DJIBOUTI CODE OF CONDUCT / JEDDAH AMENDMENT

STANDARD OPERATING PROCEDURES FOR THE REGIONAL MARITIME INFORMATION SHARING NETWORK

OCTOBER 2023

FOREWORD

In an interconnected world, effective communication and collaboration are pivotal in addressing the challenges of maritime security and promoting global stability. These Standard Operating Procedures (SOPs) serve as a comprehensive guide to facilitate seamless information exchange and cooperation among participating entities in line with the objectives of the Revised Code of Conduct concerning the repression of piracy, armed robbery against ships and other illicit maritime activity in the Western Indian Ocean and the Gulf of Aden Area, also known as the Jeddah Amendment to the Djibouti Code of Conduct 2017, (DCoC/JA). They are primarily intended for the multi-agency National Maritime Information Sharing Centres (NMISCs) and other Centres and international partners working in collaboration with regional States in combating maritime security threats in the western Indian Ocean and the Gulf of Aden Area.

The multi-agency NMISC, established under the oversight of the respective National Maritime Security Committee and within the scope of the State's National Maritime Security Strategy, serves to enhance both national and regional Maritime Domain Awareness (MDA). Its purpose is to promote maritime safety and security through the reliable exchange of information. The NMISCs are a constituent part of the DCoC/JA information sharing network.

The DCoC/JA Information Sharing Network embodies the spirit of collective security, fostering partnerships and knowledge-sharing among countries, organizations, and institutions committed to ensuring safe and secure maritime environments. This document outlines the fundamental principles, procedures, and guidelines that will underpin the operations of this network.

As we navigate the complexities of maritime security threats, the SOP for the DCoC/JA Information Sharing Network stands as a testament to our shared dedication. By adhering to the guidelines detailed herein, we pave the way for swift and effective responses to evolving challenges, leveraging the strength of collaboration to protect our oceans and seas.

This SOPs file is a living document, subject to updates and improvements based on the experiences and insights of network participants. It is a product of collective efforts, reflecting the commitment of all involved parties to enhance maritime security and promote stability on regional and international scales.

We extend our appreciation to each participant, partner nation, and organization for their contributions to the development of this document. Your commitment to our shared objectives is vital as we work together to uphold the principles of the Djibouti Code of Conduct and the Jeddah Amendment.

The SOPs have been developed by subject matter experts from the DCoC/JA participating States with the support of the following international partners, representing the Friends of the DCoC/JA: India, United Kingdom, United States of America, IMO, UNODC, European Union, EU NAVFOR ATALANTA, INTERPOL, INTERPORTPOLICE, UNODC, SKY LIGHT, and the Jeddah Academy for Maritime Science and Security Studies. Thank you for your dedication to maritime security, and we look forward to a future of increased collaboration, stronger partnerships, and a safer maritime domain for all.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF APPENDICES

Appendices Number	Description

ACRONYMS AND ABBREVIATIONS

DCOC/JA- Djibouti Code of Conduct/Jeddah Amendment

NMISC- National Maritime Information Sharing Centre

ISN- Information Sharing Network

SOP- Standard Operating Procedures

EXECUTIVE SUMMARY

The Maritime domain is critical in sustaining humanity and the way of life as it has offered a medium of interconnectivity for centuries that has been vital for the growth and prosperity for many nations. Over 90% of the world's commerce moves by sea and 95% of telecommunication cables that are the bedrock of globalisation are carried via subsea fibre optic cables. The fishing industry that is critical in providing food security is sustained by artisanal fishing and Distant Fishing Nations (DFNs) that have fleets which traverse across the oceans. More than 50% of the world's oil and gas that is critical for industrialisation and transportation reaches the coastal nations through various supply chains across the sea.

The foregoing underscores the importance of having a holistic understanding of the maritime domain that is achieved through Maritime Domain Awareness (MDA). This is an effective understanding of anything associated with the maritime domain that could impact security, safety, the economy, or the environment. A robust MDA mechanism is essential for the DCOC/JA signatory states in achieving a sustainable blue economy.

In November 2022, the DCOC Regional High-Level Meeting on the implementation of the Jeddah Amendment adopted two resolutions; Resolution 1 on enhancement of the DCOC/ JA Information Sharing Network and Resolution 2 on responding to evolving maritime challenges and security priorities of Signatory states to the DCOC/JA. This consequently led to the Regional Workshop on Standard Operating Procedures for the DCOC/JA Information Sharing Network in August 2023.

The Standard Operating Procedures (SOPs) for the National Maritime Information Sharing Centres (NMISCs) provide a standardised consistent framework for the DCOC/JA signatory States in mitigating maritime security and safety threats stipulated in the DCOC/JA Agreement. The SOPs also provide the baseline guidelines that will enable the NMISCs to develop from Initial Operational Capability to Full Operational Capability.

The foregoing is achieved by bringing to the fore the importance of MDA and contextualising it within the DCOC/JA Information Sharing Network, the development of the mission, vision and core values of the centre, highlighting the overarching role of the National Maritime Security Committee (NMSCs) in the provision of an oversight role to the NMISCs, the roles and functions of the NMISCs, specific duties and responsibilities of the NMISC personnel, standardised working definitions and the DCOC/JA lexicon, data fusion procedures and the daily battle rhythm of the NMISC.

The SOPs also focused on key thematic areas on maritime security and safety that are cross cutting within the DCOC/JA signatory states. The SOPs have provided guidelines on the mitigation of the following maritime security and safety incidences; piracy and armed robbery against ships, Illegal unregulated and Unreported (IUU) fishing, drug smuggling, environmental incidents, maritime safety incidents, terrorist activity, irregular migration, trafficking and contraband smuggling, hybrid maritime security threats and Search & Rescue.

The mitigation measures highlighted in the key thematic areas of maritime security and safety are focused on a multiagency approach at the national and regional level. In this regard, a whole-of-government approach at the national level in tackling maritime security and safety threats is the bedrock to a robust regional maritime security framework.

The SOPs are meant to provide a guiderail to the DCOC/JA signatory States' NMISCs and can be adjusted as appropriate to suite the specific signatory State's needs while at the same time maintaining consistency so as to be relevant across the region. Consequently, this shall ensure that all the maritime stakeholders uphold laws and regulations and adhere to norms that promote a free, fair, and open maritime domain.

