# Opinion of the European Economic and Social Committee on the 'Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Towards the integration of maritime surveillance: a common information sharing environment for the EU maritime domain'

*COM(2009) 538 final*

(2011/C 44/32)

Rapporteur: **Mr LIOLIOS**

On 15 October 2009 the European Commission decided to consult the European Economic and Social Committee, under Article 262 of the Treaty establishing the European Community, on the

*Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Towards the integration of maritime surveillance: a common information sharing environment for the EU maritime domain*

COM(2009) 538 final.

The Section for Transport, Energy, Infrastructure and the Information Society, which was responsible for preparing the Committee's work on the subject, adopted its opinion on 1 June 2010.

At its 464th plenary session, held on 14 and 15 July 2010 (meeting of 14 July 2010), the European Economic and Social Committee adopted the following opinion by 164 votes to 1 with 6 abstentions.

## 1. **Conclusions and recommendations**

1.1 The EESC welcomes the Communication and supports the range of possible measures for integrated maritime surveillance (IMS) towards the effective understanding of all activities carried out at sea that could impact the security, safety, economy, or environment of the European Union (EU) and its Member States.

1.2 The EESC agrees in principle with the recommendations made by the abovementioned Communication and believes that the inclusion of rules on the dissemination and handling of data as well as the introduction of control mechanisms from/to all participating organisations will improve the situational awareness in the maritime domain.

1.3 The EESC notes that the surveillance communication is a positive contribution to the increased security problems faced by the EU including illegal immigration, trafficking, drug selling as well as efficient and effective protection of the environment and of the life and wealth of EU citizens.

1.4 The EESC acknowledges that the sustainability of the integrated maritime policy for the EU depends on the sustainability of its policy actions and amongst them the Integrated Maritime Surveillance is no exception. To this extent, the proposed integrated maritime surveillance system should be built to provide in a sustainable manner accurate, timely, quality and cost-effective data when and where needed and for the exact reason required. Therefore, the expandability of the IMS system must also be considered.

1.5 The EESC supports a common EU wide surveillance mechanism based upon a harmonised legal framework which will cater for the sharing of sensitive and non-sensitive information amongst the EU Member States' authorities, agencies and users.

1.6 The EESC acknowledges the importance of the international dimension of the maritime domain and urges the need to develop technical and legal standards and explore the cooperation opportunities with third countries.

1.7 The EESC believes that interlinking maritime surveillance systems presupposes thorough consideration of diverse legal issues related to the exchange of information collected for different purposes and from different sources. Member States have different obligations and data confidentiality and the protection of personal data are key issues. It is yet to be defined the nature of the data involved, the purposes (and the methods) of the exchange and the potential recipients of the data, the necessary safeguards with regard to the confidentiality and security of data and the protection of personal data, where relevant.

1.8 The EESC suggests that data should be disseminated 'on a need to know basis' in order to safeguard data protection and undue proliferation of data. It is also imperative to define clearly the confidentiality levels as well as the authoritative level for data usage, through the development of a concrete and transparent access right granting scheme.

1.9 The EESC understands that the validation of collected data is a critical and difficult task, and proposes the development of a framework that will collect that data and verify its correctness, as well as ensuring information security during its dissemination process.

1.10 The EESC advocates that a roadmap should be followed towards the implementation of the integrated maritime surveillance, utilising the experience of pilot projects, expert groups, and impact assessment in dealing with the legal and technical aspects of information integration.

1.11 The EESC recommends the development of single national coordination mechanisms and one information hub per national user group (community) in order to facilitate the development and operability of the integrated maritime surveillance.

1.12 Bearing in mind the numerous existing systems, the EESC proposes to avoid overlapping of existing systems, so that the integrated maritime surveillance will not change how information is collected but how information is disseminated.

1.13 The EESC invites the EU to adopt a more centrally managed network approach where coordination will be achieved through the network's formal structure and central communications.

1.14 In order to safeguard the interlinking process of the user communities, the EESC suggests that the EU should define a clear and robust platform regarding the access granting scheme, based on a common EU understanding of the different political views as well as on an operational effectiveness. The beneficiaries of the access right provided have to be governed by the EU Transparency Regulation.

1.15 The adopted system architecture should have feedback loops to enable adjustments and updates utilising inter alia the evolving legal framework.

