Questions and answers on the Common Information Sharing Environment (CISE) and its contribution to maritime security

The Maritime Common Information Sharing Environment (CISE) seeks to further enhance and promote relevant information sharing between authorities involved in maritime surveillance from coastguards and navies to port authorities, fisheries controls, customs authorities and environment monitoring and control bodies. It is not replacing or duplicating but building on existing information exchange and sharing systems and platforms. Its ultimate aim is to increase the efficiency, quality, responsiveness and coordination of surveillance operations in the European maritime domain and to promote innovation, for the prosperity and security of the EU and its citizens. It is a cross-cutting tool of the EU Integrated Maritime Policy, and a building block of the EU Maritime Security Strategy.

Why is Maritime CISE needed?

By ensuring enhanced information exchange, the efficiency, quality, responsiveness and coordination of surveillance operations in the European maritime domain will be increased and innovation promoted, for the prosperity and security of the citizens of EU. In particular, information collected by one maritime authority and considered necessary for the operational activities of other authorities should be shared instead of being collected and produced several times.

What will Maritime CISE change?

Maritime surveillance professionals will have access to more relevant information within their existing systems and on their existing screens if maritime surveillance systems (computers) will be connected across sectors and borders at national and EU level. The idea is that information and knowledge will be exchanged near real time wherever possible and necessary. What is needed in particular is that military authorities (coast guards and navies) will share relevant information with civilian ones (and vice versa) so this will be one of the main priority areas for further work.

Will this not lead to duplication?

No, the intention is not to create any new maritime surveillance system, but simply to connect existing systems by making them interoperable. Existing systems which have already been developed under various sectorial policies (EUROSUR, SafeSeaNet, the National Single Window, etc) will therefore remain unchanged. A lot of progress has already been made to enhance information exchange in particular between civilian surveillance authorities and this progress is the point of departure of Maritime CISE.

Will Maritime CISE lead to any transfer of competence from Member States to the EU?

No. Maritime CISE is essentially a process for co-operation between national authorities. The role of the Commission is to act as a facilitator in order to ensure that cross-border issues are dealt with in the best possible manner.

The relevant maritime surveillance authorities who could be connected through Maritime CISE are almost all national authorities (some authorities at European and regional level could also connect).

How have the Member States been involved so far?

Member States have been fully involved in the process throughout the past three years, since the launch of the CISE roadmap in 2010. Progress is regularly discussed in expert group meetings with Member States representatives and much of the progress achieved until today has been achieved through Member State lead projects such as the co-operation project and various pilot projects.

The involvement of Member States will continue also in the future, inter alia through a project under the EU's 7th Research Framework Programme in order to test Maritime CISE on a large scale which is envisaged to be launched in autumn 2014.

If there are so many advantages with this policy, why doesn't the EU legislate?

Creating new legislation is not an objective as such. Various legislative initiatives of different sectors have led to enhanced information exchange (VTMIS Directive, CFP Regulation etc). At this stage, non-legislative measures are deemed more efficient in order to make further progress. For example, one of the main areas for further work is civil-military co-operation, and that is an area for which legislative measures are neither feasible nor desirable.

How does this process relate to the newly adopted maritime security strategy of the EU?

Maritime CISE is one of the building blocks to achieve the objectives of the EUMSS (European Union Maritime Security Strategy). Enhancing maritime awareness, surveillance and information sharing is one of the five work strands of the strategy adopted by the Council in June. This means that Maritime CISE is one of the actions to implement this strategy.

Does this process also include collaboration with third countries?

The process will focus on collaboration between EU Member States. This doesn't mean however that the process will exclude third countries which demonstrate a clear interest in participating in the project. The EU is always interested in close collaboration with such third countries to exchange best practices not only on exchange of surveillance information, but also on cooperation on maritime security issues. Cooperation with third countries is also one of the core elements of the Maritime Security Strategy.

What about data protection issues, will maritime surveillance data become publically available through this initiative?

No, maritime surveillance data will always be subject to data protection rules like any other data. This means that surveillance data which can be classified as personal data or commercially sensitive will not become public and will only be shared with authorities that have a justified need to receive the data (the need to know principle). Security mechanisms will also be put in place to allow the secure exchange of sensitive maritime surveillance data, on the basis of justified and bilateral agreements.

See also: IP/14/782

Contacts :

For the press:

Helene Banner (+32 2 295 24 07)

Lone Mikkelsen (+32 2 296 05 67)

For the public: **Europe Direct** by phone **00 800 6 7 8 9 10 11** or by e-mail