Brussels,
SEC(2009) 836

COMMISSION STAFF WORKING DOCUMENT

Accompanying document to the

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
establishing an Agency for the operational management of large-scale IT systems in the
area of freedom, security and justice

and

Proposal for a

COUNCIL DECISION

conferring upon the Agency established by Regulation XX tasks regarding the
operational management of SIS II and VIS in application of Title VI of the EU Treaty

SUMMARY OF THE IMPACT ASSESSMENT

{COM(2009) 292 final}
{COM(2009) 293 final}
{COM(2009) 294 final}
{SEC(2009) 837}

1. **INTRODUCTION**

   The Council and the European Parliament, in joint statements attached to the SIS II[1] and VIS[2] legal instruments, invited the Commission to present, following an impact assessment containing a substantive analysis of alternatives from the financial, operational and organisational perspective, the necessary legislative proposals entrusting an agency with the long-term operational management of the Central SIS II and parts of the Communication Infrastructure as well as VIS. The statement attached to the VIS Regulation stipulates that the impact assessment for the operational management of VIS can form part of the impact assessment carried out for the operational management of SIS II. In these statements the Commission committed itself to presenting, within two years of the entry into force of the SIS II and VIS legal instruments,[3] the necessary legislative proposals to entrust an agency with the long-term operational management of these systems.

2. **PROBLEM DEFINITION**

   The Commission is entrusted with the operational management of SIS II and VIS during a transitional period. It may delegate some operational management tasks to national public sector bodies in two different Member States. The legal instruments foresee that the systems shall be located in Strasbourg in France (central units) and near Salzburg in Austria (back-up units). The transitional period should not last for more than five years from the date from which the SIS II legal instruments apply and the VIS Regulation enters into force.

   EURODAC[4] is currently managed by the Commission and as such does not require a change to its management structure. However, a technical assessment carried out in 2005 indicated that EURODAC would need to be upgraded in terms of capacity after the new Member States joined the EU in 2004 and 2007. The biometric matching functionality, in the form of the service-orientated architecture of the Biometric Matching System (BMS), will, in the first instance, be made available for VIS. It is likely to be provided at a later stage for SIS II and EURODAC. Accordingly the operational management solution for EURODAC has also been reviewed in this impact assessment. Combining the systems in a joint Agency could provide opportunities for considerable synergies such as sharing facilities, staff and a common technology platform.

---

[1]   Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) and Council Decision 2007/533/JHAof 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)

[2]   Regulation (EC) No 767/2008 of 9 July 2008 of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).

[3]   The SIS II Regulation entered into force in January 2007.

[4]   EURODAC was established on the basis of Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention.

The systems cannot function without a long-term central operational management authority to ensure continuity, operational management of the systems and the uninterrupted flow of data.

3. ASSESSMENT CRITERIA

The general objective of the Impact Assessment is to establish an appropriate solution for managing the SIS II, VIS and EURODAC in the long-term[5].

The operational management solution will need to take into account the following considerations:

- Guaranteeing that the operational management of the systems will be effective in guaranteeing operational continuity and uninterrupted service (24/7), data integrity and security, and that it is carried out by a public sector body capable of delivering the quality of service required by the users of each system.

- Establishing an operational management and governance structure for SIS II, VIS, EURODAC and possibly other large-scale IT systems in the area of freedom, security and justice that is transparent and accountable to supervisory bodies (European Parliament, Court of Auditors) and to the public at large.

- Ensuring effective control by a heterogeneous set of participating countries (*"géométrie variable"*[6]) and the Commission in their respective roles.

- Ensuring sound, continuous, efficient and accountable financial management for SIS II, VIS, EURODAC, and potentially other large-scale IT systems in the area of freedom, security and justice, which optimises savings and economies of scale achieved through synergy.

- Ensuring that the operational management and governance structures and procedures provide appropriate data protection and/or liability mechanisms whilst acknowledging foreseeable changes resulting from the planned entry into force of the Lisbon Treaty.

