external counter-terrorism action[45], with the aim to adopt new Council Conclusions at the June 2017 Foreign Affairs Council.

A first EU-Neighbouring Countries Workshop on **Critical Infrastructure Protection** (CIP) took place in Bucharest on 16-17 March 2017, as part of widening the external dimension of the European Programme for Critical Infrastructure Protection. Besides Member States, participants included representatives from eight Eastern European and Western Balkan countries. The aim of this first workshop was to establish contacts and exchange information

---

[43] COM(2017) 213 final (12.4.2017). The eight crime threat priorities identified by the Commission are: cybercrime, drugs crime, migrant smuggling, organised property crime, trafficking in human beings, firearms trafficking, VAT fraud and environmental crime.

[44] See the non-paper from the Commission Services: Progress report following the Conclusions of the Council of the European Union on improving criminal justice in cyberspace (2.12.2016): http://data.consilium.europa.eu/doc/document/ST-15072-2016-INIT/en/pdf. In its Conclusions on improving criminal justice in cyberspace of 9 June 2016, the Council called on the Commission to take concrete actions, develop a common EU approach and to present deliverables by June 2017.

[45] Council Conclusions on counter-terrorism (9.2.2015): http://www.consilium.europa.eu/en/press/press-releases/ 2015/02/150209-council-conclusions-counter-terrorism/.

on measures and tools to protect critical infrastructure. Possible areas for further cooperation were identified, including joint training or exercises centred around practical (operational) aspects, regional interdependencies studies and peer reviews of national strategies of critical infrastructure protection.

## V. CONCLUSION

The Commission calls on the European Parliament and the Council to advance on the delivery of legislative priorities on information systems for security, border and migration management. This will strengthen existing systems and close already identified information gaps, responding to the needs of border guards, law enforcement officers including customs officials, immigration officials and judicial authorities as well as creating the basis for making these systems more interoperable.

As a follow up to the Communication of April 2016 on stronger and smarter information systems for borders and security, and in light of the recommendations of the High-Level Expert Group on Information Systems and Interoperability, the Commission has set out a new approach to the management of data for borders and security, whereby all centralised EU information systems for security, border and migration management are interoperable, in full respect of fundamental rights. To that end, and building on the ongoing legislative and technical work on information systems, the Commission will present a legislative proposal in June 2017 to strengthen eu-LISA's mandate enabling it to ensure the implementation of this new approach, followed by a legislative proposal on interoperability as soon as possible. The Commission invites the European Parliament and the Council to hold a joint discussion on the proposed way forward. This would allow the three institutions to reach a common understanding on the way forward on interoperability and on the necessary steps for its implementation by 2020, in full compliance with fundamental rights. Implementing the approach on interoperability set out would make data management in the EU more effective and efficient to better protect the external borders and enhance internal security for the benefit of all citizens.