Council of the
European Union

Brussels, 21 November 2014
(OR. en)

15701/14

JAI 897
DAPIX 175
CRIMORG 109
ENFOPOL 372

"I/A" ITEM NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee/Council
No. prev. doc.:	11153/2/14 REV 2
Subject:	Draft Council Conclusions on an updated Information Management Strategy (IMS) for EU internal security

1. On 30 November 2009, the Council approved Conclusions on an Information Management Strategy (IMS) for EU internal security[1]. The Strategy as such has a long-term focus and can be further developed and updated as the overarching vision develops. Therefore, the Strategy was approved by the Council in 2009 on the understanding that it should be reviewed by the end of 2014.

2. The IMS aims at supporting, streamlining and facilitating the management of information necessary for carrying out expedient cross-border information exchange between law enforcement authorities, authorities responsible for border management and judicial authorities dealing with criminal matters. The IMS provides guidance on how to translate business needs into structures and content, and contained under a number of focus areas the strategic goals to be achieved.

[1] Document 16637/09 JAI 873 CATS 131 ASIM 137 JUSTCIV 249 JURINFO 145

3. The Strategy was complemented by an action list/road map defining concrete goals, processes, roles and deadlines. So far three action lists with a life-span of 18 months each were issued. The 2nd Interim Report on the Implementation of the IMS Action Lists[2] outlines the objectives and results achieved so far.

4. DAPIX discussed the assessment and review of the strategy at its meetings on 1 July and 23 September. Delegations recommended to clearly distinguish between the strategy as such, the implementation at national or EU level and the setting up of further action lists. Discussions concluded that the Strategy was deemed a sufficiently robust instrument which should be re-affirmed subject to some updates. However, as to the implementation of the Strategy by means of action lists, delegations asked for more commitment of the actors involved and a focus on practical results, operational and coordination issues.

5. Consequently, the Presidency suggested to draw up Council Conclusions on an updated EU Information Management Strategy (IMS) for EU internal security that take account of the work done in this field over the last five years.

6. DAPIX examined the proposal and agreed on the draft Council Conclusions at its meeting on 19 November with a scrutiny reservation from UK.

7. Coreper is therefore requested to invite the Council to approve the draft Council Conclusions on an updated Information Management Strategy for EU internal security, as set out in Annex.

[2] Document 13032/14 JAI 663 DAPIX 111 CRIMORG 76 ENFOPOL 260

ANNEX

DRAFT COUNCIL CONCLUSIONS

ON AN UPDATED INFORMATION MANAGEMENT STRATEGY (IMS)

FOR EU INTERNAL SECURITY

THE COUNCIL OF THE EUROPEAN UNION,

RECALLING

– the Hague Programme on strengthening freedom, security and justice in the European Union[3], in particular section 2.1, calling for improved exchange of information to fight crime, established the principle of availability for cross-border information exchange and specified that "the methods of exchange of information should make full use of new technology and must be adapted to each type of information",

– the European Council's acknowledgement in the Stockholm Programme of the need for coherence and consolidation in developing information management and exchange, inviting the Council to adopt and implement an EU Information Management Strategy, entailing business driven development, a strong data protection regime, interoperability of IT systems and a rationalisation of tools as well as overall coordination, convergence and coherence,

– the Conclusions of the European Council of 26/27 June 2014[4], in particular Chapter 1 on Freedom, Security and Justice, where it is stated that "In its fight against crime and terrorism, the Union should back national authorities by mobilising all instruments of judicial and police cooperation, with a reinforced coordination role of Europol and Eurojust, including through the improvement of cross border information exchange, including on criminal records."

