EUROPEAN COMMISSION

Brussels, 20.10.2010
COM(2010) 584 final

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT

on a Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT

on a Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain

Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain

1. INTRODUCTION

On 15 October 2009 the Commission adopted a Communication[1] "Towards the integration of maritime surveillance in the EU: A common information sharing environment for the EU maritime domain" (CISE), setting out guiding principles towards its establishment.

In its conclusions of 17 November 2009, the External Relations Council[2] endorsed the above Communication, requesting the Commission to present by end 2010 a step by step roadmap to establish the CISE. This roadmap is to be further detailed in 2011 to take into account the results of the pilot projects. The Commission is also tasked to deliver by 2013 an assessment of the financial resources necessary for the implementation of the CISE. The General Affairs Council[3] reiterated the same approach in its conclusions of 14 June 2010 on the Integrated Maritime Policy.

The present communication responds to the Council's request.

In preparing the present draft Roadmap the Commission consulted the Member States Expert sub-Group on the integration of maritime surveillance ('MS EXPERT GROUP') acting as the forum for coordination, as mandated by the Council's conclusions. The wide cross-sectoral representation in these meetings, including representatives from the Defence Community at Member States' level, allowed for a substantial contribution to the common understanding of the issues at stake. In the preparation of the roadmap the Commission also liaised with other sectoral groups, such as the High Level Group for SafeSeaNet.

The aim of integrated maritime surveillance is to generate a situational awareness of activities at sea, impacting on maritime safety and security, border control, maritime pollution and marine environment, fisheries control, general law enforcement, defence as well as the economic interests of the EU, so as to facilitate sound decision making.

---

1 COM (2009)538 final

2 http://ec.europa.eu/maritimeaffairs/pdf/external_relations_council_conclusions_17112009_en.pdf

3 http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/genaff/115184.pdf, page 16

The added value of integrating maritime surveillance is to enhance the present sectoral maritime awareness pictures of the sectoral User Communities[4] of EU Member States and EEA States, with additional relevant cross-sectoral and cross-border surveillance data on a need to know and, a need and responsibility to share basis. The requirement to share information, particularly in case of an imminent threat, should be balanced by its owner against the risk of not sharing it. Such enhanced pictures will increase the efficiency of Member States' authorities and improve cost effectiveness.

Tackling this information sharing exercise from an overarching European perspective will ensure that all User Communities are represented in an equal footing, that their sectoral objectives and constraints are taken into account and that development of the Common Information Sharing Environment also results in added value for each sectoral User Community. Additionally it will also ensure that European systems are put to best use whilst complying fully with the principle of subsidiarity.

2. OVERVIEW OF THE ROADMAP

The discussions in the MS Expert Group concluded that this roadmap should lead to the creation of a decentralised information exchanging system, interlinking all User Communities both civilian and military. The setting up of the CISE should be a flexible process allowing for technical improvements and sectoral enhancements. Existing and planned systems shall be duly taken into account while developing the CISE. This process shall also not hinder the development of existing and planned sectoral information systems, as long as the need for interoperability enabling information exchange with other systems is taken into account. The experience gained from information exchange systems allowing for civil-military cooperation should be utilised.

Considering the significant number of potential participants in the CISE, the diversity of legal frameworks and possible exchanges, it is highly unlikely that one single technical solution will fit each and every exchange of information within the CISE. For this reason the CISE architecture should be designed as a *cost effective decentralised interconnection* of different *information layers* that *increases efficiency* of maritime surveillance systems by *filling existing information gaps* across Europe while *avoiding data duplication*.

These layers are managed by the respective owners of related information at Member States and EU level based on the applicable legal instruments. The competences of national authorities, as well as the mandates of EU Agencies set out in these legal instruments will thus be fully respected.

Common needs to most of the User Communities are to obtain an enhanced basic maritime situation awareness picture useful to all user communities. This picture may be composed by data stemming from a combination of systems and sensors detecting cooperative and non cooperative targets of any size.

Data of this basic maritime traffic picture is not classified and could be shared without any restrictions between all Communities provided the necessary safeguards are put into place.