1. **OVERVIEW OF MARITIME DOMAIN AWARENESS (MDA)**

MDA is an essential part in ensuring maritime safety and security within the oceans. The mission and objective of MDA is to achieve a full understanding of the threats and opportunities in the maritime domain, including awareness of the maritime situation of the coastal state, through continuous collection and analysis of data.

This analysed data guides the rightful authorities in ensuring targeted and intelligence-led law enforcement activities. MDA also helps in the mitigation of contemporary maritime safety and security threats through actionable intelligence.

MDA involves collectively using technological aids and human sources to help better maritime law enforcement. Some of the technological devices utilised include; ships' automatic identification systems (AIS), Internet based tools, long range radars and long-range unmanned aerial vehicles (UAVs).

Currently, the major challenge of the MDA is proper synchronisation and combination of the information gathered. Also, the information should be collated appropriately and shared to other concerned entities and nations. An effective MDA mechanism can only be achieved through symbiotic and proactive sharing of the analysed information to find a common understanding.

The importance of MDA in securing the Sea Lanes of Communication (SLOCs) to enhance trade and the blue economy cannot be overemphasised. A robust MDA allows traders, ship insurers, charterers, and shipping organisations to know about their maritime assets and logistics. Specific MDA tools identify global shipping trends, monitor the movement of vessels, port activity, and trade flows, and share real-time vessel data.

Globalisation and International Trade have brought the importance of MDA to the fore. This ensures:

MDA provides the data, intelligence and international visibility required to enhance a competitive advantage. It allows shipping companies to monitor their commercial vessels and effectively optimise trade.

The complexities and interdependency involved in MDA oblige law enforcement agencies, maritime companies, business and financial institutions and governments to work in cooperation and keep a check on the supply chains. This collaborative approach also ensures that all maritime stakeholders operate within the stipulated environmental regulations and monitor any deceptive shipping practices. This is through the promotion of good shipping practices that ensure the territorial waters, and the exclusive economic zones (EEZs) of coastal states are safe and secure from any form of illegal activities like Human trafficking, Illegal unreported and unregulated fishing, Illegal human migration, and Contraband smuggling.

Many international organisations emphasise the need for all parties to focus jointly on ensuring maritime security and safety in the world's oceans. This can only be achieved through collective MDA.

2. REGIONAL PERSPECTIVE ON ENHANCING MARITIME INFORMATION SHARING UNDER THE DCoC/JA

Addressing sea blindness and bolstering MDA and maritime safety and security are paramount objectives of the DCoC/JA. Through the establishment of NMISCs, the sharing of crucial information, and collaborative endeavors involving signatory states and external partners, the realization of a secure maritime environment in the Western Indian Ocean and the Gulf of Aden, comes distinctly into focus. This regional viewpoint on maritime information sharing underscores the collective dedication to safeguarding the seas and nurturing a future characterized by stability and prosperity.

The maritime domain, a vital conduit of global trade and connectivity, faces multifaceted challenges, including piracy and armed robbery against ships, maritime terrorism, Illegal, Unreported and Unregulated (IUU) fishing, trafficking in arms, narcotics and psychotropic substances, illegal trade in wildlife and other items in violation of the Convention on International Trade in Endangered Species of Wild Fauna and Flora, illegal oil bunkering, crude oil theft, human trafficking and human smuggling, and illegal dumping of toxic waste. All these challenges underscore the urgent need for collaborative efforts and comprehensive strategies to ensure the security, sustainability, and prosperity of our maritime environment.

The maritime threat scenario is continually evolving, with emerging new threats, including cyber-attacks on ships, ports, and critical coastal infrastructure, maritime terrorism, and new modes of attacks on ships and vital coastal installations using drones, mines, etc. These challenges call for concerted efforts to address them. Cooperation between states and effective information sharing are essential to tackle these evolving threats. Drawing lessons from regional experiences in combating piracy and armed robbery, regional States have agreed to establish a robust information-sharing network to strengthen cooperation among signatory countries and effectively confront these challenges through resolute information sharing.

The regional initiative to enhance information sharing is spearheaded by the DCoC Working Group One on information sharing. Under this framework, the regional information sharing network is envisioned to be founded on strong national foundations, where every signatory nation establishes a robust National Maritime Security Committee (NMSC) framework. This structure oversees the operations of a dynamic Multi-agency National Maritime Information Sharing Center (NMISC), designed to gather, analyze, and disseminate dependable maritime safety and security information. The ultimate purpose of these centres is to empower signatory states with the information required to make judicious maritime security decisions, fortifying the safety of national waters.

This spirit of collaboration transcends national boundaries, with member states partnering to exchange vital information through NMISCs. This cooperative network further extends to the "Friends of the DCoC," including external allies such as the European Union, United Kingdom, United States of America, RMIFC, and RCOC, as well as key stakeholders like the maritime industry and coastal communities. These partnerships are fortified through building strong relations to face common challenges and establishing pathways for enriched maritime information sharing.

To realize the DCoC's vision, a meticulous roadmap has been developed and adopted by the DCoC. This blueprint synthesizes feedback from the working group on Enhancing Information Sharing and insights gleaned from experts adept at architecting robust information-sharing networks. The roadmap outlines a strategy involving the inception and operationalization of NMISCs in all signatory states. This process encompasses identifying the core operational requisites, gauging existing capabilities, addressing gaps, and directing resources and capacity building to bolster the efficacy of NMISCs across all participating states.

This regional perspective on maritime information sharing underscores the collective commitment to safeguarding the oceans and fostering an era of unwavering stability and prosperity.