[3] Document 16504/04 JAI 559

[4] Document EUCO 79/14 CO EUR 4 CONCL 2

TAKING INTO ACCOUNT

– the Council Conclusions on intensifying the implementation of the "Prüm Decisions" after the deadline of 26 August 2011[5],
– the Council Conclusions on the implementation of Council Framework Decision 2006/960/JHA ("Swedish Framework Decision")[6],
– the Council Conclusions on further enhancing efficient cross-border exchange of law enforcement information[7],
– the European Commission's Communication of 7 December 2012 on the European Information Exchange Model (EIXM) and the Council Conclusions thereon[8], in particular with regard to the task to further discuss the automation of existing data exchange processes in the framework of the Information Management Strategy (IMS);

UNDERLINING

– that the strategic goal of the future renewed EU Internal Security Strategy (ISS) to strengthen a comprehensive and coherent approach in the fight against trans-national crime and terrorism through, in particular, access to, availability and exchange of information, will be supported by further aiming at interoperability of systems and enhancing and simplifying existing tools for cross-border law enforcement information exchange, in compliance with existing data protection legislation;

[5] Document 17762/11 JAI 892 DAPIX 163 CRIMORG 233 ENFOPOL 441 ENFOCUSTOM 160

[6] Document 15277/11 JAI 714 DAPIX 129 CRIMORG 176 ENFOPOL 346 ENFOCUSTOM 115 COMIX 719

[7] Document 10333/12 JAI 356 DAPIX 65 CRIMORG 57 ENFOCUSTOM 43 ENFOPOL 147

[8] Document 9811/13 JAI 400 DAPIX 82 CRIMORG 76 ENFOCUSTOM 88 ENFOPOL 146

TAKING INTO CONSIDERATION

- that the Council Conclusions on an Information Management Strategy (IMS) for EU internal security[9] were approved by the Council on the understanding that the Strategy has a long-term focus and could be further developed and updated and therefore should be reviewed by the end of 2014,
- that the Strategy was complemented so far by three action lists with a life-span of 18 months each which defined concrete goals, processes, roles and deadlines,
- that the Strategy was deemed a sufficiently robust instrument which should be re-affirmed subject to some updates,
- that in view of the objectives and results outlined in the 2nd Interim Report on the Implementation of the IMS Action Lists[10], the further implementation of the Strategy requires a stronger commitment of the actors involved both at national and at EU level, as well as a focus on practical results, operational and coordination issues,
- that euLISA started operations on 1 December 2012 aiming at providing viable, long-term solutions for the management of large-scale IT systems and gradually developing into a center of excellence,
- that the volume of cross-border information exchange has increased over the past years and Member States are expecting this to continue, something that can be mitigated by the efficient use of modern technology, e.g. automation, as well as the streamlining of routines and workflow;

[9] Document 16637/09 JAI 873 CATS 131 ASIM 137 JUSTCIV 249 JURINFO 145

[10] Document 13032/14 JAI 663 DAPIX 111 CRIMORG 76 ENFOPOL 260

RECOGNISING THAT

– Effective and secure cross border exchange of information[11] is a precondition to achieve the goals of internal security in the European Union.

– The tasks of internal security (the "business" side) are divided across a range of authorities depending on national structures, competences and legal frameworks and this division is different from one Member State to the next.

– Information management across sectors provides for the multidisciplinary approach needed to develop an Area of Freedom Security and Justice, notably the potential of enhanced information exchange and closer cooperation between all the parties involved in order to increase efficiency in the fight against cross-border crime.

– With regard to the widely split landscape of cross-border information exchange, Member States have expressed at several occasions the priority for a coherent and consolidated implementation of existing instruments and arrangements rather than embark upon new initiatives.

– The need for a coherent and effective cross-border approach is exacerbated by the growing mobility of citizens, the increasing complexity of crime phenomena and hence the EU policies to counter them, as well as by the necessity for the EU and the Member States to maximise their resources.

– Citizens require that privacy would appropriately be balanced against their expectations of security.

[11] *In this context, information means information and intelligence required by the competent national authorities and available to them under the relevant regulatory framework for the objective of improving the EU internal security of the EU citizens.*

UNDERLINING THAT

– the Strategy aims to provide guidance on how to ensure a supply of information that takes account of both business needs and the rights of the individual,

– the Strategy aims to define the preconditions for the professional, business driven and cost effective development and management of IT,

– the Strategy aims to show the way towards a structured information exchange and forms a basis for enhanced decision making processes and governance;

WELCOMING AND ENCOURAGING

– the work on the technological modalities of cross-border information exchange and, in particular, the progress made on the Universal Message Format (UMF) for an enhanced structured information exchange across borders, and
– the further development of the Universal Message Format (UMF) as one of the key elements of the EU information exchange architecture as set out in the UMF 2 Final Conference Conclusions[12],
– the work on-going on interoperability and further synergy of systems, and automation of information exchange;

