Statewatch Analysis

SIS II: *fait accompli?*
Construction of EU's Big Brother database underway

- after four years of secret negotiations a host of new functions are being built into SIS II

- new categories of "violent troublemakers", "suspected terrorists" and "visa over-stayers" planned

- EU Visa Information System to share "biometrics platform" with SIS II - fingerprints and photographs to be included - widened access for law enforcement

- European and national parliaments not yet consulted

Introduction

In September 2004 the European Commission signed a €40 million contract with a consortium of IT specialists to build two new EU law enforcement databases: the 'second generation' Schengen Information System (SIS II) and the new Visa Information System (VIS). SIS II and VIS will provide EU law enforcement agencies with a powerful apparatus for surveillance and control with very serious implications for the people who will be registered. In reality, SIS II and VIS will be a single system that is scheduled to go online early in 2007.

The Council has agreed on the scope, function and system architecture of SIS II after four years of secret discussions but – incredibly – has still to consult the European or national parliaments or the wider public on these issues. With the new functionalities already being built into SIS II, the question now is whether there is any possibility at all for democratic input, or whether instead the system is now a 'fait accompli', with the prospect that the Council will try to 'bounce' the European Parliament into a quick decision on the long awaited draft legislation.

This analysis by *Ben Hayes* analyses the development of SIS II, the new functions, the implications for groups and individuals that will be registered, and the decision-making process.

Background: the SIS

The Schengen Information System went online in 1995 between the first seven Schengen member states (France, Germany, Belgium, the Netherlands, Luxembourg, Spain and Portugal). Italy, Austria and Greece joined in 1997 and the

Nordic EU states of Denmark, Sweden and Finland, together with non-members Norway and Iceland, joined 'SIS 1+' in 2000. By this time, the SIS had been incorporated into the EU Justice and Home Affairs framework under the Amsterdam Treaty. The UK and Ireland are the only EU member states not yet participating, though the UK is to be incorporated later this year, with Ireland to follow. SIS II will incorporate the ten new EU member states.

Conceptually, the SIS can be seen as a kind of EU-wide version of the UK's Police National Computer, alerting police officers, border guards and customs officials across the Schengen area to persons and items of interest to one another. Indeed, the incorporation of the UK into the SIS is a direct extension of the PNC – every routine PNC check will automatically check data against the SIS (but because of the UK and Ireland's limited application of the Schengen agreement and refusal to lift internal border controls the two states will not have access to the immigration data in SIS).

Though the SIS and UK PNC both allow persons of 'interest' to be 'flagged', there are crucial differences. The UK PNC contains detailed historical information and identification data, including criminal record data and fingerprints, which maybe used for investigative purposes, whereas the SIS contains only basic information and works on a 'hit/no hit basis'. SIS II is to change all this.

At present, the SIS contains six kinds of alert (record):

- *people wanted for arrest and extradition (Article 95 - 14,023 records)*

- *people to be refused entry to the Schengen area(Article 96 - 780,922)*

- *missing and dangerous persons (Article 97 - 32,211)*

- *people wanted to appear in court (Article 98 - 34,413)*

- *people to be placed under surveillance (Article 99 - 16,016)*

- *lost and stolen objects (Article 100)*

Since 1995 more than 15 million records have been created on the SIS. The vast majority of records concern lost or stolen items (Article 100), and the vast majority of these are lost and stolen identity documents. The latest figures available (June 2003) show that **more than one million records have been created on persons** (877,655 plus 386,402 aliases). The vast majority of these – **780,922 - are alerts on people to be refused entry** (under Article 96), with another 96,663 registered in the other four categories.

There are serious concerns about the SIS, particularly the broad grounds under which people can be registered as "illegal aliens" to be refused entry (art. 96) or for "discreet surveillance" and "specific checks" (art. 99).