Specific needs for certain User Communities to complement this basic maritime picture are:

---

[4] For a detailed list of all the User Communities see point 3.1 and the annex

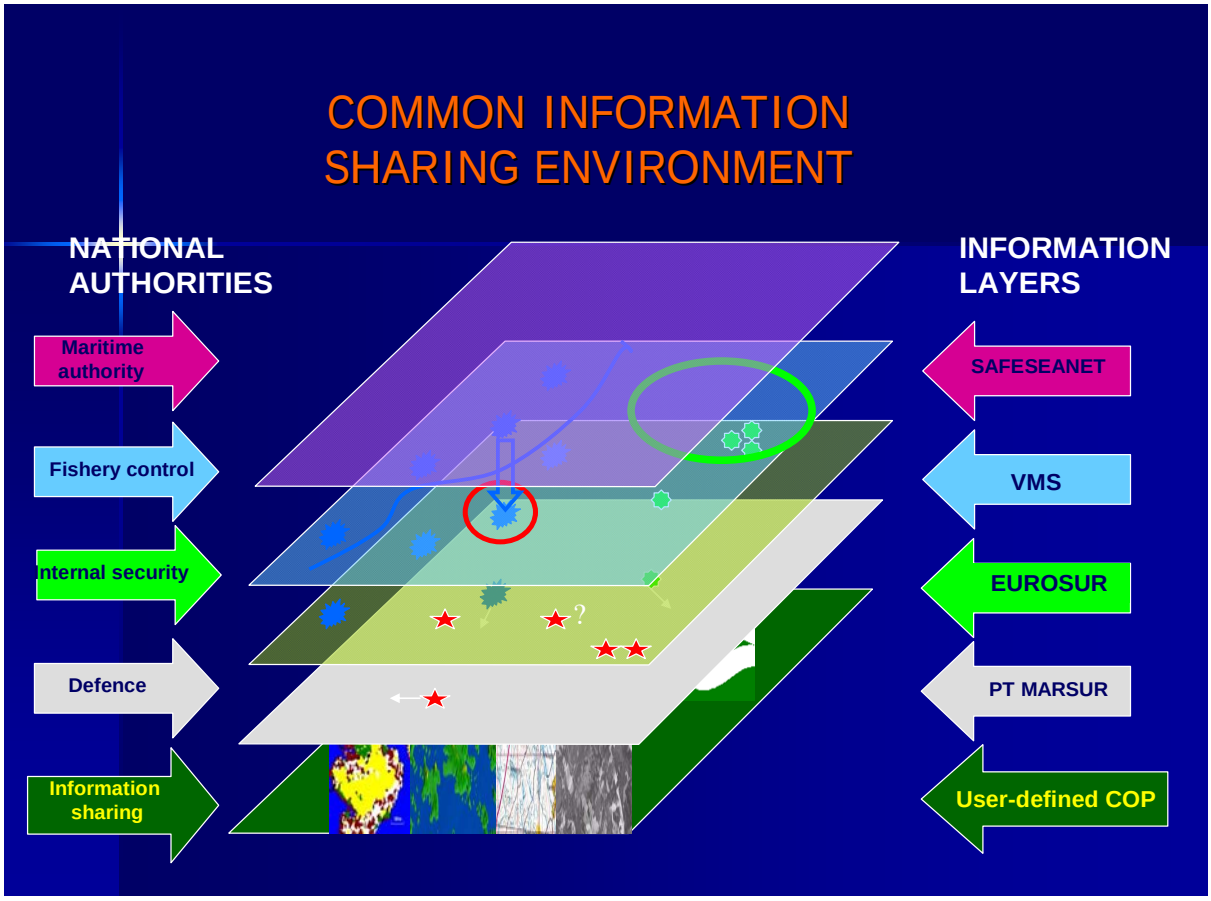
(a) To obtain data as regards illegal activities and threats impacting on both internal and external EU security, and involving any type of vessel. Such information is gathered essentially by coast guards, border guards, police services and defence forces.

(b) To obtain specific catch information, combining it with position information of fishing vessels to fight against illegal fishing.

(c) To obtain advanced electronic data concerning all goods entering and leaving the EU customs territory in order to enable a pre-assessment of the safety and security of goods.

Some of the information handled by these Communities is highly sensitive and may therefore be transmitted only point to point or via and between secured sectoral networks. At present, the information and intelligence exchanged within these communities take place within a strictly defined scope, often framed by international agreements. The CISE will therefore not be based on the principle "everybody shares everything", but it shall be based on "sharing on a need-to-know and responsibility-to-share basis".

Example of information layers (non-hierarchical)



User communities will have to be fully involved in elaborating the following six steps and an impact assessment identified by the Commission and the MS Expert Group as necessary for the CISE development:

Step 1 - Identifying all User Communities: Member States and the Commission shall *identify the participants* to the information exchange. Due to the diversity in administrative organisation in the EU Member States and EEA States it is necessary to focus on "functions" based on already established 'User Communities' rather than on types of national authorities.

