Briefing
Initial Appraisal of a European Commission Impact Assessment

European Parliament

February 2018

Interoperability between EU information systems for security, border and migration management

Impact Assessment (SWD(2017) 473, SWD(2017) 474 (summary)) of a Commission proposal for a regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 (COM(2017)793) and of a Commission proposal for a regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) (COM(2017) 794)

Background

This note seeks to provide an initial analysis of the strengths and weaknesses of the European Commission's impact assessment (IA) accompanying the above proposals on (1) borders and visa; and on (2) police and judicial cooperation, asylum and migration, submitted on 12 December 2017 and referred to Parliament's Committee on Civil Liberties, Justice and Home Affairs. In 2016, the European Commission stressed the need for interoperability between EU border and security information systems.[1] Likewise, the Joint Declaration on the EU's legislative priorities for 2018-2019 identified interoperable EU information systems as a key priority. The initiative aims to make information exchange and data sharing between the various EU information systems more effective and efficient, fully upholding fundamental rights, so as to boost the protection of the EU's external borders, improve migration management and enhance internal security.[2] Interoperability[3] is not a new topic, already in 2004 the European Council called for enhanced interoperability between the Schengen Information System (SIS) II, the Visa Information System (VIS) and Eurodac (the EU asylum fingerprint database).[4]

Problem definition

The IA identifies two problems: first, information provided by EU systems is not always complete, accurate and reliable. This, in turn, makes it difficult to detect multiple identities or to combat identity fraud. Second, end-users do not always have fast and systematic access to all the information they need to perform their tasks. 'For most users' purposes, the issue is not that the access rights of the end-users, as set out in EU legislation, are too limited. The problem is rather that the existing access rights, as laid down in the EU legal instruments that

[1] Communication on stronger and smarter information systems for borders and security, COM(2016) 205, European Commission, 6 April 2016.
[2] For further information, see C. Dumbrava, Interoperability of European information systems for border management and security, EPRS, European Parliament, June 2017; and C. Dumbrava, European information systems in the area of justice and home affairs: An overview, EPRS, European Parliament, May 2017.
[3] The European Commission defined interoperability as 'the ability of information systems to exchange data and to enable the sharing of information', see European Commission communication, COM(2016) 205, 6 April 2016, p. 14.
[4] E. Brouwer, *Digital Borders and Real Rights – Effective Remedies for Third-Country Nationals in the Schengen Information System,* Martinus Nijhoff, 2008, pp. 2, 132-134.

EPRS | European Parliamentary Research Service
Author: Katharina Eisele
Ex-Ante Impact Assessment Unit
PE 615.649

govern the systems, cannot be used to the full because of a lack of technical and practical means at national level' (IA, p. 9). The Commission identifies two problem drivers:

- a fragmented architecture of data management for borders and security where information is stored separately in unconnected systems, leading to blind spots;
- a complex landscape of differently governed information systems (IA, pp. 9-12).

The difference between problem drivers 1 and 2 is not entirely clear, they appear to be inherently intertwined. Moreover, it seems that the problems that the Commission identifies are self-inflicted in the sense that the EU introduced the various information systems with their different access rules in 'separate silos' itself in the first place (IA, p. 11). It seems that the reason for introducing the information systems in 'separate silos' was in particular based on the principle of purpose limitation.[5] Questions arise as to whether and, if so, how the issue of interoperability was discussed when the various systems were created. The IA provides little background information in this respect. Neither is it clear how the initiative would in fact tackle the first problem, because it is the national authorities that have to feed the EU information systems with data.

In addition, it would have been useful if the Commission had provided indications or estimations regarding the scale of the problem of multiple identities/identity fraud; alternatively, if that was not possible, the Commission could have explicitly stated so. A clearer problem description, underpinned by evidence, was in fact also one of the issues raised by the European Data Protection Supervisor (EDPS) in his reflection paper,[6] which analyses the Commission's inception impact assessment of July 2017. Contrary to what the Commission has suggested in the past,[7] interoperability has different dimensions, including technical, legal and political ones.[8]

Annex 7 of the IA includes a matrix with more detailed descriptions of each of the systems covered by the proposal. No impact assessments were conducted for the three new Commission proposals concerning the European Travel Information and Authorisation System (ETIAS), the European Criminal Record Information System for third-country nationals (ECRIS-TCN system) and the revised mandate for the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), which will manage the centralised systems.

