PUBLIC

COUNCIL OF THE EUROPEAN UNION

Brussels, 26 June 2007

11312/09

LIMITE

JAI 417
CATS 76
ASIM 72
JUSTCIV 163

NOTE

from :	incoming Swedish Presidency
to :	Ad Hoc Working Group on Information Exchange
Subject :	Proposal for an EU Information Management Strategy for Justice and Home Affairs

The incoming Swedish Presidency proposes in annex draft Council conclusions setting out an EU information management strategy.

The strategy targets what has to be achieved in terms of information availability and exchange. It translates business needs into clear structures and content and contains, under a number of focus areas, the goals to be achieved by 2014 or beyond and, broadly, the action that needs to be taken to achieve them.

In the short term, the process of developing the strategy is also intended to contribute to the Stockholm Programme and its Action Plan. The strategy as such has a long-term focus. It will be further developed and updated as the overarching vision develops or changes and should be revised by the end of 2014.

The Information Management Strategy is the top document, which will be complemented by an action list/road map defining concrete goals, processes, roles and deadlines.

The Ad Hoc Working Group on Information Exchange will be invited to examine and agree upon it with a view to its approval by the Council.

THE COUNCIL OF THE EUROPEAN UNION,

RECALLING

- the Hague Programme on strengthening freedom, security and justice in the European Union[1], in particular section 2.1 that calls for improved exchange of information to fight crime and therefore establishes the principle of availability,

- the Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union[2], in particular point 3.1.(k) that calls for a definition of a policy for a coherent approach on the development of information technology (IT) to support the collection, storage, processing, analysis and exchange of information,

- the report of the Future Group of ministers for home affairs, recommending the implementation of a "European Union Information Management Strategy" (EU IMS) to remedy to the current situation of an "uncoordinated and incoherent palette of information systems and instruments" which have "incurred costs and delays detrimental to operational work" and thus going "beyond the limited perspective of a case-by-case approach and aim for a holistic objective in law enforcement information management.";

BUILDING UPON

- the work accomplished by the Friends of the Presidency[3] on the technical modalities to implement the principle of availability,

[1] 16504/04, JAI 559
[2] 9778/2/05 REV 2, JAI 207
[3] 13558/1/05 REV 1

- the proposed Council Conclusions[4] on the definition of a policy for a coherent approach on the development of information technology (IT);

- conclusions of the 2007 and 2008 COPE conferences[5] and the Common Requirements Vision[6];

RECOGNISING THAT

Effective and secure cross border exchange of information[7] is a precondition for the successful prevention, detection and investigation of crime in the European Union.

The Hague Programme established the vision for the exchange of information in the EU, *i.e.* the Principle of Availability (PoA), that "*throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement of ongoing investigations in that State.*"

This requires the right information to be available at the right time, for the right person and in the right place. To do so, "the methods of exchange of information should make full use of new technology and must be adapted to each type of information".
It also requires citizens' expectations of privacy to be balanced against their expectations of protection. Furthermore, the Member States and authorities involved need a high level of trust in one another's management of information.

[4] Document 15478/05 CRIMORG 152 CATS 87
[5] Documents 10063/07 CATS 70 and 13592/08 CATS 74
[6] Document 7758/08 CATS 21
[7] In this context, information means any information or criminal intelligence needed by Member States competent authorities to fulfil their task preventing, detecting or investigating crime.

At several occasions, Member States have expressed the need for coherence and consolidation and a need to implement existing instruments and arrangements rather than embark upon new initiatives.

In view of the growing number and complexity of crime phenomena as well as the effects of the economic downturn the EU and the Member States must maximise their limited resources.

HEREBY RESOLVES

1. To adopt and implement an Information Management Strategy for Justice and Home Affairs

   on the basis of the following principles:

   - the Information Management Strategy is an essential tool, but remains a means to an end, not a purpose in itself. Priorities set in the strategy must correspond to priorities set for the JHA area and support the business vision for law enforcement and justice cooperation;

   - information management is purpose-based, as opposed to competence-based. It follows that the EU Justice and Home Affaires Information Management Strategy provides for the multidisciplinary approach needed to develop an Area of Freedom, Security and Justice;

   - the strategy strives for a balanced law enforcement information exchange where good supply of information takes account of both business needs and the rights of the individual. It defines the preconditions for the professional, business driven and cost effective development and management of IT. The strategy shows the way towards a structured information exchange and forms a basis for enhanced decision making processes and governance;

   and consisting of the following focus areas, which are elaborated in annex:

- needs, requirements and added value are assessed as a precondition for development
- development supports agreed law enforcement workflows, intelligence models and intelligence requirements
- a balance between data protection requirements and business operational needs
- interoperability and co-ordination both within business processes and technical solutions
- standard technical solutions are used and kept to a minimum
- re-utilisation is the rule: do not re-invent the wheel
- 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
- interdisciplinary co-ordination is ensured within the JHA area

2. To take the necessary steps to develop and update as necessary a detailed action plan in order to fulfil the overall aims and objectives of this strategy.

INVITES

- primarily, its preparatory bodies dealing with issues of information exchange and IT development to 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 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 guidance for policy makers, CIO's and other decision makers in their competent authorities when dealing with issues related to international information exchange and IT development ("national housekeeping").