Figures published by *Statewatch* in April show that **Italy and Germany are together responsible for more than three-quarters of the Article 96 records**, apparently registering failed asylum-seekers and people who fall foul of immigration rules *en masse*. [1] Many of the people registered on these grounds will not have committed any criminal offence - nevertheless they are now effectively banned from western Europe. The majority of Schengen states have a stricter interpretation of Article 96

and are not registering "illegal" immigrants to nearly the same extent. Is it then proportionate or desirable for all the member states to have to enforce a policy of exclusion pursued by the more zealous among them?

The data protection framework is also cause for concern because there is no guarantee that people can even find out if the SIS contains a record on them (the authorities are given wide-ranging discretion to refuse such requests). If people can not access their data files, then the 'right' to have information corrected or deleted, or to seek compensation, is meaningless. These concerns and others have been well-documented by *Statewatch* and other organisations over the past ten years.

SIS II – a summary

The plans for SIS II are based on a complex series of decisions agreed by the EU Council, its sub-groups and working parties (these are explained below). Together they provide for five critical new functions in SIS II:

> *(i) the addition of new categories of alert;*
>
> *(ii) the addition of new categories of data, including 'biometric' data;*
>
> *(iii) the interlinking of alerts;*
>
> *(iv) widened access to the SIS;*
>
> *(v) a shared technical platform with the Visa Information System.*

These new functions, it is worth stating again, *are already being built into SIS II* and will fundamentally transform the SIS, requiring wholesale amendment of the Schengen Convention. This raises various legal and political issues that should surely have been resolved (or at least debated!) *before* the development of the SIS II got underway, but, as we shall see later, the Council and Commission have conspired to prevent any wider discussion.

SIS II – new categories of alert

SIS II will be

> *"a system that can be expanded progressively with additional functionalities"*

which means that new categories of alert may be created at will. Four new functions have been discussed at length by the officials developing SIS II, though more may be planned. The member states have *already agreed* that one new category of alert will be children to be prevented from leaving the Schengen area. This would presumably apply in kidnap and parental separation cases and is relatively uncontroversial. Not so the new category of **"violent troublemakers"**, which is among the definitive list of new functionalities despite apparent disagreement among the member states. Alerts in this category would be used to prevent 'football hooligans' *and protestors* travelling to events in other Schengen countries where there is a "risk" that they may cause disorder (this would also depend on the enactment of national legislation based on the travel bans currently issued to 'hooligans' by several member states). A third potential new alert would

cover **"suspected terrorists"**, possibly creating a "restricted access terrorist database". However, there is already plenty of scope for including suspected terrorists in the SIS (under articles 96 and 99) and individuals on the proscribed 'terrorist lists' have already been registered (see below). Finally, the common platform with the Visa Information System (described in detail below) raises the possibility that alerts on all 'overstayers' (visa entrants who have not left the Schengen area) will be automatically issued on SIS II. This was discussed in 2001 and reported by *Statewatch* but apparently not discussed since. [2] From an immigration control perspective this is a logical 'dual use' of the two systems and will be a simple technical step (see further below).

SIS II – new categories of data

The personal data that can be held on the SIS is expressly limited under Article 94(3) of the Schengen Convention to six basic fields – (a) name/surname, (b) distinguishing features, (c) initial of second forename, (d) date and place of birth, (e) sex and (f) nationality – together with four categories of information for police officers – whether the person is (g) armed or (h) violent, (i) the reason for the report, (j) the action to be taken.

The "progressive expansion" of SIS II will also allow new categories of data – fields within the alerts/records – **to be added at will.**

The member states have already agreed that **'biometric' data - digitised photographs and fingerprints – are to be included as soon as SIS II is launched**. This must be seen in the wider context of future mandatory biometric registration of the European population. The EU has also agreed that all passport holders, residence permit holders and visa applicants will be photographed and fingerprinted using harmonised technology; something that has long been the case for all asylum applicants (whose data is held in the Eurodac database). Those EU citizens who do not have passports face biometric profiling in national ID card schemes. The upshot is that biometric data for anyone being registered on the SIS/SIS II will soon be available for inclusion in the database.