Objectives of the legislative proposal

The **general** objectives of the Commission proposal are to improve the management of the Schengen external borders and to contribute to the internal security of the European Union (IA, p. 15). The IA defines seven **specific** objectives of the proposal. The first four specific objectives, also labelled as 'operational', were derived from 'the report of the high-level expert group[9] and additional follow-up discussions with all stakeholders' (IA, pp. 15-16):
(i) ensuring that end-users, particularly border guards, law enforcement officers, immigration officials and judicial authorities have fast, seamless, systematic and controlled access to the information that they need to perform their tasks, whilst respecting the existing access rights laid down in the respective EU legal instruments;
(ii) providing a solution to detect multiple identities linked to the same set of biometric data, with the dual purpose of facilitating identity checks for *bona fide* travellers and combating identity fraud;

[5] According to the principle of purpose limitation, data is to be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, see Article 5(1)(b) of the General Data Protection Directive.
[6] European Data Protection Supervisor, Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice, 17 November 2017, p. 8.
[7] Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597, European Commission, 24 November 2005, p. 3.
[8] See European Data Protection Supervisor, Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice, 17 November 2017, p. 6; and P. de Hert and S. Gutwirth, 'Interoperability of Police Databases within the EU: An Accountable Political Choice?', *International Review of Law, Computers & Technology*, Vol. 20, Nos 1 and 2, March-July 2006, pp. 21-35, p. 23.
[9] Final report of the high-level expert group on information systems and interoperability, May 2017.

(iii) facilitating identity checks on third-country nationals, on the territory of a Member State, by authorised officers;
(iv) facilitating and streamlining access by law enforcement authorities to non-law enforcement information systems at EU level, where necessary for the prevention, investigation, detection or prosecution of serious crime and terrorism.
In addition, the IA defines three 'ancillary' objectives (IA, p. 16):
(v) facilitating the technical and operational implementation by Member States of existing and future new information systems;
(vi) strengthening and streamlining the data security and data protection conditions that govern the respective systems;
(vii) improving and harmonising data quality requirements for the respective systems.

The general objective combines migration management and security aims, however, as pointed out by the EDPS, repeatedly referring to migration, internal security and the fight against terrorism almost interchangeably brings the risk of blurring the boundaries between migration management and the fight against terrorism.[10] Furthermore, the IA mixes the specific and operational objectives of the initiative.[11]

Range of options considered

To address the objectives defined in the IA, the Commission considers three policy options, including the baseline option. No non-regulatory policy option was proposed.

Option 1: baseline representing the current situation (IA, pp. 16-17)
The baseline under option 1 would consist of the existing (SIS, Eurodac, VIS) and planned or proposed systems (Entry/Exit System (EES), ETIAS, ECRIS-TCN) as defined in the latest relevant legal acts (Commission proposals for ETIAS, SIS, Eurodac and ECRIS-TCN system, adopted legal instrument for EES). The existing Interpol systems[12] and Europol data are also part of the baseline. The IA points out that at technical level, the baseline scenario assumes no interoperability measure is implemented other than the integrated use of VIS and EES, and the common identity repository of EES and ETIAS. According to the Commission, the current silo approach presents Member States and end-users with serious practical and technical difficulties in accessing data to which they legally have access, and in cross-checking relevant data between systems (IA, p. 16; see also p. 12). The Commission, the Council and the European Parliament have therefore rejected option 1 (IA, p. 17).

Option 2: high-level expert group approach to data management for borders and security (IA, pp. 17-22)
Option 2 comprises the following three technical components, as confirmed by the high-level expert group:[13]

- a **European search portal (ESP)**, which would enable the simultaneous search of multiple systems (SIS, Eurodac, VIS, the future EES, the proposed ETIAS, the proposed ECRIS-TCN system; as well as Europol data and Interpol systems) using biographical and biometric identity data. Depending on the purpose of the search, and the corresponding existing access rights, the ESP would be provided with specific configurations;

- a **shared biometric matching service (shared BMS)**, which would enable the simultaneous search of biometric data[14] from several central systems (SIS, Eurodac, VIS, the future EES and the proposed ECRIS-

[10] European Data Protection Supervisor, Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice, 17 November 2017, p. 9; see also E. Guild and A. Baldaccini, *Terrorism and the Foreigner: A Decade of Tension Around the Rule of Law in Europe*, Martinus Nijhoff, 2006.
[11] See Tool #16 of the Better Regulation Toolbox on 'How to set objectives', pp. 100-101; operational objectives are typically option-specific.
[12] Notably Interpol's Stolen and Lost Travel Documents database (SLTD).
[13] See Annex 8 of the IA for more detailed information on the three technical components.
[14] The biometric data include fingerprints and facial images.