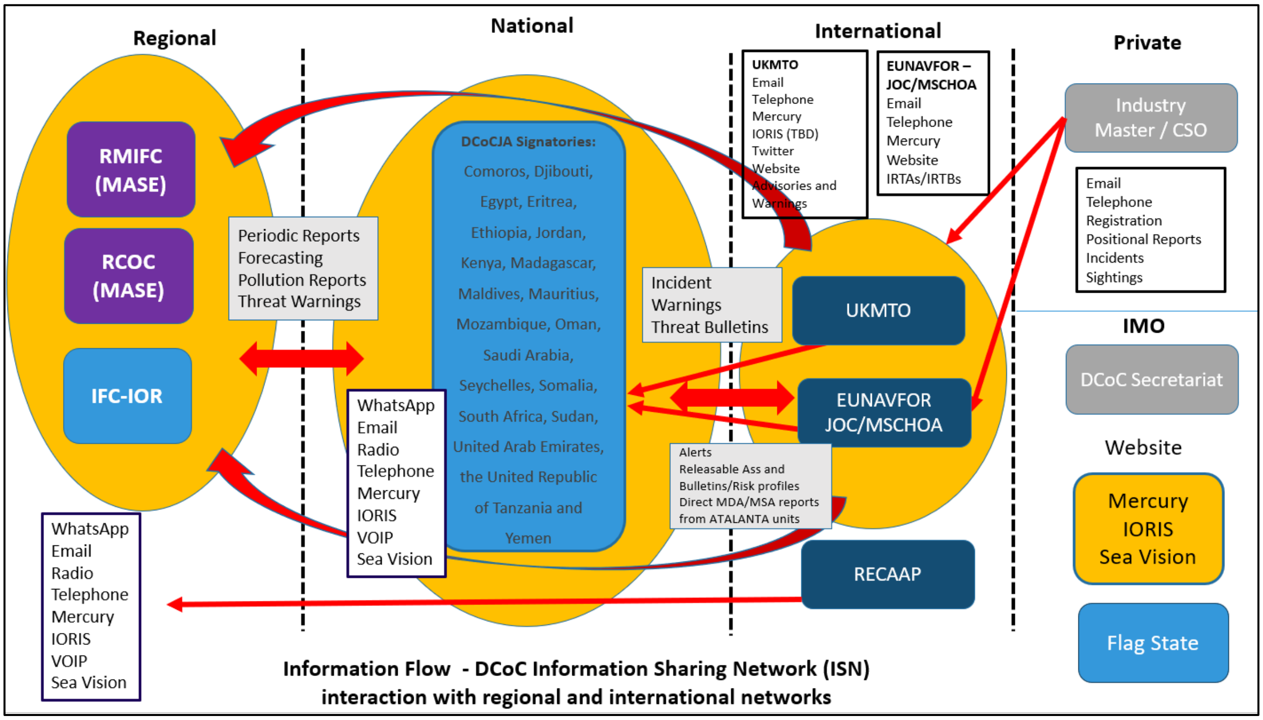


Figure 1. DCoC Information Sharing Network Architecture

3. MISSION, VISION, AND CORE VALUES OF NMISCs

The effective operationalisation of the NMISCs shall be guided by the following Mission, Vision, and Core Values;

Mission:

The multiagency National Maritime Information Sharing Centre (NMISC) shall collect, analyse, and share maritime safety and security information in order to enhance MDA and understanding. This will empower national maritime stakeholders and facilitate inter-agency cooperation to ensure safety, security, and economic prosperity in the maritime domain.

Vision:

1. All national agencies with responsibility for aspects of maritime security actively collaborate and engage in seamless information sharing through the NMISC.

2. The NMISC actively facilitates inter-agency coordination, cooperation and communication and supports the implementation of the National Maritime Security and Facilitation Committee's policies through information exchange and the adoption of best practice.

3. The NMISC facilitates effective operational responses through the timely provision of accurate, actionable information to entities responsible for exercising direct command and control over maritime assets.

4. Through the full realization of its mission, the NMISC acts as the national focal point for international/regional information sharing and cooperation.

5. The NMISC achieves its mission through ensuring the highest standards of integrity, proactivity, professional training, and motivation of its staff, supported by competent managers and effective equipment.

Core Values:

To fulfil its mission and achieve its vision the NMISC operates based on key core values which are as follows:

1. Collaboration: Encouraging cooperation and collaboration among all stakeholders recognizing that maritime security is best achieved through collective efforts.

2. Information Sharing: Promoting the timely exchange of accurate and relevant information respecting security and privacy considerations.

3. Trust: Building and maintaining trust among participants by fostering open communication integrity and mutual respect.

4. Innovation: Embracing technological advancements and innovative approaches to enhance information sharing and maritime security capabilities.

5. Professionalism: Upholding the highest standards of professionalism competence and ethics in all activities.

6. Continuous Improvement: Committing to a culture of ongoing learning evaluation and improvement to adapt and respond effectively to emerging threats and challenges.

4. ROLES AND FUNCTIONS OF NATIONAL MARITIME SECURITY COMMITTEES AND NATIONAL MARITIME INFORMATION SHARING CENTRES

Within the DCoC information sharing framework, the National Maritime Security Committee has an overarching responsibility in ensuring the effective operationalization and running of the Multiagency National Maritime Information Sharing Centre. The key roles of the NMSC are as follows:

1. Facilitating full consultation on security issues,
2. Identifying Security Threats and Vulnerabilities,
3. Establishing Security Priorities,
4. Planning, Co-ordinating and Evaluating Security Initiatives,
5. Developing or contributing to the National Maritime Security Strategy,
6. Handling major security issues with multi-organization implications,
7. Addressing Jurisdictional Issues involving member organizations.

The National Maritime Information Sharing Centre has the following roles and functions within the DCoC Information Sharing Network;

1. **Enhance maritime security**: By sharing information and intelligence related to maritime threats such as piracy, smuggling and terrorism the NMISC will contribute to improved maritime security. This helps in preventing illegal activities, managing maritime risks, and ensuring the safety of maritime trade and transportation.

2. **Effective MDA**: Collecting, analyzing, and disseminating information about maritime activities within a country's territorial waters and exclusive economic zone. This helps to develop a comprehensive understanding of maritime traffic, identify potential security threats, and respond to incidents in a timely manner.

3. **Coordination and collaboration**: the NMISC acts as a central point for coordinating and collaborating with various stakeholders involved in maritime security. This includes government agencies, law enforcement, naval forces, intelligence agencies and industry partners. By fostering collaboration and information sharing NMISC can improve the overall effectiveness of maritime security efforts.

4. Improved response capabilities: The timely sharing of accurate information and intelligence enables faster and more effective responses to maritime incidents and threats. An NMISC can facilitate communication and coordination among different response agencies, improving their ability to address security challenges, conduct search and rescue operations and respond to environmental hazards.

5. Maritime situational awareness: Through the collection and analysis of maritime data the NMISC can develop comprehensive situational awareness of the maritime environment. This helps in monitoring and managing maritime traffic, identifying patterns of suspicious activities, and supporting decision-making processes related to maritime security and resource allocation.