4. POLICY OPTIONS

The assessment process consisted of two steps: first, the options were assessed with regard to their legality, acceptance by key stakeholders and ability to deliver effective and accountable operational management for SIS II, VIS and EURODAC. These criteria allowed options to be eliminated or adjusted. Secondly, following this pre-screening process, five possible options to achieve the objective of establishing an appropriate solution for managing the SIS II, VIS and EURODAC in the long-

---

[5] The Impact Assessment was adopted by the Impact Assessment Board in March 2008. Therefore, it does not cover the legal developments after that date.
[6] SIS II, VIS and EURODAC involve both EU Member States and associated countries (Norway, Iceland, and in the future Switzerland and Lichtenstein). At the same time, some of the Member States (UK and Ireland) participate only partly in the systems or on a different legal basis (Denmark).

term were identified and analysed. The possibility of adding other IT systems in the area of freedom, security and justice was also considered.

4.1. Options retained

- Option 1 - "Baseline": the operational management set-up for SIS II and VIS during the transitional phase would be continued as a permanent solution with operational management functions performed by the Commission which would entrust two Member States with operational management tasks. EURODAC's day-to-day operational management set-up would also remain as it is, under the responsibility of the Commission. The Commission would remain responsible and accountable for the operational management of the large-scale IT systems, while the Member States would remain responsible for the day-to-day operational management tasks.

- Option 2 - "Baseline+": the Commission would entrust the operational management of SIS II, VIS and EURODAC to Member States' authorities. This option is therefore very similar to the Baseline option, with one main difference: operational management tasks for EURODAC would also be entrusted by the Commission to the two Member States.

- Option 3 - "a new Regulatory Agency": this would assume responsibility for the long-term operational management of SIS II, VIS, and EURODAC. The agency would be established as a first pillar agency with accompanying acts covering third pillar legal issues. It would become a "centre of excellence" with specialised operational staff. Member States would play an important role controlling the systems as they would be represented in the Management Board of the Agency. The day-to-day management would be carried out by the Executive Director and the Management Board. In order to address issues arising from the different constituencies of the three systems, it is necessary to consider establishing a form of advisory group(s) to support the Management Board on system-specific issues. Depending on the mandate, a Regulatory Agency could be responsible for both the operational management of the existing systems and for the development and for the operational management of other large-scale IT systems as well as for some of the more technical issues covered by the implementing measures in the legal instruments establishing the systems.

- Option 4 - "FRONTEX for SIS II, VIS and EURODAC": would entail changes both in FRONTEX Regulation as well as in its governance structure. Efficient operational management under this option would imply consideration of relocating the systems to the FRONTEX site or to a facility nearby.

- Option 5 - "Europol" (currently) a third pillar agency: would be responsible for managing SIS II and the Commission would manage VIS and EURODAC. The current Europol Convention provisions are not adequate for the operational management of first pillar systems (first pillar elements of SIS II), as the involvement of relevant Community stakeholders (European Parliament, Commission, European Data Protection Supervisor, European Court of Justice) would be very limited.

5.   **COMPARING THE OPTIONS**

For the purpose of this impact assessment, the key legal and political issues, as well as the operational and organisational challenges[7] were evaluated. It is the existence of the systems themselves that may have economic, environmental and, most of all, social impacts. All the IT systems have an impact on problems such as crime, terrorism, security and fundamental rights. However, their operational management mode will not be a differentiating factor between the scales of these impacts.

The following categories of impact criteria were used:

operational – the effectiveness of operational management in dealing with procurement, technological requirements, emergencies, providing services to Member State users;

governance – accountability of operational management and the level of control that the EU institutions and Member States may have over management decisions;

finance – efficiency of operations and ability to assure adequate funding;

legal – legality of the options and availability of guarantees for data subjects and users.

Under each of these categories criteria were applied to determine the expected individual performance of each option, thereby permitting comparison.