TCN system). It would be a key enabler to help detect connections between data sets and different identities assumed by the same person in different central systems. Without a shared BMS, the ESP and the common identity repository would not be able to function as regards biometric data;

- a **common identity repository (CIR)**, which would provide for a unified view on biographical identity data[15] of third-country nationals that will be or are present in Eurodac, VIS, EES, the proposed ETIAS and the proposed ECRIS-TCN system. Each of these systems records or will record biographical data on specific persons for specific reasons. A common repository was proposed as part of the EES/ETIAS proposals to hold common data. This initiative extends it to a CIR that would be the shared component between all these systems to store and search, and potentially enable the linking of identity data.

Neither the ESP, nor the shared BMS, nor the CIR would handle any new data or modify any end-user access rights. This option would envisage concepts for enhanced data quality, such as automated data quality control and a 'data warehouse'. According to the Commission, this option would not generate any additional data protection or fundamental rights concerns as it is 'fully aligned with those legal instruments'.

Option 3: enhanced identity management and streamlined law enforcement access (pp. 22-28)
Option 3 builds on option 2 but includes in addition the following elements:

- introduction of a **multiple-identity detector (MID)**, which would allow checks on whether the biographical identity data contained in the search existed in any of the systems covered by the CIR[16] or in the SIS. This would enable the detection of multiple identities linked to the same set of biometric data, with the dual purpose of facilitating identity checks for *bona fide* travellers and combating identity fraud. The linking functionality would thus no longer be part of the CIR but would be completely covered by the MID. SIS data would no longer be part of the CIR;[17]
- amendment of the rules on the use of EU information systems for **checks within the territory**. This new purpose for the CIR would establish end-user access rights to its data in cases where competent authorities needed to identify a third-country national within the territory;
- amendment of the rules on access to EU information systems for law enforcement purposes by **'flagging' in a two-step approach:** the 'hit-flag' functionality would restrict access to data by limiting it to a mere 'hit/no-hit' notification, indicating the presence (or absence) of data. The end-user performing a search with biographical data or biometric data could search various central systems at the same time while the only results returned would be a 'hit-flag' in cases where this data existed in a particular system. Only in a second step and where considered necessary would the end-user request access to those systems that provided a 'hit-flag', on the basis of existing access rights and conditions.

The IA notes that these complementary elements under option 3 are closely linked to the problem drivers and that the high-level expert group discussed these problems without, however, developing solutions. The Commission also points out that the MID 'is the only possible additional component to achieve interoperability that has been identified as a policy option to consider beyond the technical components of option 2. This new component establishes end-user access rights for those very specific cases where identity fraud or the need for identity disambiguation is detected' (IA, p. 23). The range of options is rather limited taking into account that option 1 (baseline option) was discarded (IA, p. 17), which left two options for consideration. **The Commission's preferred option is option 3** taking into account the costs and benefits, data protection impacts, and feasibility and enforcement (IA, pp. 46-52).

[15] The biographical identity data include last name, first name, gender, date of birth, and travel document number.
[16] CIR covers Eurodac, VIS, the future EES, the proposed ETIAS and the proposed ECRIS-TCN system.
[17] The IA highlights that the CIR in option 2 would become extremely complex and expensive when extracting the biographic data from SIS and migrating this to the CIR. To provide an alternative to not including SIS data in the CIR and not being able to link SIS data with biographical data of third-country nationals, a new component – in form of the MID – would be necessary (IA, p. 23).

Scope of the impact assessment

The IA analyses successively social and economic impacts, the impact on public services, the impact on fundamental rights, in particular under the EU Charter of Fundamental Rights (EU Charter), and safeguards. The Commission considers that 'the major social impact will be the improvement of border management and increased internal security within the European Union. The new facilities will streamline and expedite access by national authorities to the required information and identification of third-country nationals. (...) The new facilities are also expected to generate increased public trust by ensuring that their design and use increases the security of European citizens' (IA, p. 29). The IA notes that the initiative 'is not expected to have a direct impact on a significant number of EU citizens',[18] and that third-country nationals are not directly affected (see, however, the paragraph on the impact on fundamental rights below) (IA, pp. 29-30). The Commission's reasoning is rather general, and the causal link between interoperability, increased security and increased public trust, which the Commission anticipates, appears to lack more concrete explanations and evidence (see also IA, p. 14).