Step 2 - Mapping of data sets and gap analysis for data exchange to ensure that there is an *added value* to the CISE: By (a) drawing up a map of data exchanges already taking place at EU and national level and (b) drawing up a gap analysis to identify the sectoral demand for data currently not matched by supply.

Step 3 - Common data classification levels, addresses the problem that sectoral User Communities classify same type of data in a different manner. Without interfering with national data classification levels and for the purpose of enabling data exchange within the CISE, Step 3 shall identify which national classification levels correspond to each other and thus establish common grounds for data exchange under the CISE.

Step 4 - Developing the supporting framework for the CISE defines the *supporting technical framework* for the CISE, thus for setting up the interfaces between the existing and planned sectoral systems in view of enabling cross-sectoral data exchange. This should be worked out by the representatives of the various sectoral user communities based on available results of FP7 and pilot projects (e.g. MARSUNO, BluemassMed, EUROSUR pilot project on the communication network, GMES, PT MARSUR, SafeSeaNet based pilot projects).

Step 5 - Establishing access rights entails the identification of the *rights of users* belonging to different sectoral communities to cross-sectorally access various data sets. This relates only to data which should be shared via the CISE in the EU and the EEA[5]

Step 6 - Ensuring respect of legal provisions aims at ensuring that there is a clear *legal framework* for the exchange, defining at least the nature of the data involved, the capability and the right of the data providers and recipients to exchange the data, the purposes (and the methods) of the exchange as well as incorporating the necessary safeguards with regard to the confidentiality and security of (certain) data and the protection of personal data, where this may be relevant. Obstacles to the exchange of the data present in EU legislation must be identified and solutions to overcome them should be explored.

3. STEPS TOWARDS A ROADMAP

Principle 1:	An approach interlinking all User Communities including the Defence Community

3.1. Step 1: Identifying all User Communities

Aim: to identify the members of the CISE

Description: Considering that the internal organisation of the Member States' authorities varies considerably, it is proposed to determine the User Communities participating in the CISE in relation to the following *'functions'* performed:

[5] Environmental data should be open access in line with the Aarhus Convention.

(1) Maritime Safety [6] (including Search and Rescue), Maritime Security [7] and prevention of pollution caused by ships[8],

(2) Fisheries control

(3) Marine pollution preparedness and response; Marine environment

(4) Customs[9]

(5) Border control[10]

(6) General law enforcement[11]

(7) Defence[12]

An indicative description of those functions is given in Annex.

Action: Each Member State should identify which authority(ies) perform(s) the above mentioned functions. More than one authority can be identified per function. On this basis, these authorities will be recognised as members of the User Community and as such entitled to "*provide and/or receive information at national level from international, regional, Community, military and internal security systems and mechanisms, in line with conditions of use and defined user access rights, in order to build up its individual user-defined situational picture*" (Principle 1 of the 2009 Communication).

Each identified authority shall additionally indicate if it is linked to a national, regional or European network and identify the other members of the said network.

In particular at EU level, function (1) is already covered by the European Vessel Traffic Monitoring Directive[13]. As the system is operational, its users have already been defined.

At EU level, function (5) will be covered by EUROSUR, which will give Member States the appropriate technical and operational framework for increasing the situational awareness at their external borders and for improving the reaction capabilities of their national authorities.

Function (6) concerns a wide area, covered in particular by internal security responsibilities dealt with by EUROPOL and other relevant agencies**.** The integration of data within the EUROSUR network should also be taken into account.

---

6 Maritime Safety, within the scope of relevant IMO conventions in particular the SOLAS, STCW and COLREG conventions and related EU legislation.

7 Maritime Security, within the scope of SOLAS Chapter XI-2, Regulation 725/2004 and Directive 2005/65/EC. According to Article 2 of Regulation 725/2004: "maritime security" means the combination of preventive measures intended to protect shipping and port facilities against threats of intentional unlawful acts.

8 MARPOL 73/78 Convention and related EU legislation

9 With focus on control of goods.

10 With focus on the prevention of illegal immigration and cross-border crime at EU external borders.

11 With focus on the prevention of any criminal / illegal activity and on police administrative activities in the EU maritime domain.

12 See also principle 3 below.

13 2002/59/EC as amended by 2009/17/EC.

In parallel to this action, the Commission shall list the relevant EU agencies/institutions under the relevant functions.