Moreover, **it has been agreed that in a second stage a biometric search facility will be introduced into SIS II, allowing fingerprints or photographs from crime scenes or suspects to be checked against the database. This will fundamentally transform the role of the SIS**.

At present the system is used to verify that individuals entering an EU member state, or caught up in that state's criminal justice system, are not banned or wanted by another member state.

The new functionalities will allow SIS II to be used as an investigative tool, enabling speculative searches (so-called 'fishing expeditions') in which people registered on the SIS will form a key suspect population.

And there are to be more categories of data. European Arrest Warrants (EAWs) will be issued by the member states as alerts under Article 95 of the Schengen Convention (the SIS has in fact long acted as a *de facto* arrest warrant system). All the information from the EAW form is therefore to be included in SIS II, with the result that at a number of new data fields will be created – maiden name (where applicable); residence and/or known address; languages that the person understands; information relating to the warrant, judicial proceedings and type of

offence (ten categories); other information relevant to the case; and information on related search and seizure orders.

At present, 'supplementary information' such as that in an arrest warrant is exchanged in "standard forms" through the "Sirene Bureaux" *after* a hit on the SIS (Sirene is a dedicated communications system designed for this purpose; the Sirene bureau in the UK is located in the National Criminal Intelligence Service (NCIS)). The inclusion of this additional information *within* SIS II raises two important questions. Firstly, will these additional data fields (and others that may be created for the new categories of alert) apply to all the SIS records by default? What little can be gauged about the design the system suggests that they will. This would expand significantly the amount of personal information held in the SIS. The second question concerns the related issue of including data exchanged through the Sirene bureaux within the SIS database. The terms of reference for the final feasibility study on SIS II were actually expressly amended, *post facto*, to include this possibility. Given that detailed and highly personal information can be exchanged through Sirene, is it at all proportionate to add this data to SIS records?

This step would see SIS II more closely resemble the UK Police National Computer, in which historical data allows the police to 'keep tabs' on suspects.

It is also worth considering the link between SIS II and other planned law enforcement databases. The agreed new functionalities refer expressly to "other biometric data" – likely DNA – which could see the EU return to long-standing ambitions for an EU DNA database. Then there is the proposed EU criminal records database, though this has been shelved at present in favour of a mechanism for the exchange of such data. The fact is that should these should these ambitions find favour in the future, it will apparently be a simple technical step to include them in SIS II.

SIS II – the interlinking of alerts

The interlinking of SIS alerts, which is not currently possible, may appear uncontroversial and even logical. A wanted kidnapper (Article 95) may be linked to a missing child (art. 97), or an arrest warrant on a suspected car thief (art. 95) to a particular stolen vehicle (art. 100) for instance. However, the discussions in the EU have much wider implications. One intention is to link "family members", "gang members" and even "suspected gang members" to one another. Another is to link "illegal immigrants" to be refused entry (art. 96) with their suspected "traffickers" (art. 99). And another is to create links between persons subject to discreet surveillance (art. 99) and wanted persons (art. 95) or those to be refused entry (art. 96).

The Council's list is exhaustive (often providing implausible justifications such as

> "*96-99: husband convicted criminal to be refused entry + wife suspected terrorist"* (!)

The result is that supposition and 'intelligence' will creep steadily into SIS II – 'criminal gangs', 'crime families', 'illegal immigration networks' and, presumably, suspected 'terrorist networks' may even be registered *en masse*.

This is another significant extension of the 'investigative' powers of the SIS and, needless to say, greatly improves the chances of innocent people suffering

serious repercussions as a result of being 'associated' with criminals (or even suspected criminals) and/or specific crimes (even criminal phenomenon).