Regarding economic impacts, the IA states that they will be limited to the design, development and operation of the new facilities. The costs will fall to the EU budget and to the Member State authorities operating the systems. The impact on tourism, airports, seaports and carriers is expected to be positive (IA, pp. 30-31). The IA includes cost-benefit analyses for options 2 and 3.[19] Option 3 would be more expensive than option 2 (€169.8 million versus €86.1 million in one-off costs, and €28.5 million per year versus €13.6 million per year in recurrent costs).[20] The benefits would be, however, about €50 million per year higher for option 3 than for option 2. The cost recovery period of option 3 would be of 3.3 years and that of option 2 of 5.5 years (IA, pp. 46-52, see also Annex 4). The Commission admits that there is a lot of approximation about these figures. It would have been useful if the IA had provided the various assumptions upon which the calculations are based directly in the IA (rather than only in Annex 4, pp. 14 and 17).

As far as public services are concerned, the IA considers the impact on border, migration and asylum management, and also on police cooperation and law enforcement, as positive. In particular, police cooperation and law enforcement would benefit from interoperability (notably under option 3) because of consistent identity management across systems through the shared BMS and MID, the identification of third-country nationals within the Member States' territories, and the streamlining of access rules by 'flagging' (IA, p. 32).

In terms of fundamental rights, the Commission views the proposed interoperability measures as 'complementary components to existing systems. As such, they would not alter the balance already ensured by each of the existing central systems as regards their impact on fundamental rights.' The IA admits that 'interoperability does have the potential of having an additional, indirect impact (both positive and negative) on a number of fundamental rights' as enshrined in the EU Charter, including on the right to respect for private life (Article 7), the right to dignity (Article 1), the right to life (Article 2), the prohibition of slavery and forced labour (Article 5), the right to asylum (Article 18) and the prohibition of *refoulement* (Article 19) (IA, pp. 33-34). The question is how the proposed interoperability measures would not alter the existing balance as regards the impact on fundamental rights, while indirectly affecting, if only potentially, core rights enshrined in the EU Charter.

The IA outlines the impact on the right to personal data protection (Article 8) in a prominent, separate 10-page section. The Commission first acknowledges that interoperability has an impact on the right to the protection of personal data and that data protection is closely linked with the right to respect for private and family life. It subsequently examines the proposed functionalities (ESP, the shared BMS, the MID and the streamlining of law

[18] Regarding EU citizens holding multiple nationalities, including a nationality from a third country, the IA states that such persons will not use a third-country nationality to enter or exit the EU (IA, p. 30).
[19] See IA, tables on cost/benefits analyses on pp. 47 and 50.
[20] The text box on p. 52 of the IA wrongly indicates the amount of €14.1 million per year in recurrent costs under option 2; it should read €13.6 million per year in recurrent costs, see table, p. 47 of the IA.

enforcement access via a 'two-step 'hit-flag' approach) against three criteria, including the objective of general interest, necessity and proportionality.[21] The shared BMS and CIR would ensure against duplication of data. The Commission concludes that all comply with the above criteria (IA, pp. 34-44). The IA lists possible safeguards for the new elements under option 3, which 'may in certain ways affect fundamental rights', which are, however, not further discussed. These safeguards[22] include *inter alia* appropriate end-user management by Member States and agencies; appropriate monitoring and evaluation of components and functionalities; appropriate monitoring of accuracies, false-positives and false-negatives of the shared BMS and the CIR; appropriate security measures to protect data; extension of the eu-LISA security plan, business continuity, and a disaster recovery plan (IA, pp. 44-45). More specific information in the IA concerning possible unintended consequences or side effects of the proposed measures, risk management by eu-LISA, but also on the sensitive issue of biometrics (technically, in terms of data errors and legally, in terms of fundamental rights) would have been desirable.[23]