6. International cooperation: the NMISC plays a crucial role in facilitating international cooperation and information sharing with neighboring countries and regional maritime security initiatives. This helps in addressing transnational maritime crimes, enhancing regional security, and promoting maritime stability in an interconnected global maritime domain.

5. **DUTIES AND RESPONSIBILITIES OF NMISC PERSONNEL**

Head of NMISC

Executes the Centre mission.

Determines priority of cases

Responsible for overall Coordination Centre performance

Briefs commanders and senior staff

Handles media requests and interactions.

Maintains oversight of the Centre budget

Maintains oversight of Centre manning

Overall administration of the Coordination Centre

Represents the Centre in court and any other legal commitments.

Coordinates with external organizations

Ensures the Centre has all available technology to support the mission.

Ensures national, regional, and international information exchange is conducted to the maximum extent possible

Head of Operations / Deputy Head of NMISC

Manages the day-to-day operation of the Centre.

Establishes work plans based on priority of cases.

Briefs the Head, commanders, and senior staff.

Provides support to the Head on media requests and interactions.

Manages the Centre budget.

Manages Centre internal/external training.

In charge of coordination and planning of the watch floor

Manages Centre manning.

In charge of validation of productions

Leads crisis management.

Duty Officer / NMISC Supervisor

Supervises the day-to-day operation of the Centre.

Assigns work plans based on priority of cases.

Briefs the Deputy Head and Head of the Centre

Based on the budget, ensures the Centre is properly supplied

Executes internal training program.

Manages and coordinates subordinate duties.

POC with the outside world regarding collection and sharing of information.

Directs orientation of info searches

Assists Head of Operations during crisis

Reviews and Approves Centre products.

Organize ad hoc meetings for incidents.

Manages Centre manning.

Assistant Duty Officer

Carries out regular checks of communications via emails, chat and/or phone.

Updates Centre Shift Log

Searches for information by calling partners in the maritime sector by phone or email.

Prepares and compiles daily information for the weekly and monthly reports.

Prepares the watch floor for visitors.

Carries out weekly communications checks by phone, email, or chat to other operational centres.

Contacts all national informants dispersed and present in the different coastal localities.

Analyst

Completes daily work plans.

Maintains a high level of Area of Responsibility situational awareness.

Maintains expert knowledge of available tools and information resources.

Has strong knowledge of AOR patterns of life (vessels, weather, & fish migrations)

Conducts analysis of available maritime information

Adjusts MDA tool settings to operate at peak performance.

Analyzes system-generated alerts and warnings.

Identifies pertinent maritime information for further analysis.

Keeps the Centre Supervisor informed of work plan progress.

Communicates with other remote Users via installed chat tools.

Reviews watch lists.

Develops and delivers briefings to the Center Supervisor, Deputy Head, and the Head

Operator/ Watchkeeper/ WatchStander

In charge of daily communications technology check and proper operation of MDA platforms in the Centre

Ensures the monitoring of MDA platforms as well as available open and online sources.

Monitors and reports vessels of interest (VOIs)

In charge of collecting and classifying maritime events and information according to the Centre's thematic areas of interests

Drafts reports on maritime events and information.

Updates daily production matrices

IT/Technology Specialist

Completes daily work plans.

Ensures Centre infrastructure functions at peak capability.

Identifies shortfalls in the Centre communications architecture.

Ensures Centre IT equipment is up to date.

Ensures Centre IT equipment is able to support required software.

Ensures Centre software tools are of the latest versions.

As required, coordinates with software tool developers and technicians to resolve issues.

Adjusts MDA tool settings to operate at peak performance.

Analyzes system-generated alerts and warnings.

Communicates with other remote Users via installed chat tools.

6. WORKING DEFINITIONS AND CATEGORISATION OF MARITIME SAFETY AND SECURITY INCIDENTS

Piracy and Armed Robbery against Ships

Piracy. Article 101 of the UNCLOS defines piracy as any of the following acts:

> (a) Any illegal act of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:
>
> (i) On the high seas, against another ship, or against persons or property onboard such ship.
>
> (ii) Against a ship, persons, or property in a place outside the jurisdiction of any State.
>
> (b) Any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft.

(c) Any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).

Armed Robbery against Ships. In accordance with the Code of Practice for the Investigation of Crimes of Piracy and Armed Robbery against Ships of the International Maritime Organisation (IMO) Assembly Resolution A.1025(26), armed robbery against ships is defined as:

(a) Any illegal act of violence or detention, or any act of depredation, or threat thereof, other than an act of "Piracy", committed for private ends and directed against a ship, or against persons or property onboard such ship, within a State's internal waters, archipelagic waters, and territorial sea.

(b) Any act of inciting or of intentionally facilitating an act described above.

Note*: It has been observed that sometimes the exact location of an incident is unavailable in order to classify it as piracy and armed robbery. Hence, while capturing the incident, the sub-categories used in the Piracy and armed robbery against ships cluster are listed below.*

3 **Sub-categories of Piracy and Armed Robbery against Ships**. The incidents of piracy and armed robbery (attempted/ successful) are classified as follows:

(a) **Hijack**. An illegal act of violence where attackers have illegally boarded and taken control of a ship against the crew's will with an objective which could include armed robbery, cargo theft or kidnapping.

(b) **Kidnap**. An illegal act of violence involving unauthorised forcible removal of persons belonging to the vessel.

(c) **Attack**. An act of violence, where a ship has been subjected to an aggressive approach by a vessel AND weapons have been discharged.

(d) **Illegal Boarding**. An act where persons have boarded a ship, either aggressively or passively, with the intent to steal or cause harm but HAVE NOT taken control. Command remains with the Master.

(i) **Sea Theft**. Any illegal act of stealing property from a vessel without any violence against the crew or passengers.

(ii) **Sea Robbery**. Any illegal act of stealing property from a vessel committed with arms or with violence against the crew or passengers.

(j) **Attempted Boarding**. An action involving a close approach or hull-to-hull contact where boarding paraphernalia is employed or visible in the approaching boat, but is thwarted by BMP measures, including Privately Contracted Armed Security Personnel (PCASP), weather conditions, or lack of appropriate equipment, etc.