1.16 The EESC recommends that advanced security risk management should remain a top priority for the European maritime domain. To this extent, a tiered architecture that ensures data validity and data security is preferable.

## 2. **Introduction**

2.1 On 15 October 2009 the Commission published the Communication 'Towards the integration of maritime surveillance: A common information sharing environment for the EU maritime domain' (COM(2009)538 final) and referred to the European Economic and Social Committee based on Article 262 of the EC Treaty to give an opinion on this matter.

2.2 The European Commission in its Communication 'An Integrated Maritime Policy for the European Union' aims before 2013 to 'take steps towards a more interoperable surveillance system to bring together existing monitoring and tracking systems used for maritime safety and security, protection of the marine environment, fisheries control, control of external borders and other law enforcement activities'.

2.3 The EU has already established a number of surveillance initiatives integrating more than one sectoral activities: Vessel Traffic Monitoring including data on ships' movements and cargoes are collected and exchanged between Member States, SafeSeaNet (Directive 2002/59/EC) [1], an exchange of maritime data between Member States' maritime authorities aims to prevent accidents, marine pollution as well as to increase the efficiency of the response in case of incidents or accidents at sea.

2.4 To that extent, the European Index Server (EIS) is operated and STIRES (SafeSeaNet Traffic Information Relay and Exchange System) is under development. In addition, short range maritime traffic data are currently collected and long range data will in the future be available on demand from the EU Long Range Identification and Tracking Data Centre (EU LRIT DC - Resolutions of the IMO Marine Safety Committee MSC 202 (81) and MSC 211 (81), amending the International Convention of Safety of Life At Sea, 1974 (SOLAS)) in cooperation with Member States. Furthermore, the development of the European Border Surveillance System (EUROSUR) envisages an integrated surveillance solution for the EU.

2.5 Further to the above, this Communication considers all the additional relevant actions taken by the EU, including the creation of the European Maritime Safety Agency (EMSA), the European External Borders Agency (FRONTEX), European Defence Agency (EDA) and the Blue Book for Transport. In parallel two pilot projects to test in a theatre of operations how integrating maritime surveillance can work in practice are being launched. One in the Mediterranean basin and another in the Northern European sea basins.

2.6 The goal of the proposed IMS policy is not to create an additional surveillance system, but to set up interfaces and subsequently integrate existing systems across sectors and borders, in order to improve the effectiveness of national authorities in charge of implementing surveillance actions and increase the cost-efficiency of actions carried out at sea. Work towards the development of a secure cross-sectoral network that can meet the ever increasing requirements for the provision of a common and recognised picture will need to carefully plan access rights and security provisions of users.

2.7 The EESC recognises that materialising an IMS includes complex, multifaceted and numerous activities which often overlap and but are to the interest for the EU as a whole.

[1] OJ L 208, 5.8.2002, p. 10-27.

2.8 The EESC welcomes the Communication as a basis for integrating the currently existing stand alone systems into a Common Information Sharing Environment that will be able to support the future European maritime transport policy, to safeguard the environment and European shipping services for both global and European trade as well as improving the daily life of EU citizens, especially those populating EU external sea border areas.

2.9 The EESC points out that this Communication comes at a critical time of serious challenges affecting maritime transport: (a) the world economic and financial crisis aggravating the structural and cyclical shipping crisis, (b) illegal immigration taking place especially in the southern and eastern EU borders, (c) illegal activities including trafficking, arms and drug trade, (d) sensitive material for military and nuclear installations all need to be monitored and confronted.

2.10 The EESC stresses also the fact that security and piracy issues affecting EU maritime services occurring in non EU waters (i.e. East Africa, Indonesia, etc) which have to be addressed and controlled.

## 3. **Communication on the integration of maritime surveillance through a common information sharing environment for the EU maritime domain**

3.1 As stated in a previous opinion [2] the EESC 'endorses the proposals regarding the European network for maritime surveillance and the improved cooperation between Member States coast guards. Such measures will promote maritime safety and security, fisheries control and control of external borders and protect the marine environment. […] The EESC reiterates that a coordinated approach regarding bilateral ship boarding agreements with third countries is desirable to meet enhanced security considerations. It also urges EU action concerning the proliferation of incidents of armed robbery and piracy at sea against merchant vessels in South East Asia and Africa'.