Subsidiarity / proportionality

The main legal bases of the Commission proposal are Articles 16(2), 74, 77(2)(a) and (b), 78(2), 79(2)(c), 82(1)(d), 85(1), 87(2)(a) and 88(2) of the Treaty for the Functioning of the European Union (IA, p. 11). Regarding subsidiarity, the IA highlights that 'key common databases at EU level are in place or in the process of being put in place. Enhanced interoperability among these databases necessarily entails EU-level action. At the heart of the proposal is the improved efficiency and use of centralised systems managed by the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA). By reason of the scale, effects and impact of the envisaged actions, the fundamental objectives can only be achieved efficiently and systematically at EU level' (IA, p. 13). In addition, the IA analyses the EU added value 'from the point of view of EU citizens'. The IA states that EU citizens appear confident regarding the level of cooperation between the police and other law enforcement agencies at national level. A Special Eurobarometer survey on Europeans' attitudes towards security shows that the EU's strategy of sharing information at EU level to combat crime and terrorism has widespread public support: 'almost all respondents (92 %) agree that national authorities should share information with the authorities of other Member States to better fight crime and terrorism' (IA, p. 13). No reasoned opinions from national parliaments have been submitted; the deadline for submission is not indicated at the time of writing.

Budgetary or public finance implications

According to the explanatory memorandum to the proposal the total budget required over nine years (2019-2027) amounts to €424.7 million, covering the following items: a budget of €225 million for eu-LISA; a budget of €136.3 million for Member States; a budget of €48.9 million for Europol; a budget of €4.8 million for the European Border and Coast Guard Agency; a budget of €2 million for the European Union Agency for Law Enforcement Training (CEPOL); and a provision of €7.7 million for the European Commission's DG Home.[24]

SME test / Competitiveness

The IA notes that overall the proposed measures are not expected to have an impact on SMEs (IA, p. 30).

Simplification and other regulatory implications

This initiative falls within the scope of the broader process that was launched by the 2016 Commission communication on stronger and smarter information systems for borders and security, and the subsequent work

[21] The IA notes the importance of a series of principles under the General Data Protection Regulation, such as the principles on data minimisation and purpose limitation in this context.
[22] For an analysis of legal boundaries in the use of databases and biometrics in border surveillance and migration policy, see E. Brouwer, 'Legal Boundaries and the Use of Migration Technology', in H. Dijstelbloem and A. Meijer (eds), *Migration and the New Technological Borders of Europe*, Palgrave Macmillian, 2011, pp. 134-169.
[23] See European Union Agency for Fundamental Rights, Fundamental rights and the interoperability of EU information systems: borders and security, July 2017; see also E. Kindt, *Privacy and Data Protection Issues of Biometric Applications*, Springer, 2013.
[24] See explanatory memorandum, pp. 19-21, for more details.

of the high-level expert group.[25] The Commission points out that the initiative aims to strengthen the existing systems, address gaps by establishing new systems, and enhance interoperability between these systems.[26]

Quality of data, research and analysis

The IA is mainly based on the Commission's 2016 communication on stronger and smarter Information systems for borders and security,[27] the final report of the high-level expert group on information systems and interoperability of 11 May 2017, and three supporting 'feasibility' studies (IA, Annex 2). The high-level expert group (set up in May 2016) comprised experts from Member States and associated Schengen countries, and from the EU agencies eu-LISA, Europol, the European Asylum Support Office (EASO), the European Border and Coast Guard Agency (Frontex) and the EU Agency for Fundamental Rights (FRA). The EU Counter-Terrorism Coordinator and the European Data Protection Supervisor also participated as full members of the expert group. In addition, representatives of the secretariat of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (the LIBE committee) and of the General Secretariat of the Council attended as observers.[28] No academic experts seem to have been included in the high-level expert group. The three feasibility studies dealt with a European search portal, a shared biometric matching service, and a common identity repository. While the IA includes an executive summary of the first study (see Annex 5.1 of the IA), the results of the other studies are not publicly available at the time of writing and it is not indicated who authored these feasibility studies. The IA does not make direct reference to any academic or scientific publications.