(k) **Suspicious Activity**. An action that cannot be accounted for in the prevailing conditions, sudden changes in course towards ship and/or aggressive behaviour by the craft.

Contraband Smuggling. Contraband is any item that is illegal to produce or possess. Smuggling is most prominently a form of customs violation, avoidance of duties, and tax fraud. Contraband smuggling involves movement of goods that are against the law to be imported or exported.

(a) **Drug Smuggling**. The broad understanding of drug smuggling is derived from the commentary of the United Nations Convention against Illicit Traffic in Narcotics Drugs and Psychotropic Substances, 1988. For the purpose of this report, “drugs” also refers to UNODC’s definition of any natural or synthetic substances in Schedules I and II under the Controlled Substances Act, and “illicit traffic” under the International Drug Control Convention. The report categorises drugs by *type* and *effect* under the following definitions:

(i) **Opioids**. Substances that bind to μ-opioid receptors, including opium and derivative substances, such as heroin and morphine. Also includes semi-synthetic opioids of varying strength such as codeine, fentanyl, carfentanyl, methadone, hydrocodone, hydromorphone, meperidine, tramadol, and oxycodone.

(ii) **Cannabinoids**. All substances derived from or synthesized to emulate and bind to cannabinoid receptors in the brain. Includes hashish, cannabis, ganja, charas, marijuana, bango, and synthetic cannabinoids.

(iii) **Amphetamine Type Substances (ATS)**. Amphetamine and derivatives, predominantly methamphetamine, captagon, ecstasy, syabu, yaba, and mephedrone; includes ephedra as a precursor for synthetic drugs.

(iv) **Other Drugs**. There are several additional drugs noted in this report that are not easily placed into these categories. They include khat, cocaine, LSD, magic mushrooms, and ketum.

(b) **Domestic Products Smuggling**. Goods that are either common household products or manufactured items. Examples include rice, flour, salt, turmeric, gas cylinders, and cars.

(c) **Natural Resources Smuggling**. Goods or resources that are harvested from nature, including gold, wood, sand, and metals.

(d) **Fuel Smuggling**. Smuggling fuel is a form of arbitrage aimed at bringing lower priced fuel from one jurisdiction into a higher priced jurisdiction in order to obtain a profit through the price differential. Examples include petroleum, crude oil, and gas.

(e) **Tobacco Smuggling**. Any product of the tobacco plant, including cigarettes, cigars, and chewing tobacco.

(f) **Alcohol Smuggling**. Smuggling of alcoholic beverages that are illegal to be imported or exported.

(g) **Weapons Smuggling**. Goods designed for inflicting bodily harm or any form of damage, including guns, knives, explosives, and fireworks.

(h) **Wildlife Smuggling**. Live animals, bird, or animal parts listed under the Convention on International Trade in Endangered Species (CITES) of Wild Fauna and Flora, including elephant tusks, pangolin scales, sea cucumber, tortoises, turtle eggs, and shells.

(j) **Others**. Items not falling in any of the categories above such as ancient artefacts, ammonium nitrate, etc.

Illegal Unreported and Unregulated (IUU) Fishing

5. **IUU Fishing**. A range of offences covering fishing without permission or in violation of regulations of the flag state or host nation, misreporting, or failure to report catches to relevant authorities where required to do so, fishing vessels without a flag or national registration, or fishing on stocks without management measures in place. These following terms are defined in the International Plan of Action to prevent, deter, and eliminate IUU fishing (IPOA-IUU), prepared by the Food and Agriculture Organization (FAO) of the United Nations:

(a) **Illegal Fishing**. Fishing conducted by national or foreign vessels in waters under the jurisdiction of a State, without the permission of that State, or in contravention of its laws and regulations; conducted by vessels flying the flag of States that are parties to a relevant regional fisheries management organisation but operate in contravention of the conservation and management measures adopted by that organisation and by which the

States are bound, or relevant provisions of the applicable international law; or in violation of national laws or international obligations, including those undertaken by cooperating States to a relevant regional fisheries management organisation.

(b) **Unreported Fishing**. Fishing activities which have not been reported, or have been misreported, to the relevant national authority, in contravention of national laws and regulations; or are undertaken in the area of competence of a relevant regional fisheries management organisation which have not been reported or have been misreported, in contravention of the reporting procedures of that organisation.

(c) **Unregulated Fishing**. Fishing Activities in the area of application of a relevant regional fisheries management organisation that are conducted by vessels without nationality, or by those flying the flag of a State not party to that organization, or by a fishing entity, in a manner that is not consistent with or contravenes the conservation and management measures of that organization; or in areas or for fish stocks in relation to which there are no applicable conservation or management measures and where such fishing activities are conducted in a manner inconsistent with State responsibilities for the conservation of living marine resources under international law.

6. While undertaking analysis of the reported incidents, the Centre observed that it is difficult to categorise incidents into distinct ‘illegal’, ‘unreported’, or ‘unregulated’ fishing. Therefore, to avoid

inaccurate representation of data, the reported incidents are categorised as 'Local IUU Fishing' and 'IUU Fishing - Poaching.'

(a) **Local IUU Fishing**. IUU fishing conducted by fishing vessels of a state, in the waters under the jurisdiction of the flag state, without valid license/ permit of that state, or in contravention of its laws and regulations. Offences by licensed foreign fishing vessels are also counted under this category.

(b) **Poaching**. IUU fishing conducted by foreign flagged vessels, in waters under the jurisdiction of a state, without valid license/ permit of that state, or in contravention of its laws and regulations.

Irregular Human Migration

7. **Migrant Smuggling**. United Nations Office on Drugs and Crime (UNODC) defines Migrant Smuggling as the facilitation, for financial or other material gain, of irregular entry into a country where the migrant is not a national or resident.

8. **Human Trafficking**. UNODC defines Human Trafficking as the recruitment, transportation, transfer, harbouring or receipt of people through force, fraud, or deception, with the aim of exploiting them for profit.

9. **Irregular Human Migration**. The incidents have been placed in a single category of Irregular Human Migration due to the challenges associated with conclusively determining the will and intent of illegal migrants.

***Note**: Only Migration/ Trafficking incidents/ attempts in the maritime domain are recorded and analysed by the Centre.*

Maritime Safety Incidents (Accidents / Casualties)

10. **Fire**. Incidents involving fire and/ or explosion in the maritime domain.

11. **Grounding**. Incidents involving vessel running aground.