Actors: Member States, the Commission and the relevant agencies

Timing: End 2010

3.2. Step 2: Mapping of Data Sets and Gap Analysis for Data Exchange

Aim: To determine existing and future maritime surveillance data sets and to identify the EU wide demand for cross-sectoral data exchange currently not matched by supply. This is to be carried out at national, regional and EU level.

Description: Monitoring and surveillance data relevant for the CISE is to be found in EU and national systems developed under EU law as well as in national and regional systems developed under national provisions. Drawing up a map covering each User Community's available surveillance data and its demand for relevant data from other communities shall allow to identify the respective gap between demand and supply for maritime surveillance data.

Identifying such present *gap* shall reveal the *added value* that will be achieved by bridging it through future cross-sectoral maritime surveillance data exchange throughout the EU.

Action:

(a) *Data mapping:* Each User Community in coordination with their respective working groups and EU Agencies (if appropriate) should identify the relevant surveillance data it currently avails of (supply mapping), its demand for relevant data from other communities (demand mapping) while indicating the corresponding legal basis per data set and whether it contains information involving personal data or intellectual property rights (IPR) or any other legal restrictions.

(b) *Gap analysis*: Based on this mapping the gap between demand and supply shall be established.

Actors: MS Expert Group in close coordination with sectoral working groups.

This work should be facilitated by a multidisciplinary ad hoc Technical Advisory Group (TAG) composed of representatives of each User Community, a representative from BLUEMASSMED and MARSUNO as well as the pertinent EU Agencies and initiatives. Each of these experts is meant to bring in full knowledge of sectoral advancement. The TAG will provide a pattern for the above demand and supply data mapping on the basis of which individual User Communities shall provide their input. The work of this group should be facilitated by the Joint Research Centre of the European Commission making best use of current and planned initiatives at EU level. Any progress made should be presented to the MS Expert Group.

Timing: End 2011

Principle 2:	**Building a technical framework for interoperability – Making best use of existing**

	systems but maintaining dedicated (point to point connections) for certain types of data

3.3. Step 3: Common Data Classification Levels

Aim: In order to facilitate cross-sectoral information exchange, User Communities should develop a common approach when attributing classification levels.

Description: Due to the fact that the CISE is meant to be only a transmission tool between different user communities, but not a (centralised) platform to store exchangeable data, each User Community remains responsible for gathering and storing its data by means of its own sectoral systems and security standards. This however leads to the problem where the same data sets may be classified by the different user communities in a different manner. In order to build sufficient trust for exchanging data in a decentralised cross-sectoral manner, there is a need to develop a common approach with regard to classification levels. The commonly recognised data classification levels established by legislation of the Council and the European Commission[14] should be applied.

Action: Developing a common ontology in order for same data to have the same or compatible classification in view of facilitating cross-sectoral information exchange, in two stages:

(1) A comparative overview with regard to the attribution of *data classification levels* (e.g. EU Restricted, EU Confidential, etc.) to relevant data sets. Those levels will be reflected in future definition work.

(2) User Communities should verify their current practices with regard to attributing the various data classification levels to relevant data sets.

Actors:

Stage 1 should be carried out by the MS Expert Group with support from the above mentioned TAG.

Stage 2 should be carried out by the relevant User Communities, with support from the relevant expert working groups and EU Agencies as appropriate taking into account any other relevant initiatives such as ongoing pilot projects. The MARSUNO and BluemassMed pilot projects on integration of maritime surveillance should assist user communities in this endeavour.

Timing:

Stage 1: 2011

Stage 2: First trimester 2012

3.4. Step 4: Developing the supporting framework for the CISE

Aim: To establish interoperable services and a common technical language to exchange maritime surveillance data in a decentralised manner.

[14] Commission Decision of 29 November 2001, OJ L 317 of 3.12.2001 as amended The above Commission decision is based on Council Decisions of 19 March 01 OJ L 101 of 11.4.01 as amended.

Additionally, attention should be paid to ensure and develop the overall IT security of the CISE.

Description: Once the data to be exchanged has been identified under Step 2, the best technical means to exchange the data needs to be established.

A *common informatics language approach* could be worked out in view of allowing for the interoperability of data between relevant systems. Under such an approach, User Communities could *translate* their own data coming from their own systems into a *commonly agreed format* available to all User Communities and readable by any computer system authorised to access the network. To some extent, the common software needed could be developed jointly under an open source type umbrella.

The advantage of such an approach for data exchange would be to:

(1) Allow for a Common Information Sharing Environment 'CISE' in a *relatively simple* manner (avoiding major standardisation work between different surveillance systems) to be developed step by step starting from the information that could be more easily shared.