SIS II – widened access

Access to the SIS is currently 'restricted' to police officers, border guards, immigration officers and customs officials who can *only* check the data relevant to the exercise of their duties. Nevertheless, **there are at least a staggering 125,000 access points to the SIS among the 15 participating states** – so many that EU officials can only estimate. Not only will the ten new EU member states plus the UK and Ireland participate in SIS II, but five new user groups will have access. The negative relationship between data security and the number of people that have access to that data should be cause for concern.

Dedicated legislation on access to the SIS for four new user groups has already been agreed by the Council. [3] These are: (i) vehicle registration authorities, (ii) 'Europol', the European police Office, (iii) 'Eurojust', the EU prosecutions agency, and (iv) national and judicial prosecuting authorities. In addition, access for **internal security and external intelligence agencies** has been agreed *and implemented* informally. With the exception of vehicle registration authorities, who should logically have access to the data on the one million or so stolen vehicles registered in the SIS, the decision to widen access to the SIS is highly controversial.

Europol has long sought access but this had been blocked by several member states until 2003 (the idea of having Europol run the SIS was even floated though now looks highly unlikely). Europol argued initially that it needs the data for its analysis work on 'organised crime', something that clearly falls *outside* the Schengen Convention. The ultimate justification for Europol's access to SIS data is that this is necessary in accordance with Europol's role as a police "information broker" for the member states. However, with 125,000 access points to the SIS, it is surely beyond any credibility to suggest that an EU-level information broker is needed. Europol clearly wants the information in the SIS to use in conjunction with its own extensive *investigative* database. Eurojust and national prosecuting authorities' will also use SIS II for investigative purposes; it is worth stating again that ***the use of the SIS is currently limited to police and immigration checks*. SIS II will be an altogether different proposition with a host of law enforcement and 'security' functions**.

The decision to give the security and intelligence services access to the SIS was apparently implemented following an informal agreement in the EU SIS working party in the aftermath of 'September 11' 2001. Rather than amend the Schengen Convention, which clearly limits access to the SIS to police, border control and customs agencies, it was decided instead to *reinterpret* its provisions. Since the purpose of the SIS under Article 93 is to "maintain public order and security, including State security" **it was decided to ignore Article 101 which expressly precludes widened access to the SIS, and grant access to those authorities with a "responsibility to combat terrorism"**. [4] Whether or not Article 101 has been breached this was surely a matter upon which the European and national parliaments and data protection supervisors should have been consulted.

Just in case anyone else should need access to the SIS, the design of SIS II is such that it will be possible to add new users at a stroke, including

> ***"the possibility to give partial access with a purpose different from the original one set out in the alerts".***

This is a flagrant breach of one of the fundamental principles of data protection – that data may only be used for the purpose for which it was collected – and also clearly prohibited in Article 102(1) of the Schengen Convention.

SIS II and the Visa Information System

The EU Visa Information System is already controversial. EU officials took the decision to develop the VIS in 2002 and in early 2003 decided that it would share a "common technical platform" with SIS II. However, the European Parliament was not consulted until February 2004, and then only on primary legislation that would authorize the Council and Commission to develop VIS from the EC budget (there was no mention of the planned scope and function of VIS or its link to SIS II). Unsurprisingly, **the EP voted to reject the proposal but the Council simply ignored it** (as it often has where justice and home affairs (JHA) policies are concerned) and went on to adopt the VIS Decision in June 2004, in time to award the contract for the development of SIS II and VIS in September.

The Council adopted the VIS decision by *qualified majority vote* (QMV), taking advantage of the changes to EU decision-making procedures in the JHA structure that came into affect on 1 May 2004 (under QMV votes are weighted so larger member states have a bigger say). However, the EP should then have had "co-decision" and the power to throw out the proposal (this is the *primary* condition under which QMV is introduced).

The VIS Decision was an outrageous manipulation of the decision-making procedures set out in the Amsterdam Treaty: neither the European nor national parliaments could feasibly intervene (the EP was only consulted (and ignored) and member states with parliamentary scrutiny reserves (or other reservations) could simply be outvoted). The legal basis for the development of VIS is very shaky indeed.