HEREBY RESOLVES

To re-affirm and further implement the Information Management Strategy (IMS) with a view to supporting, streamlining and facilitating the management of information which

a) is based on the following principles:

[12] Document 10158/14 DAPIX 69

– information management in the area of freedom, security and justice is an essential tool to implement the objectives of increasing EU internal security and protecting its citizens,

– cross-border law enforcement information exchange has to strike a balance between business needs and the safeguarding of citizens' fundamental rights,

– priorities set for information management and exchange must correspond to political, policy and operational priorities and support the business vision on how to implement the above-mentioned objectives,

– data protection, data security and data quality have always to be respected,

– IT development and management have to be professional, business driven and cost effective,

– information management is functionally defined, i.e. depends on the task to be carried out, as opposed to competence-based or organisationally defined,

– information management must provide for the multidisciplinary approach needed to develop an Area of Freedom, Security and Justice;

b) consists of focus areas grouped under the following headlines and elaborated in annex:

I. Needs and requirements

- Needs, requirements and added value are assessed as a precondition for development
- Development follows agreed law enforcement workflows and criminal intelligence models
- Development supports both data protection requirements and business operational needs

II. Interoperability and cost efficiency

- Interoperability and co-ordination are ensured both within business processes and technical solutions
- Re-utilisation is the rule

III. Decision-making and development processes

- Member States are involved from the very start of the process
- There is a clear responsibility for each part of the process, ensuring competence, quality and efficiency

IV. Multidisciplinary approach

- Multidisciplinary coordination is ensured within the JHA area

To take the necessary steps to develop and update as necessary detailed future action plans with realistic time horizons and a focus on practical results in order to fulfil the overall aims and objectives of this Strategy.

INVITES

– preparatory bodies of the Council dealing with issues of information exchange and IT development to further implement the strategy
– EU officials and Member States representatives and experts in EU structures and agencies to take account of the strategy in their work preparing decisions, including on information exchange on a bilateral or regional level and with third countries or organisations, as well as preparing and running programmes and projects for information exchange and IT development
– Member States to support the common efforts at EU level by adopting the strategy at national level as guideline for policy makers and other decision makers in their competent authorities when dealing with issues related to or influenced by international information exchange and IT development (including "national housekeeping" and dealings with third countries or organisations).
– the Commission to apply the methodology agreed upon in these Conclusions when further elaborating its European Information Exchange Model (EIXM) and to ensure adequate funding for actions needed to further implement this Strategy.
– the Commission to examine the possibility of consolidating and increasing the efficiency of existing legislation on law enforcement information exchange.

I. Needs and requirements

1. Needs, requirements and added value are assessed as a precondition for development.

This focus area sets out the requirement for an assessment of added value before any new information exchange is established. It also reflects the vision of the availability of information based on purpose, necessity and proportionality.

It will require an assessment of the business needs as well as business and legal requirements for the concerned co-operation, including how the solutions will be used, and how useful they will be for enhancing the actual operational co-operation and working methods.

As a consequence, development will be based on and driven by the needs and requirements of the authorities involved. An assessment of usefulness (including cost/benefit analysis) will also help to set priorities for development.

This means that:

when initiatives regarding information exchange or technical solutions are put on the agenda, end-users and the management level in different areas need to be involved. Without their support it is impossible to assess the importance and value of an initiative. Their participation is also relevant when it comes to clarifying the balance between data protection and business needs;
ideas or discussions regarding technical solutions have to be subordinated to the analysis of needs and requirements;
work on legislative instruments and/or pre-studies for technical solutions should not start before the business requirements are identified and documented;
any initiative in the field of information exchange has to be based on an in-depth analysis of existing solutions on EU level and in the Member States, the definition of needs, requirements and the added value as well as assessment of legal, technical and financial impact of the new initiative;
clear assessment criteria, supported by systematic evaluation programmes should be developed;
assessment of the usefulness in developing for example specific information types should derive from a strategic prioritisation process;

2. Development follows agreed workflows and criminal intelligence models.

Improving the exchange of information relies heavily on support from IT solutions. For IT to support information exchange, it has to support the business processes of international law enforcement co-operation.