12. **Collision**. Incident involving collision of vessels or collision of vessel with navigational hazards/ aids.

13. **Mechanical Failure**. Incidents involving failure of mechanical shipboard systems such as engine, steering, switchboards etc.

14. **Medical Evacuation (MEDEVAC)**. Incidents involving evacuation of crew from their vessel due to a medical emergency.

15. **Search and Rescue (SAR)**. Incidents involving conduct of search and rescue by authorities or maritime personnel to locate missing person or vessel.

16. **Sunk**. Incident involving vessels sinking at sea due to maritime accidents attributable to collision, weather, or other constraints.

17. **Capsize**. Incident involving capsizing of vessels sinking at sea due to maritime accidents attributable to collision, weather, or other constraints.

18. **Flooding**. Incidents involving water ingress into the vessel not classified as collision, grounding, sunk, capsize, etc.

19. **Man Overboard**. Incidents involving crew/ passengers falling overboard from a vessel.

20. **Vessel Detained.** Incidents involving apprehension of vessels by maritime authorities of a state for engaging in unauthorised activities within the maritime jurisdiction of the state.

21. **Violent Confrontation.** Incident involving acts of violence (such as use of force) in an encounter between two or more parties in the maritime domain.

22. **Cargo Mishap.** Incidents involving cargo including containers falling overboard at sea.

23. **Missing**. Incidents involving mariners reported missing due to accidents at sea. 24. Death. Incidents involving loss of life at sea attributable to collision, weather, or other constraints.

25. **Grouping of Maritime Safety Incidents.** For ease of comprehension, the individual categories have been grouped into the following three broad classifications (some incidents may involve both vessels and individuals):

(a) **Incidents Affecting Vessels.** Fire, Grounding, Collision, Mechanical Failure, Flooding, Sunk, Capsize, Cargo Mishap and SAR.

(b) **Incidents Affecting Individuals.** MEDEVAC, Man Overboard, Missing and Death. (c) Incidents with Legal Connotations. Vessel Detained and Violent Confrontation.

Maritime Security Threats (Hybrid)

26. An action conducted in the maritime domain by state or non-state actors, whose goal is to undermine or harm a target at sea or in maritime ports by combining overt and covert military and non-military means, conventional capabilities, irregular tactics and formations, indiscriminate violence, and coercion, as well as criminal disorder. 27. Includes the use of conventional military measures like rockets, missiles, and floating mines, with unconventional measures like unmanned, remotely controlled Water Borne Improvised Explosive Devices (WBIEDs), unmanned aerial vehicles (UAVs), and drones.

Maritime Terrorism

While Terrorism has not yet been universally defined, Maritime Terrorism can be broadly defined into two main categories:

(a) **At Sea**. Maritime terrorism incidents involving attacks against ships at sea.

(b) **From the Sea**. Maritime Terrorism from the Sea comprises of direct or indirect attacks ashore from the sea.

Maritime Cyber Security Threats

Single actors or groups targeting maritime systems, vessels, or organizations for financial or other gains to undermine electronic systems, or to cause disruption, panic, and fear, including attacks using malware, viruses, trojans, spyware, ransomware, adware, botnets, phishing, and denial of service. These may include attacks on Information Technology (IT) and/or Operational Technology (OT) systems.

Environment Pollution & Climate Change

30. The Centre monitors incidents related to the environment and climate change, including:

(a) **Natural Events**. Natural Events, or incidents involving violent or destructive natural events beyond human control, such as earthquakes, tsunamis, tropical storms and hurricanes, and lightning strikes.

(b) **Environmental Hazards**. Environmental Hazards, or any substance, situation, or event which has the potential to threaten the surrounding natural environment or adversely affect people's health.

Others

31. This category encompasses incident and events in the maritime domain which do not fall under the previous eight definitions.

7. **NATIONAL VESSEL OF INTEREST (VOI) LEXICON**

The National Vessel of Interest (VOI) Lexicon aims to provide rapid and readily understood categorization guidance to describe vessels that may post a national security, law enforcement, or regulatory threat to the DCoC signatory states. This unclassified standardized categorization aims to minimize confusion, facilitate a shared understanding of the potential threat of a VOI, and maximize intelligence and information sharing among NMISCs. This VOI Lexicon intends to support agencies focused on maritime security and safety in decision making in relation to the prevailing threat. The VOI Lexicon is also intended to assist in the development of the most appropriate response.

CATEGORIES		
1. NATIONAL SECURITY	**2. LAW ENFORCEMENT**	**3. REGULATORY**
A. Armed Robbery against Ships	**A**. Piracy	**A**. Environmental incidents (Pollution and Biofouling)
B. IUU Fishing	**B.** Contraband Smuggling	**B.** Port State Control/Flag State Control

C. Maritime Safety Incidents	**C**. Irregular Human Migration	**C.** Public Health
D. Maritime Security Threats {Hybrid}	**D**. Environmental Pollution and Climate Change	**D**. Sanctions/UN Security Council Resolution Violations
E. Maritime Terrorism	**E**. Trafficking in Arms	**E**. Unusual transit
F. Maritime Cyber Security Threats	**F.** Trafficking in narcotics and Psychotropic substances	**F.** Reporting False Information
	G. Illegal trade in Wildlife and other items in violation of the Convention on International Trade in Endangered Species (CITES) of wild fauna and flora	
	H. Illegal Oil Bunkering	
	I. Crude Oil Theft	
	J. Illegal dumping of toxic waste	

8. DATA FUSION PROCEDURE: OODA LOOP MODEL

The NMISC must have the capability of collecting, processing, analyzing and dissemination of maritime safety and security events in a timely manner. This shall enhance effective response by the relevant maritime law enforcement agencies. The Observe Orientate, Decide and Act (OODA) loop Model can be used to increase the efficiency of decision making and action taken by the Center.

The OODA Loop model is a four-point decision loop that supports quick, effective, and proactive decision-making. The four stages of the Loop are:

Observe – collect current information from as many sources as practically possible.

Orient – analyze this information and use it to update the current situation.

Decide – determine a course of action.

Act – follow through on the decision and course of action.

The OODA Loop cycle can be continuous by observing the results of the initial actions, assessing whether they achieved the intended results, reviewing and revising the initial decision, and moving to the next action. Observing and orienting correctly are key to making a successful decision. If these steps are flawed, they'll lead to make a flawed decision, and, subsequently, a flawed action.

