European Maritime Safety Agency

# CISE – incident alerting service (pre-operational) - Annex

The purpose of this document is to draft the specification for establishing a pre-operational "incident alerting service" in the CISE network. This service will exchange information about incidents occurred on board of a vessel or any type of maritime asset.

## Scope of the service

Sharing incident information is envisaged in CISE, since it is part of the CISE Data and Service model. The "incident alerting service" will be used by the personnel in charge to disseminate or consume information about incidents occurred on board of a vessel or any other type of maritime asset (including people infected by COVID-19).

The CISE "incident alerting service" is meant to be complementary to initiatives in place in the MS or at EU level (i.e. the notification service implemented within the maritime single window reporting system - SafeSeaNet) for two main reasons: CISE reaches a wider variety of Public Authorities comparing to sectorial networks (CISE is a cross sectoral initiative), and CISE can be used to exchange sensitive/classified information. CISE connects Public Authorities (PA) belonging to 7 different sectors: maritime security and safety, defence, law enforcement, fisheries, customs, marine environment and border control. Sharing incident information in CISE will contribute to:

- Sending and receiving information between Public Authorities in EU that are not connected to existing sectorial platforms, networks or communities;
- Simplifying the procedure in place in MS to distribute information among different Public Authorities (some MS are using CISE as a platform to share/distribute information among different legacy systems owned by different PA within the country);
- Addressing sensitive or classified information (i.e. list of passengers, crew list or detailed information about the persons affected by the incident).

This service will be implemented in three stages. In the 1st stage the service will be operated on the basis of the tools already implemented, in the 2nd stage the service will be connected to the MS legacy systems (automatizing the information sharing), and the 3rd stage will address also the exchange of sensitive/classified information. This set of specifications addresses the 1st stage of the service. The 2nd and 3rd will be planned on the grounds of the results of this 1st stage. It is important to mention that while the 2nd stage of this service could be planned during the Transitional Phase of CISE, the 3rd stage will be addressed when CISE will have moved to the Operational Phase.

## Service specifications

The configuration of the "incident alerting service" will be based on a push pattern to exchange information based on the "INCIDENT" CISE data model. The information disseminated in the 1st stage of the service will make use of the CISE UNCLASS network. Thus, the information shall be delivered to all the Participants (Public Authorities) connected to the nodes that requested to be part of this service.


CISE
Project funded by the European Union
cise@emsa.europa.eu
emsa.europa.eu/cise

The workflow (*) to be implemented for the 1st stage of this service is:

1. **Information Provider**. When an incident is detected by a Participant, the Participant's duty officer has to fill-in the "INCIDENT-DATAMODEL" and disseminate it through the CISE node by the CISE simulator (or any other tool implemented in the MS);
2. **Information Consumer**. The Node Operator has to verify the reception of INCIDENT-DATAMODEL from other nodes regularly. In case there will be information sent by other nodes, the Node Operator has to forward it to the Participants.

*(*) on the grounds of the interest by the MS to use this service, CISE TEAM can implement a solution to automatize the editing of the INCIDENT DATAMODEL (i.e. embedding this work in the CISE simulator);*

To enable this workflow the following actions are required:

1. *Action: Participants shall define the step in their procedure to be used by their duty officer to trigger the dissemination of the INCIDENT-DATAMODEL through the Node;*
2. *Action: CISE TEAM drafts the INCIDENT-DATAMODEL to be used as template and further filled-in by the duty officer based on the specific information related to the alert to be disseminated;*
3. *Action: CISE TEAM organizes the training (in VTC) to the Node Administrators and duties officer in order to perform their tasks;*
4. *Action: Node Administrators with the support of CISE TEAM will configure the service in their node instance.*

For the 1st stage the provision of this service must be considered on a "best effort" basis, therefore there will not be formal obligations (i.e. SLA) to be considered, however the Node Owner should commit resources in order to have the following in place:

3. **Information Provider**. The dissemination of information about an incident should be performed within 8 working hours since its detection;
4. **Information Consumer**. The Node Operator should verify the reception of INCIDENT-DATAMODEL from other nodes at least every 4 working hours.
5. **Report about the use of the service**. Every month the Node Owner shall draft a report including: number of messages sent, number of messages received and processed (further sent at least to one of the Participants), and if a message was not compliant with the service quality defined in this document provide a justification. The report should be sent to cise@emsa.europa.eu no later than 10 working days after the reporting period.

The provision of this service should be done at least during working hours (8 hours per day, 5 days per weeks, excluding bank holidays applied in the country where the node is installed).

The technical and operational support for the node and the CISE network will be provided by the CISE TEAM according to the service and procedures agreed during the 1st CISE Stakeholder Group (see [1]). Each Node Owner is in charge to maintain and operate the adaptors and the legacy systems connected to the node.

Once activated this service will be in a pre-operational mode until the end of the Transitional Phase, unless the Node Owner will decide to withdraw the provision of this service earlier.

# Resources

For the 1st stage of this pre-operational service the technical costs are already covered by the current network set-up. MS shall allocate human resources (Node Operator) in charge to manage the information disseminated through the CISE network as specified in section “Service ”.

For the 2nd and 3rd stage of the service DG MARE is looking into the possibilities to contribute to the costs that MS will incur, potentially through an implementation project for these stages of the service.

# Plan

The kick-off of this service will take place in VTC (indicatively end of June 2020).

| **Actions** | **Actor** | **Start** | **Timing to be completed** |
|---|---|---|---|
| Action 1 (procedure) | Node Owners | T0 | T0 + 4 weeks = T1 |
| Action 2 (incident data model template) | CISE TEAM | T0 | T0 + 4 weeks = T1 |
| Action 3 (training) | CISE TEAM / Node Owners | T1 (T0 should be completed) | T1 + 3 weeks = T2 |
| Action 4 (node configuration) | CISE TEAM / Node Owners | T2 (T1 shall be completed) | T2 + 2 weeks =T3 |
| T3: 1st stage of the service rolled out in pre-operation mode | | | |
| Reports. Node Administrator shall deliver the service report. | Node Owners | T3 | Every month |
| Revision of the service (VTC) | Node Owners | T3 | Every quarter |

# References

[1] EMSA, *Technical and Operational Support,* EMSA, 2019.