Business processes must allow the quick, efficient, user friendly and cost-effective exchange of information and criminal intelligence. The work flows must therefore be described, known and accessible. They should be an integral part of the work to develop and procure systems. As a consequence, there will be better management and documentation of development and the needs of international law enforcement co-operation will steer development.

This means that:

work on the existing Common Requirements Vision (CRV) should be complemented by analyses of substantial requirements, made together with and by national authorities;
an ”information map” should continuously provide an overview of business processes and the corresponding information flows of international co-operation, so as to identify on that basis the interfaces at which harmonisation is needed.

3. Development supports both data protection requirements and business operational needs.

Cooperation with a view to ensuring the EU internal security places high demands on data protection and/including data security. Personal privacy as well as business security have to be ensured, while providing for business needs to use and share information.

A high level of security will protect business interests as well as citizens' private lives, without reducing the availability of information, so that correct information is available to authorised users in a traceable way, when needed and permitted by existing legislation. Adequate use of modern technologies, but also adaptation of business processes and measures to implement data protection, facilitate this. Enhanced trust in these areas between competent authorities is an important step towards an attitude of data-sharing by default.

This means that:

the legal requirements for protection of personal data and for security standards must be assessed together with business needs for use and exchange of information, so that the right levels of business and technical security standards are ensured for information exchange and IT systems;
data collection must be well targeted, in order to protect personal privacy as well as to avoid information overflow for the competent authorities and facilitate efficient control over the information;
data security is a precondition of data protection and must be ensured through organisational as well as technical means;
the different tools, such as applications and support tools, must be rationalized with a view to simplifying the work of the competent authorities and the end users; this will minimize the risks of damage, as will training about the available tools and their use;
adequate measures to implement data protection must provide for proper and regular operational checks and ensure that appropriate sanctions are effectively applied in the event of any breach;
systematic evaluation and monitoring mechanisms should be developed to assess the quality and the effect of data protection measures.

II. INTEROPERABILITY AND COST EFFICIENCY

4. Interoperability and co-ordination are ensured both within business processes and technical solutions.

Interoperability concerns multiple levels, such as legal, semantic, business and technical levels. Interoperability is both a prerequisite for and a facilitator of efficient information exchange. Interoperable solutions and capacities build on initiatives and proposals that start from business needs and requirements.

Technically, IT solutions and their components should comply with commonly agreed standards and principles. Standard solutions should be used and kept to a minimum.

Their use will provide greater coherence both in the development and management of solutions.

This also supports interoperability and co-ordination between systems. As a consequence, there will be better and increased use of existing solutions, and IT systems will be able to support larger parts of work processes. The need for double storage and double registration will decrease and the IT support will become more user-friendly. By applying commonly agreed standards, information exchange can be supported by several suppliers rather than a few, minimizing dependence on special suppliers. In the long run it will also decrease the cost of adaptation in Member States.

This means that:

the "information map" should include a comparative overview of EU and Member States legal situation in the area of information exchange;
the [proposed] European interoperability strategy should be applied;
existing, commonly agreed, accreditation/standardisation functions should be used;
integration enablers, such as standard technologies and capabilities, which facilitate integration and are designed to provide security, scalability and performance, should be identified;
measures to implement data protection should be coordinated at and between both the EU and national levels.

5. Re-utilisation is the rule

Development means high costs and considerable investment, but also long-term costs for management, maintenance and support. Normally, only a small part of the total cost is used for the development phase. This is not an issue only for technical development, but also a question about not creating new legal bases or practical arrangements, when existing ones can be used or extended.

As a consequence, sharing and re-utilisation of sustainable solutions must be a priority for development and technical improvement. Re-utilisation helps to avoid parallel solutions and to further develop existing instruments and systems, their integration and usefulness. As a consequence, there will be increased use of past investment and less need for new investment. The time necessary for development will also decrease the more components are at hand.