VIS will contain all the data from every visa application to every EU member state – whether the application is successful or rejected. All visa applicants will have to provide the two forms of biometric data – digitised photos and fingerprints – and this too will be stored in the VIS. This is one of the motivations for developing VIS and SIS II together, the Commission Working Party on SIS II having decided in March 2003 that this would:

> *"provide for one secure location, one Business Continuity System (BCS) and one common platform. Moreover, it could yield a two digit million € saving.* ***The biometrics platform (which is expensive) could be paid for under VIS****. Some other synergies might be found at end-user level, planning, maintenance & support, efficient use of systems and networks interoperability." [6]*

The Council maintains that that

> *"the VIS and the SIS II will be two different systems with strictly separated data and access".*

In reality, a **"centralised architecture" and a "common technical platform" is a**

convoluted way of describing a single computer system. "Interoperablility" between databases (more spin) is "institutional speak" for the integration of those databases – either the data sets, or access to them. The Council has already agreed that there will be broad law enforcement access to VIS (including access for the security and intelligence services), providing, in conjunction with SIS II, an EU-wide fingerprint database of wanted persons, suspects and *all* visa entrants.

It is worth remembering here that 'biometrics' are also to be introduced into *all* travel documents – EU passports, residence permits as well as visas – and that this data too is to be stored in future in a central EU database. What price then a "common technical platform" and "interoperability" with SIS II/VIS for the future biometric EU population register?

The Decision-making process

The SIS II is beginning to resemble a 'dream come true' as far as law enforcement is concerned – a dream that will be a technical reality in a little over a year – and this is a suitable description of the decision-making process. The design of SIS II began in earnest in 2000 with the Article 36 Committee's decision to draft a 'wish list' of all possible "future functionalities". The mandate for the EU Working Party (WP) on the SIS, which drafted the list, expressly provided for ***requirements not agreed upon by all delegations***. [7] The representatives of the interior ministries and national police forces that sit in the SIS WP took three years to finalise the list, taking full advantage of their mandate.

The JHA Council of June 2003 adopted the list of "new functionalities for SIS II" in the form of binding Council Conclusions – meaning no consultation of the European or national parliaments. [8]

The 'wish list' (which was dissected in the analysis above) was then divided into three categories (i) agreed new functions, (ii) "functions on which full to wide-ranging agreement exists" and (iii) functions in which "a certain interest exists". **Despite the evident *disagreement* among the member states, the list was considered a "definite list of functionalities" and *all* were to be included in the call for tender to build SIS II.** In June 2004, more Council Conclusions added more new functionalities and these were included along with all the others in the detailed blueprint for SIS II given to the contractor. [9]

With the development of SIS II now well underway it is astonishing that the European and national parliaments, the Schengen Joint Supervisory Body on data protection and the wider public have not yet been consulted on the new functionalities. Both the EP and JSA have protested – rather meekly it has to be said, though such are the limitations of their powers – but both have been ignored. The Council first promised to conduct a "legal review" of the proposed new functionalities in 2001 but is yet to produce anything; the same is true of the Commission – despite the fact that wholesale amendment of the Schengen Convention is necessary to implement the new functions. To justify the exclusion of the EP, JSA and other interested parties, EU Council officials have invented the wholly untenable concept of "latent development", meaning the "technical pre-conditions" for all the new functions on the Council wish list will "be available in SIS II from the start, but those functions would only be activated once the political and legal arrangements are in place". [10]

This is entirely prejudicial to future decision-making – what if the European or national parliaments or data protection commissioners object to the new functionalities? They can hardly be un-built.