(2) Existing systems of the various partners are only impacted insofar as a module must be added to allow the web services to catch the required data.

(3) An open source software development approach allows for the *common informatics language* to be upgraded any time to future needs, avoiding multiple expensive and unnecessary developments, vendor lock-in and help building communities with a common interest.

Other circumstances, however, may require data exchange and interoperability based on techniques and procedures other than the envisaged approach (e.g. in cases of real-time data, especially when of a classified nature, or when simultaneously acquired over large space distances). In such cases, different techniques (e.g. based on satellite technologies) may be required, taking into account international data standards, such as those contained in the United Nations Trade Elements Directory (UNTDED), the practical experience of relevant RTD projects and already developed military information exchange systems. Results from ongoing research projects, which are relevant to the strengthening of European industrial competitiveness, e.g. in terms of developing appropriate inter-operability standards, may also be useful in strengthening the technological base for the CISE.

Action: The above mentioned TAG is to define options to be presented and discussed with the User Communities. Any progress made should be presented to the MS Expert Group.

Actors: TAG, the MS EXPERT GROUP and the sectoral working groups

Timing: 2012

Principle 3: Civilian / Military Cooperation

The Defence community must participate in the elaboration of the CISE. To do so, under Step 1, Member States identify their relevant national authorities. Each Member State therefore should ensure that their military authorities continue to take part in the development of the Roadmap by participating in the Commission's Member State Expert subgroup on the

integration of maritime surveillance. The European Defence Agency (EDA) will participate as the relevant Agency in the MS Expert Group and in the TAG contributing with its knowledge on the Project Team on Maritime surveillance (PT-Marsur).

The EDA "Wise Pen" Report has been published on 26/04/2010 and provides an important contribution towards the development of an improved cooperation between CSDP and civilian actors of maritime surveillance, notably as regards exchange of information.

Principle 4: Specific legal provisions

3.5. Step 5: Defining access rights

Aim: Step 5 consists of determining User Communities' access rights to each others data.

Description: On the basis of the previous steps each User Community should establish the access rights it is willing to grant to other user communities for any data set (EU or national data) it is willing to share and that other user communities are requesting.

User access rights need to be consolidated and updated. To address specific circumstances access rights will be dynamically managed by information owners and might include the possibility, under specific circumstances, to block or grant additional access ad hoc.

Action: On the basis of a template developed by the TAG, User Communities declare their intention to share particular sets of their data with other User Communities on the basis of the data needs identified in the above gap analysis. Since the CISE is not a platform for data storage, but a tool for point to point data transfer, it needs to be studied to which extent existing sectoral data policies can be used for cross-sectoral data exchange through the CISE. The TAG shall compile the proposals made by the User Communities into a comprehensive overview table. This table shall be submitted by the Commission to the MS Expert Group for validation.

This approach would provide the following output:

(1) Interlinking all User Communities on a need to know/share logic

(2) A non-hierarchical framework for interoperability

(3) A flexible information sharing environment allowing Member States to input national/regional data as required

(4) Common approach to attribution of data classification levels

(5) Cost efficiency as the same data is used for different purposes

Actor: TAG, sectoral working groups in close cooperation with MS Expert Group.

Timing: 2012

3.6. Step 6: Providing a coherent legal framework

Aim: To ensure that the data is exchanged under the proper legal framework.

Description: By end 2011, the pilot projects should have provided a preliminary view on the legal, administrative and technical obstacles to the exchange of data, best practices to promote the exchange and identify how to comply with confidentiality and information exchange requirements. Therefore this step aims at ensuring that for each exchange there is a clear framework regarding the respective rights and obligations of participants to the exchange. Due consideration must be given in parallel to other legal issues, such as data confidentiality, intellectual property rights, protection of personal data as well as ownership of data, in accordance with national and international law.

Action: Identify which information exchange requirements are already covered by an international or EU legal framework and those which need to be established on the basis of new legislative framework(s).

Actors: MS EXPERT GROUP in coordination with sectoral expert groups.

3.7. Impact Assessment including on financial implications

The Commission will carry out an Impact Assessment to be fed by steps 1 to 6 of the present Roadmap prior to tabling a proposal to the Council and the European Parliament for the implementation of the CISE. It will set out an appropriate timeframe for Member States and the relevant EU bodies to implement the CISE.

To ensure that the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties, as set out in Article 5 of the Treaty of the EU, whenever actions touch on issues of national competence (e.g. step 2), these will not be reflected either in the roadmap nor in the Commission's proposal.