3.2 The EESC welcomes the Communication and supports the range of possible measures whereby the EU could contribute to safer and more secure provision of services in the maritime domain. The EESC agrees in principle to this communication and welcomes further refinements that will add to the rapid materialisation of an IMS.

3.3 The Communication on an EU strategy on better integration of surveillance systems lays down four guiding principles towards the development of a common information sharing environment, that is: (1) An approach interlinking all user communities, (2) Building a technical framework for interoperability and future integration, (3) Information exchange between civilian and military authorities, and (4) Specific legal provisions to materialise this Common Information Sharing Environment. Since this communication is at level of principles, the opinion will be limited to a set of proposed principles. It remains of course, that further refinement would be required to turn these principles into legislative actions.

3.4 The EESC acknowledges that due to the global character of European shipping, situational awareness is significantly important because (a) the ship's movement is a spatial and temporal dynamic system, (b) safety, security and environmental aspects are not border constrained, and (c) decisions taken by one entity might affect other systems.

3.5 It should be noted that there are two concerns to be resolved, the public policy framework and the system workability. The implementation of an IMS might be hindered by confidentiality or other concerns at Member States level, thus the IMS must be refined to a clearly workable application.

3.6 The EESC considers that there are three major issues in materialising the IMS: legal, technical/technological and managerial issues. The most important legal issues seem to relate to confidentiality, with respect to the mixture of personal, business and military data. In addition, data (security) policies may prohibit or restrict the sharing (or further use) of certain data.

3.7 Regarding confidentiality, the provisions of key monitoring and surveillance instruments qualify a significant amount of maritime reporting and surveillance data as (commercially) confidential. As a consequence, the processing of these data will be affected by the duty of confidentiality and professional secrecy of the persons authorised to have access to the data.

3.8 Current systems have a uni-sectoral nature but they are hampered by confidentiality issues. Extending data sharing beyond that sector might induce further challenges and questions concerning confidentiality given the range of additional actors that will be involved.

## 4. **Specific comments**

4.1 The EESC agrees and supports the principles set in the integrated maritime surveillance communication.

4.2 The EESC recognises the need for further analysis along policy, legal, market and technology perspectives that would lead to a specific action plan for the IMS implementation, emphasising the legal and technology challenges. This analysis will develop a specific implementation roadmap with an exact timeframe and might be based on relevant experience gained from projects like SafeSeaNet, Freightwise, e-Freight and AIS as well as from all relevant initiatives.

[2] EESC opinion on 'An Integrated Maritime Policy for the European Union', OJ C 211, 19.8.2008, p. 31-36.

4.3 The EESC reiterates the importance of examining the results of the currently running pilot projects prior to undertaking certain decisions. Pilot projects have to be targeted both to business settings and administrations operating in representative EU maritime domains. In addition, these pilot projects should also report on the long term sustainability of the IMS. To that extent, the launching of additional pilot projects will benefit our understanding of the issues in developing the IMS. Furthermore, specific time frames should be set and monitored for the timely completion of these pilot projects.

4.4 The EESC would like to point out that the IMS strategy could draw lessons as to implementation of data sharing from other practices in the transport sector, including the Single Transport Document, which is considered to be the equivalent information sharing scheme from the business perspective (a transport document is required today to follow the carriage of goods (Regulation (EEC) 11/1960 and Directive 92/106/EEC); according to the Freight Transport Logistics Action Plan, a Single European Transport Document will be established that can be used in all transport modes enhancing the framework offered by multimodal waybills or multimodal manifests). In addition, information exchange should be based on the most widely used language in the maritime sector.

4.5 The IMS sustainability must be ensured through the provision of built-in expandability in order to accommodate the integration of future stand-alone surveillance systems.

4.6 Regarding the sharing of information the EESC advocates in favour of the principle 'as much information as needed on a need to know basis in line with conditions of use […]' instead of '[…] as much information as possible […]'. Information has to be shared to all user communities based on a clear framework ensuring the protection of personal data and other sensitive data as well. Additionally, it is imperative to control the disclosure beyond the 'grantee' organisation, i.e. to follow EU legal frameworks.