Last Autumn the European Commission stated that it would propose the substantive legislation on SIS II by the end of the year (2004): this is now over four months late. What little time that remains for what passes for 'democratic debate' in the EU clearly prejudices the decision-making process. The Council now has little alternative but to 'bounce' the European Parliament into a quick decision on the legislation if it is to meet its own schedule for the implementation of the new system. It might even be argued that the actual development of new functionalities in SIS II amounts to a breech of the express limitations on the scope and function of the SIS set out in the Schengen Convention (therefore breaching the EU Treaties). Regardless, **its development should surely not have been authorised until the EP had been consulted on the new functions and the crucial legal and political arguments had been resolved (or at least discussed!).**

At the time of writing, it also remains to be seen if the long awaited legislation will be 'substantive' and set out in detail all those new functions and data sets discussed above. Discussions on the future "strategic management" on SIS II propose that this responsibility should fall to a Management Board in the Council framework and deal with such issues as "how to integrate new functionalities". [11] It is quite possible then that some of the new functionalities will remain "latent" until such a framework is contrived to allow them to be implemented in future by the Council subject only to minimum standards of accountability (such as the consultation procedure).

Executive powers

Finally, it must be pointed out that it is the European Commission which is responsible for the development of SIS II under the 2001 Regulation authorising funding from the EC budget. [12] In practise however, the Council has restricted almost all of the Commission's executive powers over SIS II, taking all the key decisions and imposing an extremely restrictive and unusual form of what the institutions call "comitology". [13] The dual "regulatory" and "management" procedures involved mean that the same small group of police and interior ministry officials representing the member states in the Council framework take all the key decisions in the Commission's SIS II Committee. **The dual procedure is a clear breach of the EU's "comitology" rules and a highly questionable way of implementing EC Acts. The same procedure is being used to develop VIS**. [14]

There is nothing unusual about the Council restricting the Commission's powers and extending its own where justice and home affairs matters have been transferred from the (EU) "Third Pillar" to the (EC) "First Pillar". The same thing happened with the Schengen Border Manual and Common Consular Instructions, which, like the SIS, have a clear legal basis in Title IV EC ("Visas, Asylum, Immigration and other Policies related to Free Movement of Persons"). The justification is that these are politically "sensitive" issues for the member states that can not be entrusted to the Commission. This is often presented as a matter of principle relating to 'national sovereignty'.

However, the executive powers that should arguably be the preserve of the Commission have simply been granted instead to the General Secretariat of the EU Council – the issue of 'sovereignty' is a 'red herring'. In the case of SIS II, it is

clear that this body, headed by Mr. Solana (the Secretary-General), has **played a huge part in shaping the informal decisions on SIS II that bring us to this point**.

Another one of these informal decisions appears to have granted the Council General Secretariat itself access to the SIS with no apparent justification! More recently, a situation has arisen in which the power for the General Secretariat to add names to the SIS, following agreement in the Council, is a distinct possibility. The justification is the EU 'terrorist lists'. These have been agreed by the EU but the individuals named in the lists can not be added to the SIS by the EU, since only the member states have the power to create records (and because the legal liability for incorrect or inaccurate records must rest with the state that created them). In another informal decision Germany has simply added all the names on behalf of the other member states (a single alert covers the entire Schengen territory); in future it is proposed that the General Secretariat should be given the power to add names on behalf of the EU.

The way in which the Council has, aided faithfully by the Commission, managed to develop SIS II without any democratic debate whatsoever is a formidable achievement. It also demonstrates, so convoluted is the five-year conspiracy, that the Council itself – i.e. the General Secretariat – appears to have exercised at least as much influence over SIS II as any single member state. Access to the SIS, the power to add records to the SIS, and formal responsibility for the "strategic management" of SIS II (something it already enjoys in practise) will consolidate this role.

Conclusion

This analysis required painstaking research into the activities and the Council and the Commission, neither of which are at all clear from the information made public by these institutions. The deliberate shielding of this information has prevented parliamentary scrutiny and public debate around the development of SIS II and flies in the face of the EU's commitment to openness, democracy and human rights. Instead, the equally deliberate circumvention of the democratic process now threatens the human rights of those individuals who will be registered in SIS II/VIS. This system will be used to exclude millions from EU territory, to exercise surveillance and controls on the suspect population (mainly immigrants), and to create a biometric register of *all* entrants to the EU, not dissimilar to the "US Visit Program" (if much less well known).