Stage 1. Observe

At this initial point in the loop, the personnel should be gathering new information, and will need to be aware of any important, unfolding events. The more information gathered enhances a more accurate situational understanding.

Stage 2. Orient

Orientation focuses on the interpretation of the situation. This is important because the interpretation will significantly impact the decision. The Orientation has to be as objective as possible and avoid any form of inherent biasness based on previous experiences. By becoming more aware of previous perceptions, and by speeding the ability to orient to reality, one can move through the decision loop more quickly and more effectively. Constant and continuous re-orientation is important as new information comes in at the Observe stage, anything new needs to be processed and reorientated accordingly.

Stage 3. Decide

Decisions are made based on the observations made and the orientation. As the OODA Loop is continuous, new observations keep arriving, decisions and subsequent actions will change accordingly. Continuous appreciation of the situation and the decisions are a response made are a response to the continuous observation and reorientation.

Stage 4. Act

The Act stage is the implement the decision. Once a decision has been made, one can go back to the observe stage and judge the effects of the action. Actions can influence the rest of the cycle, and it's important that one keeps learning from the actions taken.

The goal of the model is to increase the speed with which the personnel at the NMISC orient and re-orient based on the new information that is received. The OODA loop enables the personnel to make a smooth and direct transition between what is observed, how it is interpreted and what is action is taken on it.

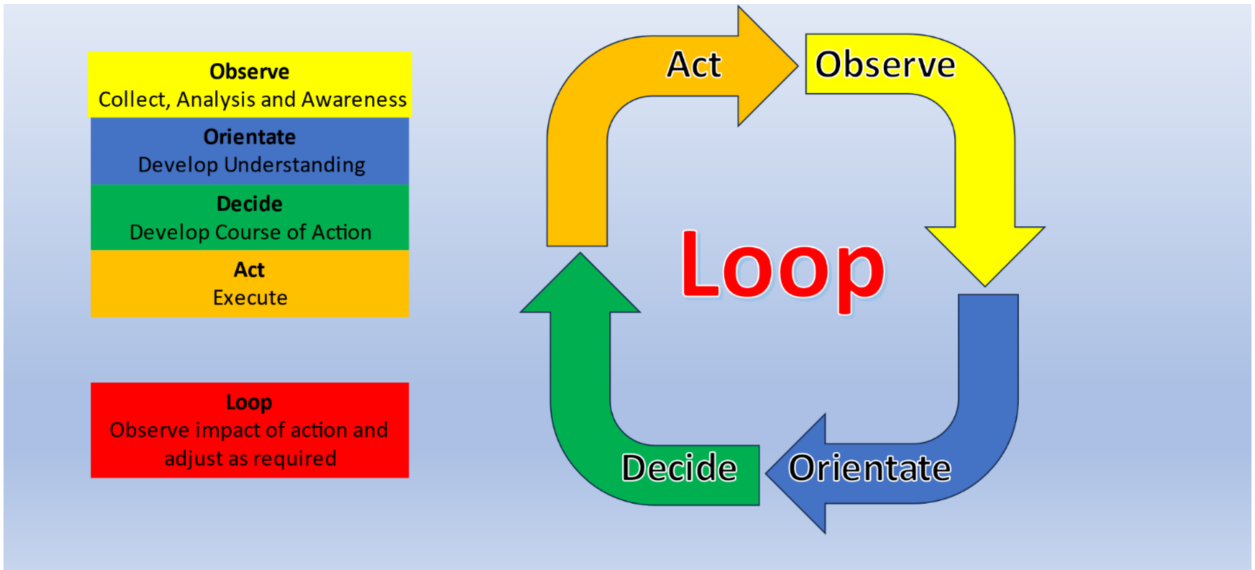


Figure 2. OODA Loop

9. **THEMATIC ANALYSIS AND REPORTING PROCEDURES**

PIRACY AND ARMED ROBBERY AGAINST SHIPS SOP

The following SOP shall be implemented by the NMISC in case a Piracy and Armed Robbery against Ships ALERT is received:

1. Piracy and Armed Robbery against Ships alert could be received via the Ship Security Officer, the flag State, Mercury Chat, IORIS, VTS, SEAVISION, GMDSS, INTERPOL, Intelligence Agencies, Regional Fusion Centres, IMB-PRC, Maritime and Aviation Stakeholders, EUNAVFOR, CMF, UKMTO, National Focal Points and by telephone, fax, and e-mails.

2. Verify and share the information with other sources (e.g., UKMTO – MSCHOA – EUNAVFOR – NATO Shipping Centre, CMF), Regional Fusion Centres, RMRCCs, EMSA, Vessels in Vicinity, Maritime and Aviation Stakeholders and other relevant contact details as listed in the directory.

3. In case of a Piracy and Armed Robbery against Ships related incident, inform the NFPs and Law Enforcement Agencies. Try to get as much information about the ship and incident. Inform the respective Law Enforcement entities of the flag and coastal States.

4. Issue the Initial report in accordance with MSC.1/Circ.1333 and send it to IMO, all NFP's, NMISCs and other relevant international agencies.

5. Keep monitoring the channel / frequency where the alert was received and record communication into the logbook.

6. Assist the NFP and Lead agencies by providing on-going details of the event.

7. Issue a security warning to other interested parties including MRCCs / coastal stations, providing the details of event into account guidance contained in MSC/Circ.1073.

8. Assist NFPs in verifying the presence and contact details of ships in the area of the event.

9. As soon as additional information is acquired, prepare a follow-up report to update the stakeholders on the event. Several follow-up reports can be issued related to the same piracy event.