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 at EU level. It also reflects the vision of the availability of information based on purpose and necessity.
It will require an assessment of the needs and requirements of law enforcement co-operation, including how the IT solutions will be used, and how useful they will be for enhancing capacity for law enforcement co-operation from the perspective of law enforcement work and working methods. As a consequence, IT development will be based on and driven by the needs and requirements of law enforcement co-operation (business requirements). An assessment of usefulness will also help to set priorities for IT development.

This means that:

- *when initiatives regarding information exchange or technical solutions are put on the EU agenda, end-users, senior officers and supervisors 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 separated from the analysis of needs and requirements ;*
- *negotiations about legislation and/or technical pre-studies (solutions) must not start before the business requirements are identified and documented .*

2. Development supports agreed law enforcement workflows, intelligence models and intelligence requirements.

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.
This means that business processes must allow the quick, efficient and cost-effective exchange of information and 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 with the existing Common Requirements Vision (CRV) should be continued and complemented by analyses of substantial requirements, made together with and by national authorities;*
- *further work with an "information map" should provide an overview of business processes and the corresponding information flows of international co-operation, so as to identify on that basis the interface at which harmonisation is needed.*

3. A balance between data protection requirements and business operational needs.

Law enforcement and judicial cooperation place high demands on information security and data protection. Personal privacy as well as business security have to be ensured, while providing for business needs to use and share information. The Principle of Availability assumes that data protection and information security are given a high priority and that conflicts between the interests of justice, freedom and security are solved at all levels.

This means that a balanced 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. Full use of modern technologies, but also adaptation of business processes and data protection regimes facilitate this. Enhanced trust between competent authorities in their respective information security and data protection 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 better 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;*
- *the different tools must be rationalized with a view to simplifying the work of the competent authorities, which will minimize the risks of damage, as will training in the available tools and their use;*
- *adequate data protection regimes must provide for real and regular operational checks and ensure that appropriate sanctions are effectively applied in the event of any breach.*

II. INTEROPERABILITY AND COST EFFICIENCY

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

Interoperability is more than a technical aspect of the exchange of data. It exists on 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 comply with defined standards and principles that support interoperability and co-ordination between systems and the exchange of information. Change is the normal situation in the technical area, which means that established recognised standards and security mechanisms to facilitate communication and prevent disruption and infringements change accordingly. 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.

This means that:

- *the "information map" should include a comparative overview of EU and Member States legislation in the area of information exchange;*
- *European interoperability models for information exchange must be described and developed;*
- *a model of how to share and re-use sustainable solutions must be produced.*

5. Standard technical solutions are used and kept to a minimum.

IT development is based on industrial standards and best practices, including well-defined open standards for communication between access points.
As a consequence, there will be greater coherence in the development and management of IT systems. By applying standards, law enforcement co-operation 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:

- *an EU law enforcement catalogue of services at EU and national level (an interoperability value map) should be created, distributed and maintained;*
- *integration enablers, such as standards technologies and capabilities, which facilitate integration and are designed to provide security, scalability and performance, must be identified;*
- *data security regimes must be coordinated at and between both the EU and national levels;*
- *existing accreditation/standardisation functions must be used when available.*

6. Re-utilisation is the rule: do not re-invent the wheel

IT development means high costs and considerable investment, but also long-term costs for management, maintenance and support. Normally, only 20 % of the total cost is used for the development phase.

This means that re-utilisation is a priority for IT development and technical improvement. Re-utilisation helps to avoid parallel solutions and to further develop existing 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 IT 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 IT also requires a constant evaluation process.

This means that:

- *the ad hoc study on the third pillar information systems must be further developed to include information flows, functions and solutions;*
- *a commonly agreed, cohesive and coordinated interoperability initiative, which includes agreements on interoperability standards and rules, has to be drawn up and put in place;*
- *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.*

III. GOVERNANCE AND PROCESSES

7. 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.
This means that Member States' authorities, which are responsible for national implementation of processes, 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 need to work on their own interoperability, both business and technical, and establish their own development processes.

This means that:

- *national and EU information management strategies have to be in line;*
- *stakeholders must be involved at both the national and EU level;*
- *authorities in Member States need to identify and develop their own development processes.*

8. 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 must be identified and organised;*
- *functions to prepare the strategic decisions on information management and IT development have to be identified/established;*
- *functions for administration, further development and evaluation of (business and technical) solutions must be in place.*

9. Interdisciplinary coordination is ensured within the JHA area.

The purpose of the Information Management Strategy is the exchange of law enforcement information within the JHA area. Since information management and exchange should be "purpose-based", i.e. depend on the purpose for which the information is needed and not competence-based, i.e. who holds the information, increased horizontal coordination is needed. The Information Management Strategy must recognise and cater for the multi-disciplinary approach needed to facilitate the transfer and re-utilisation of information within the whole JHA area.
This means that interoperability needs to go beyond law enforcement authorities. 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 security and data protection. Business needs must and will, by their very nature, respect and take account of specific work environments. To ensure the effective use of the possibilities and tools is an important part of a strategy to make information management cost effective, business driven and professional.

This means that:

- *information exchange must not be hampered by issues of competence (mutual recognition of different judicial systems)*
- *IT support and standardisation (including architecture principles and information/data models) must be as horizontal as possible and based on common principles and coordination;*
- *information security regimes must be coordinated between EU and national levels.*