Timing: The different steps of the draft roadmap and particularly the work within the MS Expert Group and the sectoral working groups are meant to constitute various preparatory elements of the Impact Assessment. The final drafting of the Impact Assessment should take place by 2013.

4. CONCLUSION

The present draft Roadmap sets a flexible step by step approach towards building the decentralised CISE reflecting extensive consultation with the MS Expert Group as requested by the Council.

Its effective implementation will depend on the commitment of the actors identified throughout the different steps. The Commission will ensure the coherent implementation of the Roadmap. The Commission and the Members States should ensure such coherence within the sectoral working groups. The MS Expert Group shall ensure overall coherence in the process of integrating maritime surveillance.

The extent to which a regional approach would be followed for the CISE should be further reflected upon by the Member States within the MARSUNO and BlueMassMed pilot projects and referred to the Commission's Member State Experts sub-Group. This group will also reflect on the extent and modalities for candidate and potential candidate countries to be associated to this initiative at the appropriate stage of the integration process. Appropriate association of certain non Member States may further be considered in the future. As requested by the Council, this Roadmap will be revisited at the end of 2011.

ANNEX

Members of the CISE (User Communities)	CISE monitoring and support functions
1. Maritime safety (including SAR) , maritime security and prevention of pollution caused by ships	Monitoring of compliance with regulations on the safety and prevention of pollution caused by ships (construction, equipment, crew/passengers, cargo); support of enforcement operations
	Monitoring of compliance with regulations on the safety of navigation (vessel traffic safety); support of enforcement operations
	Monitoring of compliance with regulations on the security of ships; support of enforcement operations
	Supporting safe and efficient flow of vessel traffic; vessel traffic management
	Early warning/identification of ships/persons in distress; support of response operations (search and rescue, salvage, place of refuge)
	Early warning/identification of maritime security threats, within the scope of SOLAS Chapter XI-2; support of response operations
	Early warning/identification of threats/acts of piracy or armed robbery; support of response operations
2. Fisheries control	Monitoring of compliance with regulations on fisheries; support of enforcement operations
	Early warning/identification of illegal fisheries or fish landings; support of response operations
3. Marine pollution preparadeness and response; Marine environment	Monitoring of compliance with regulations on the protection of the marine environment; support of enforcement operations
	Early warning/identification of incidents/accidents that may have an environmental impact; support of pollution response operations
4. Customs	Monitoring of compliance with customs regulations on the import, export and movement of goods; support of enforcement operations
	Early warning/identification of criminal trafficking of goods (narcotics, weapons, etc.); support of response operations
5. Border control	Monitoring of compliance with regulations on immigration and border crossing; support of enforcement operations
	Early warning/identification of cases of illegal migration or trafficking in human beings; support of response operations
6. General law enforcement	Monitoring of compliance with applicable legislation in sea areas, where there is policing competence and support to enforcement and/or response operations
7. Defence	Monitoring in support of general defence tasks, such as: • Exercising national sovereignty at sea; • Combating terrorism and other hostile activities outside the EU; • Other Common Security and Defence Policy tasks, as defined in Articles 42 and 43 TEU

GLOSSARY OF TERMS

BluemassMed:	Blue Maritime Surveillance System Med, Pilot project on integration of maritime surveillance co-financed by the European Commission
CISE:	Common Information Sharing Environment for the EU maritime domain
CSDP:	EU Common Security and Defence Policy
EDA:	European Defence Agency
EUROPOL:	European Law Enforcement Agency
EUROSUR:	European border surveillance system
GMES:	Global Monitoring for Environment and Security is the European Initiative for the establishment of a European capacity for Earth Observation
MARSUNO:	Maritime Surveillance in the Northern European Sea Basins, Pilot project on integration of maritime surveillance co-financed by the European Commission
PT MARSUR:	Project Team Maritime Surveillance - EDA project on 'maritime surveillance network'
SafeSeaNet:	Safe Sea Network; A European Platform for Maritime Data Exchange between Member States' maritime transport authorities.
SOLAS:	International Convention for the Safety of Life at Sea
TAG:	Technical Advisory Group; Composed of representatives of all relevant maritime surveillance user communities; under the chairmanship of the European Commission the TAG shall provide technical input to elaborating the draft Roadmap towards the creation of the CISE
VMS:	Satellite-based Vessel Monitoring System used in the Fisheries sector
Wise Pen:	A Team of five Admirals having produced a report to the EDA steering board: 'Maritime surveillance in support of CSDP'