Efficient re-utilisation requires an “information map”, providing an overview of existing information flows, functions and components. Efficient (re-)use of successful solutions also requires a constant evaluation process and a follow-up mechanism for assessing how the exchange of information operates.

This means that:

the “information map” should include information flows, functions and solutions;
an evaluation mechanism that is pragmatic, relevant and resource-effective must be presented. It should be purpose- and not competence-based; it should not be limited to certain (legal) instruments and it should be ensured that lessons learned from evaluation can be implemented;
to assess the impact of its work, the EU must create tools to measure not only criminal activity but also the effects of its efforts to combat criminality;
a model of how to share and re-use sustainable solutions should be produced taking account of practices from within the EU but also from third countries;
a critical review of existing instruments in use for information exchange should assess their efficiency and effectiveness in order to allow for a rationalisation and certainly before starting to develop new tools.

III. DECISION MAKING AND DEVELOPMENT PROCESSES

6. Member States are involved from the very start of the process.

Decisions at EU level about cooperation, information exchange and IT development have a substantial impact, in a short as well as a lifecycle perspective, on Member States' business processes, structures, investments and budgets. A fully functional end result requires intensive coordination at national level as well as reciprocity and interaction between the national and EU levels.

Member States' authorities, which are responsible for national implementation of workflows, methods and development have to be involved from the beginning of the development processes at European level. To be able to contribute fully, Member States should work on their own interoperability, both business and technical, and establish their own development processes.

This means that:

national and EU information management strategies or policies should be in line with each other;
end-users and key stakeholders should be involved at both the national and EU level;
authorities in Member States need to identify and develop their own development processes.

7. There is a clear responsibility for each part of the process, ensuring competence, quality and efficiency.

In order to better steer the development process, the roles and responsibilities of the actors involved must be clarified. Special competences are needed in different areas, such as business and technical architecture, methods and models, management, finance and control. Discussions about (technical) solutions must be kept on a level with the right technical and architectural competence. Decisions on management and political levels have to address the appropriate issues for that level.

This means that roles must be identified, responsibilities defined and structures set in place to ensure that all parties concerned are involved at the right level and at the right stage of the process, but also that there is overall coordination and coherence.

This means that:

roles and competences on different levels (within existing or planned national authorities, EU institutions, bodies and agencies etc.) must be identified and organised;
functions to prepare the strategic decisions on information management and IT development have to be identified/established;
functions for management, further development and evaluation of (business and technical) solutions must be in place.

IV. MULTIDISCIPLINARY APPROACH

8. Multidisciplinary coordination is ensured.

The current Information Management Strategy aims to support, streamline and facilitate the management of information necessary to the competent authorities to ensure the EU internal security. In practice, the authorities concerned will be essentially law enforcement authorities and judicial authorities dealing with criminal matters but information exchange with other authorities and sources is also necessary. The Information Management Strategy recognises and caters for this multi-disciplinary approach to achieve the above-mentioned goals and to facilitate the transfer and re-utilisation of information, independently of the body holding the information. Modern technology makes it possible to achieve the desired level of availability, which in turn can minimize disruption and manual re-registration and increase the quality of information. The same technology makes it possible to maintain or increase the level of data protection, including data security.

The strategy aims to facilitate the functionalities and technicalities of information exchange between relevant authorities if and when this is legally provided for. Thus, the strategy calls for and provides means to ensure interoperability. It does not in itself create links between different databases or provide for specific types of data exchange, but it ensures that, when the operational requirements and legal basis exist, the most simple, easily traceable and cost-effective solution is found.

This means that the efforts to achieve interoperability require interaction between all the relevant authorities and organisations. Which authorities and organisations will depend on the specific need that is catered for. The methodology set out in this strategy and in particular focus areas 1 to 3 will ensure that interoperability is ensured whenever necessary and proportional, among and beyond the authorities directly responsible for the EU internal security, but also that it is limited to these cases.

This means that:

information exchange must not be hampered by issues of competence (mutual recognition of different national structures)
IT support and standardisation (including architecture principles and information/data models) must be as horizontal as possible and based on common principles and coordination;
measures to implement data protection and data security should be coordinated between the EU level and Member States;

an inter-systems impact analysis should be taken into account in the framework of this multidisciplinary approach.