Stakeholder consultation

The IA identifies the practical implications of the initiative for different stakeholder groups, including third-country nationals, border, migration and asylum management, law enforcement officers, eu-LISA and IT organisation in the Member States (IA, Annex 4). The Commission conducted a 12-week online public consultation from 27 July to 19 October 2017, which contained 38 questions. The public consultation received, however, only 18 responses.[29] These came from a variety of stakeholders, including from private individuals, Member State governments, private sector organisations and other organisations, such as non-governmental organisations and think tanks (IA, p. 14). According to the Commission, the responses were broadly in favour of the underlying principles of this interoperability proposal. Respondents generally agreed that the issues the consultation identified were relevant, and that the objectives the interoperability package sought to achieve were correct. In particular, respondents considered that the options outlined in the consultation paper would help staff on the ground access the information they needed; avoid duplication of data, reduce overlaps and highlight discrepancies in data; and identify people more reliably and reduce identity fraud (IA, p. 14). Overall, stakeholders appeared to support the initiative. It is unfortunate, however, that the Commission does not provide more detailed information as to which stakeholders favoured which options – neither in the IA itself, nor in the synopsis report in Annex 3 (except for the fact that option 2 is based on the recommendations of the high-level working group).[30] Furthermore, when outlining the results of the public consultation, the Commission speaks of 'a majority of the respondents' or 'several respondents', however it is not clear who these respondents were (or to which stakeholder category they belonged), nor where they came from.[31] In addition, a series of stakeholder workshops were held in 2017 with representatives of Member States and Schengen associated countries, the EU Counter-Terrorism Coordinator, the EDPS, relevant EU agencies, the General Secretariat of the Council and the secretariat and advisors to the LIBE committee, as well as various Commission departments.[32] The Commission further organised a tripartite technical meeting with the European Parliament and Council in November 2017 (IA, Annex 2).

[25] See explanatory memorandum of the proposal, p. 11.
[26] Ibid., pp. 11-12.
[27] COM(2016) 205.
[28] See Annex 1 of the final report of the high-level expert group.
[29] The responses to the public consultation are available online on the consultation website.
[30] The IA merely states that 'respondents generally supported each of the proposed options (...)'(IA, p. 14).
[31] See in this regard the Commission's Better Regulation Guidelines, p. 84, and Tool #55 of the accompanying toolbox.
[32] The Commission organised stakeholder workshops on 27 July, and 6 and 10 October 2017 (IA, Annex 2).

Monitoring and evaluation

According to the Commission, specific mechanisms are in place to monitor the functioning of the ESP, the shared BMS, the CIR, and the MID and evaluate them against the main policy objectives. The IA states that eu-LISA 'should submit' a report on the functioning of the interoperability four years after the functionalities are put in place, and every four years thereafter. In addition, one year after each eu-LISA report, the Commission 'should produce an overall evaluation of the components' (IA, p. 53). The Commission identifies a number of operational objectives and monitoring indicators for the preferred option (option 3). Monitoring indicators include the number of identification checks performed versus the total number of transactions; and the number of detected cases of identity fraud versus the number of linked identities and total number of identities (see IA, pp. 53-54).

Commission Regulatory Scrutiny Board

The Commission's Regulatory Scrutiny Board (RSB) issued an opinion marked 'positive with reservations' on 8 December 2017. The fact that the IA was published on 12 December 2017 might be indicative of the rush in which it was prepared, but also begs the question as to how the substantial comments of the RSB could possibly have been addressed in the final IA report within three working days. The RSB identified 'significant shortcomings': the report should (i) explain how the high-level expert group's recommendations on interoperability were taken into account; (ii) explain in more detail how far the additional measures under the preferred option extend to end-users' existing data access rights in EU information systems and illustrate safeguards for data protection and fundamental rights; and (iii) clarify how option 2 integrates the SIS in the light of possible implications for the effectiveness, cost, and relative merits of that option. The IA does not include a section on how the RSB's comments were addressed, although this is a requirement in the Better Regulation Guidelines.[33]

Coherence between the Commission's legislative proposals and IA

The legislative proposals of the Commission seem to follow the general recommendations expressed in this IA. The monitoring indicators identified in the IA do not entirely match those included in the proposals.

Conclusions

The Commission made an effort to build its case for this initiative, however, the IA displays several weaknesses. The IA would have benefited from clearer problem definition, including indications or evidence regarding the scale of the problems. The range of options is rather limited. The Commission organised a number of stakeholder activities and a public consultation, to which feedback was very limited. The IA is underpinned by the work of the high-level expert group, and also by three supporting studies that are not publicly available at the time of writing. The fact that the IA was published three working days after the issuance of the RSB opinion raises the question of how the substantial comments of the RSB could have possibly been addressed in the final IA.

[33] See Tool #8 of the Better Regulation Toolbox on 'What steps should I follow for an IA?', p. 45.