5.1.   **Qualitative assessment**

Under each of the criteria, each option has been allocated one to three stars. One star (*) denotes weak, two stars (**) stands for medium and three stars (***) marks a good performance. In addition, in each of the categories of criteria, the most important criteria have been identified, taking into account the tasks of the Management Authority. These criteria have been marked in **bold** in the table showing the results of the assessment. The table below contains the scoring of different options under each impact category.

	Option 1 Baseline: COM entrusting Member States with SIS II and VIS	Option 2 Baseline+: COM entrusting Member States with all	Option 3 New Regulatory Agency	Option 4 FRONTEX for all	Option 5 Europol for SIS II; COM for VIS, EURODAC

	Option 1 Baseline: COM entrusting Member States with SIS II and VIS	Option 2 Baseline+: COM entrusting Member States with all	Option 3 New Regulatory Agency	Option 4 FRONTEX for all	Option 5 Europol for SIS II; COM for VIS, EURODAC
OPERATIONS					
Reliability and quality of service	**	**	***	**	**
Providing adequate management services to Member States' authorities, including specific needs of users (Member States)	*	*	***	**	*
Ensuring flexibility to add other existing and potential new systems	**	**	***	**	*
Capacity to provide the required security levels	**	**	***	**	***
Responsiveness to emergency requirements	*	*	***	**	*
Capacity/flexibility to incorporate new technology and to react to changing demands	**	**	***	***	*
Ability to recruit key skills	**	**	***	***	***
Length of time to develop and implement the option	***	***	*	**	**
GOVERNANCE					
Responsiveness to the requirements	*	*	***	***	*

	Option 1 Baseline: COM entrusting Member States with SIS II and VIS	Option 2 Baseline+: COM entrusting Member States with all	Option 3 New Regulatory Agency	Option 4 FRONTEX for all	Option 5 Europol for SIS II; COM for VIS, EURODAC
and views of Member States, the Commission and the EP					
Transparency (funding, accountability, decision making) vis-à-vis citizens and the systems' users and supervisors	**	**	***	**	*
Effectively adding new Member States	***	***	**	*	*
Responsiveness to the requirements and views of other stakeholders	*	*	***	**	**
Degree to which alignment with JHA policy and broader EU policy is enabled	***	***	***	**	*
Incorporating '*Géométrie variable*'	***	***	***	**	*
FINANCE					
Critical mass: exploiting synergies	**	***	***	***	*
Ability to acquire the right funding levels and resources (running cost)	**	**	***	***	**
Transition costs	***	***	*	**	**

	Option 1 Baseline: COM entrusting Member States with SIS II and VIS	Option 2 Baseline+: COM entrusting Member States with all	Option 3 New Regulatory Agency	Option 4 FRONTEX for all	Option 5 Europol for SIS II; COM for VIS, EURODAC
Access to additional funding for incidental extra costs	***	***	**	**	**
Ability to make necessary investments (OPEX and CAPEX)	**	**	***	**	*
LEGAL					
Effectiveness in ensuring fundamental rights and freedoms, in particular protection of personal data, right to an effective remedy	**	**	***	***	*
Effective liability and redress provisions	*	*	***	***	*
Weight of legal requirements to establish effective management	***	**	*	*	*
Avoiding function creep (de jure and de facto)	**	**	***	**	*

Following this assessment, a new Regulatory Agency and FRONTEX emerge as the preferred options.

5.2.   Quantitative assessment

In terms of quantitative assessment, if the Baseline option were used for executing the tasks of a Management Authority, upgrades (and a possible extension) to the

existing data centre facility at an approximate cost of €4 million would be necessary. If the Regulatory Agency were located in another Member State, there would be a need for new facilities. Should new facilities be purchased to host the Agency, including the systems, the estimated cost could be around €12.6 million. Should the Member State, in order to attract the agency, provide facilities for free, it is very likely that modifications to the buildings costing approximately €4 million would be required.

In terms of running costs, the least expensive option, at €36.1 million per annum, is a Regulatory Agency, if the Member State hosting the new Agency were to provide 1800 m2 of facilities free of charge. The second best option is a new Regulatory Agency, with a cost of €36.6 million a year, if 1800 m2 of new facilities need to be purchased in another Member State. The estimated running costs under the Baseline and FRONTEX options amount to €37.5 million a year.