4.7 Regarding technical aspects, the EESC recommends open source platforms to support the design, development, deployment and maintenance of relevant solutions. The core of the system should provide: (a) maritime domain ontology for automated data exchange; (b) tools for the design, simulation, performance analysis and optimisation of surveillance solutions; (c) registry of services; (d) tools to help resolve interoperability conflicts; (e) mechanisms for automated discovery and integration of suitable services; (f) secure interoperability; and (g) controlling and auditing mechanisms.

4.8 The EESC consents with the proposed layered system architecture. This approach will enable the cutting edge 'cloud architecture' currently used by all IT developers. Nevertheless, it should be born in mind that such architectures are more security breach prone and thus increased security mechanisms should be adopted. However an intra-organisational hierarchical decision making and data access framework might improve data confidentiality.

4.9 The EESC acknowledges the availability of technological means to collect, homogenise and disseminate meaningful data to all interested parties and urges the EU to define the common platforms to be effectively used by all interested parties in all Member States. Additionally, regarding the prevention of duplication of data collection and storage, mechanisms should be developed to avoid problems.

4.10 Regarding the first principle set in the Communication, the EESC proposes an active attempt towards establishment of common standards and data rules both at a sectoral and at a functional level in order to improve data quality.

4.11 Given the fact that the maritime domain is broad, data security may be potentially weakened from a flexible information sharing environment and the potential threat this implies.

4.12 The EESC considers that technical interoperability is important and should lead to a facilitation of data exchange by all interested industrial and governmental stakeholders (including Administration to Administration - A2A, Administration to Business – A2B, and Business to Business - B2B communications).

4.13 Regarding the third principle set in the Communication, the EESC acknowledges that further analysis for the integration of civilian and military interconnection is necessary in order to better integrate data and to facilitate better use of the information. The EESC agrees that surveillance information should be shared between civilian and military authorities. The EESC repeats the necessity for establishing underlying mandates; common standards and operating procedures for access to and use of the relevant information should be in place to allow for a legal two-directional information exchange where data usage is bound by community laws.

4.14 Regarding the fourth principle set in the Communication, the EESC would like to stress the need for further analysis regarding the protection of personal data in the scope of this document and urges the EU to reconsider and adopt all necessary actions that ensure the security of sensitive data. Although this implies a burden to this process, i.e. building up such system, it is considered to be an essential principle.

4.15 The EESC concurs with the sectoral approach for information sharing proposed in the directive. In any case, specific guidelines should be set for granting access rights to competent authorities and to authorised personnel.

4.16 The EESC invites the Commission to further investigate the existence of bilateral agreements on information sharing between EU Member States and third countries and, if necessary, activate enforcement of the *acquis communautaire* (Regulations 4055/86 and 4058/86).

4.17 With regard to the issue of space generated data specific mention is made of the GMES. Besides that, the EESC would also like to see in the communication specific mention on the use of the Galileo navigation system.

4.18 The EESC understands that processing personal data for military, state security and criminal law enforcement currently remains outside of the general legal framework for data protection. The EESC concurs with the conclusions of a study (European Commission, 'Legal Aspects Of Maritime Monitoring & Surveillance Data' – Final Report Framework Service Contract, No. FISH/2006/09 – LOT2) commissioned by the Commission on legal aspects of maritime surveillance data which clearly states that data protection is an outermost obligation for the EU and has to be addressed both at Community and Member State level. It is anticipated that advanced safeguards are required in case it would be envisaged to share personal data between authorities falling within the scope of the existing legal framework for data protection (e.g. fisheries authorities) and authorities (currently) falling outside that scope (e.g. military, state security or law enforcement authorities).

4.19 The EESC considers very important the development of a legal framework addressing issues, such as data quality, further use of data, data security, access granting mechanisms, nature of data involved, purposes (and methods) of the exchange, potential recipients of data, necessary safeguards respecting the confidentiality and security of certain data, protection of personal data and relevant procedures among others.

4.20 The EESC believes that data should be shared on a 'what, why, for how long and with whom' framework. Especially for the former, it is critical to define the designated authorities that will be entitled to control, disclose and receive the data both within EU and more cautiously with authorities outside EU.

4.21 The EESC asks the European Commission to publish an annual report on the implementation and results of its maritime surveillance activities.

Brussels, 14 July 2010.

*The President*
*of the European Economic and Social Committee*
Mario SEPI