In 1999, Thomas Mathiesen's seminal study on the SIS (published by *Statewatch*) concluded:

> ***The likely development towards a more or less integrated, totalised registration and surveillance system in Europe implies a development towards a vast "panoptical machine" which may be used for registration and surveillance of individuals as well as whole categories of people, and which may well become one of the most repressive political instruments of modernity.***

The "latent development" of SIS II is testimony to this prescient warning.

Ben Hayes
May 2005
Statewatch

Footnotes
[the links in this pdf are "live" and can be accessed by clicking on the url]

---

[1] 'Three-quarters of a million "illegal aliens" banned from Schengen area', *Statewatch News Online*, April 2005:
http://www.statewatch.org/news/2005/apr/08SISart96.htm

[2] 'EU plans to extend the Schengen Information System', *Statewatch News Online*, November 2001:
http://www.statewatch.org/news/2001/nov/19sis.htm

[3] Regulation 871/2004/EC of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, (OJ 2004 L 162/29):
http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_162/l_16220040430en00290031.pdf
'Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism':
http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2005/l_068/l_06820050315en00440048.pdf
draft 'Regulation of the European Parliament and of the Council amending the Convention implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at common borders as regards access to the Schengen Information System by the services in the Member States responsible for issuing registration certificates for vehicles', COM (2003) 510 final, 21.8.2003:
http://europa.eu.int/eur-lex/en/com/pdf/2003/com2003_0510en01.pdf

[4] See 'From the Schengen Information System to SIS II and the Visa Information (VIS): the proposals explained', *Statewatch* analysis, January 2004, first published on the SEMDOC website: http://www.statewatch.org/news/2005/may/analysis-sisII.pdf

[5] 'Council Decision of 8 June 2004 establishing the Visa Information System (VIS)':
http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_213/l_21320040615en00050007.pdf
European Parliament report on the Commission proposal for a Council decision establishing the Visa Information System (VIS)':
http://www.statewatch.org/semdoc/SEMDOCdocbin04/0262-04.pdf

[6] Minutes of the meeting of the European Commission SIS II Committee, 24 March 2003.

[7] Council doc. 8587/00, 17 May 2000 (not published by Council).

[8] Conclusions on the 'development of SIS II', Council doc. 9808/03, 25 May 2003, adopted by the JHA Council on 5-6 June 2003:
http://register.consilium.eu.int/pdf/en/03/st09/st09808en03.pdf.

[9] Conclusions on 'SIS II functions', Council doc. 10125/04, 3 June 2004, adopted by the General and Foreign Affairs Council of 14 June 2004:
http://register.consilium.eu.int/pdf/en/04/st10/st10125.en04.pdf.

[10] 'Summary of [SIS working party] discussions', Council doc. 6387/03, 25 February 2003: http://register.consilium.eu.int/pdf/en/03/st06/st06387en03.pdf

[11] 'Parameters, procedures and time schedule for decisions on the strategic management of SIS II', Council doc. 12888/04, 4 October 2004:
http://register.consilium.eu.int/pdf/en/04/st12/st12888.en04.pdf

[12] Regulation 2424/2001/EC on the development of the second generation Schengen Information System (SIS II), OJ 2001 L 328/4:
http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_328/l_32820011213en00040006.pdf
Council Decision 2001/886/JHA on the development of the second generation Schengen Information System (SIS II), OJ 2001 L 328/1:
http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_328/l_32820011213en00010003.pdf

[13] See Council and Commission statements on competence over decisions relating to SIS II, Council document 14535/01, 4 December 2001:
http://register.consilium.eu.int/pdf/en/01/st14/14535en1.pdf

[14] Council conclusions (19 February 2004) on Visa Information System, 5831/04 (Presse 37) [see pp.15-20]:
http://register.consilium.eu.int/pdf/en/04/st05/st05831.en04.pdf