Operational costs for the SIS II and VIS systems amount to €3.4 million per year. These would occur regardless of the operational management option chosen.

6.   **THE PREFERRED OPTION**

Following the qualitative assessment, a new Regulatory Agency, followed by FRONTEX, emerge as the preferred options. As a result of the quantitative assessment, in case the new Regulatory Agency were to be situated in a new host Member State, the latter, in order to become the location for the Agency, could include the necessary site or even a building free of charge in its bid, making it the most cost-effective option.

In the long term, a Regulatory Agency is most likely to provide the best quality of service to the users of the SIS II, VIS, EURODAC, and for possibly accommodating any other systems in the area of freedom, security and justice. In order to increase the operational base and better justify managerial overheads, the Agency should be made responsible for the development and operational management of the new systems, once the decision on their establishment has been taken by the legislator.

6.1.   **Advantages and disadvantages of the preferred option**

From an operational perspective, the Regulatory Agency would allow dedicated and tailor-made solutions in managing these IT systems. Its primary objective would be to provide the best quality continuous service to the users. Initially the Management Board structure may complicate rapid decision-making, but a new Agency would be able to develop effective mechanisms to deal with emergencies. Although the Agency would comply with EU staff regulations, it could hire more temporary and contractual staff than the internal Commission services. Establishing an agency may prove to be a time-consuming and complex process. Its responsibilities could include some of technical implementing measures set out in the legal instruments establishing the systems which are directly related to the operational management of

SIS II and VIS. The Treaty and the ECJ case law[8] may prevent conferring some of the tasks currently covered by comitology to the Agency.

In terms of governance, a Regulatory Agency facilitates the appropriate representation of users in the decision-making structures. The Commission's role in the Agency, through its presence in the Management Board as well as the influence, in particular on the budget and the work programme, would allow the operational management of large-scale IT systems to be aligned with wider policy objectives. Furthermore, the European Parliament's tasks of democratic control would be ensured by the institutional mechanisms to meet financial and management reporting obligations to which European agencies are subject. The Agency would also provide a visible and dedicated structure, which could prove to be a centre of excellence in fostering an active dialogue with operational constituencies, users and other industry stakeholders. A joint structure would be also more visible and approachable for civil society. The questions of different levels of participation of countries and new users in the three systems could be addressed by putting in place differentiated voting procedures in the Management Board.

Under the financial criteria, a Regulatory Agency may have significant start-up costs, but it would also have the highest potential for exploiting operational synergies and it would be more cost-effective in the long run. Savings would incur in initial capital expenditure and annual (running) costs if systems were managed together. A joint structure would require the hiring of less staff than would be the case if the systems were kept separate. Co-location of network installations would also entail synergies in installations, operational management and monitoring. Furthermore, many of the tasks related to the running of the systems, procurement and project management would overlap for several systems. It is unlikely that a centre of excellence could be achieved for one system alone. Separation of these systems would lead to the opportunity cost of not having achieved synergies in expertise and know-how in large-scale IT systems. The budget of the Regulatory Agency would be dedicated specifically to IT system operational management tasks.

Finally, due to the *géométrie variable*, establishing a Regulatory Agency would require adoption of a legislative package consisting of several legal instruments. This option would ensure that fundamental rights and freedoms are guaranteed by ensuring the appropriate accountability vis-à-vis the European Parliament, the European Data Protection Supervisor, the Court of Auditors, the European Court of Justice and the Commission. An agency option allows a clear separation of technical and operational staff from policy makers and users of the systems, which would contribute to avoiding function creep[9]. The European Court of Justice and the Court of First Instance would have full jurisdiction over the activities of a Regulatory Agency.

---

[8] Meroni & Co. v. High Authority of the European Coal and Steel Community: Cases 9 and 10/56
[9] Function creep - a process by which a system that is designed to perform a certain function is used for other purposes