INITIAL REPORT	
Priority	[How is priority determined and categorized?]
Source of Piracy and Armed Robbery against Ships Incident report	
Date and Time (including time zone)	
Ship's Name	
Ship's Type	
Ship Manifest	
Flag	
Call Sign	
MMSI	
IMO No.	
Ship Voyage Data	
Details of Owner/Operator	
Insurance Details	
Inmarsat ID. (plus Ocean Region Code)	
Other relevant information	
SHIP'S POSITION	
Latitude	
Longitude	

Bearing and Distance from known point	
Course	
Speed	
Status (e.g., Hijacked, ongoing attack, etc)	
NATURE OF EVENTS	
Attack	
Attempted Attack	
Suspicious Activity	
Any Other relevant Information	
Information received by	
Action taken	

POSITION OF INCIDENT	
Latitude	
Longitude	
Course	
Bearing and Distance from known point	
Speed	
Status	
Name of the area	
DETAILS OF INCIDENT	
Sailing	
At the anchor	
At berth	
Method of attack	
Description of suspected craft	

Number and brief description of Pirates /Robbers.	
What kind of weapon did the pirates / robbers carry.	
Any other relevant information (language spoken)	
Injures to crew and passengers	
Damage to ship (Which part of the ship was attacked)	
Brief details of stolen property / cargo	
Action	
Taken by the master/ crew	
Was incident reported to coastal Authority and to whom?	
LAST OBSERVED MOVEMENTS OF PIRATE / SUSPECTED CRAFT	
Date	
Time	
Position	
Course	
Bearing and Distance	
Speed	
COMMUNICATION STRUCTURE	
Communication channel between the NMISC and the incident reporter	
Communication channel between the NMISC and vessels and aircrafts in vicinity	
Communication channel between the NMISC and leading agency	
Appropriate Coast Radio Station	

VHF / MF/HF / Channel / frequency	
INMARSAT Ld. (plus Ocean Region Code)	
MMSI	
Date / time of report.	

ASSISTANCE REQUIRED	
Search and Rescue	
Medical Evacuation	
Assets and Equipment	

PIRACY AND ARMED ROBBERY FLOWCHART

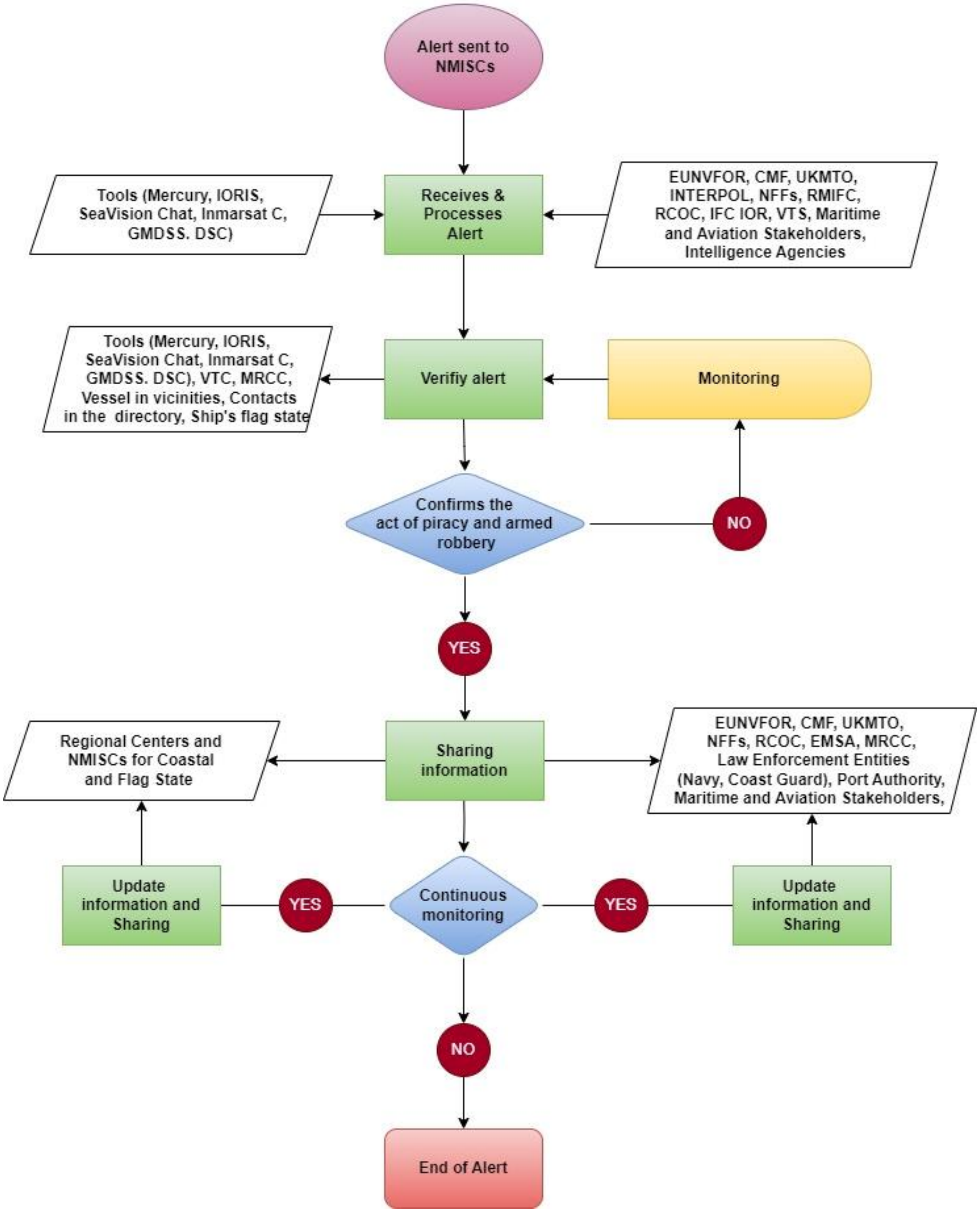

Alert sent to NMISCs
Tools (Mercury, IORIS, SeaVision Chat, Inmarsat C, GMDSS. DSC)
Receives & Processes Alert
EUNVFOR, CMF, UKMTO, INTERPOL, NFFs, RMIFC, RCOC, IFC IOR, VTS, Maritime and Aviation Stakeholders, Intelligence Agencies
Tools (Mercury, IORIS, SeaVision Chat, Inmarsat C, GMDSS. DSC), VTC, MRCC, Vessel in vicinities, Contacts in the directory, Ship's flag state
Verifiy alert
Monitoring
Confirms the act of piracy and armed robbery
NO
YES
Regional Centers and NMISCs for Coastal and Flag State
Sharing information
EUNVFOR, CMF, UKMTO, NFFs, RCOC, EMSA, MRCC, Law Enforcement Entities (Navy, Coast Guard), Port Authority, Maritime and Aviation Stakeholders,
Update information and Sharing
YES
Continuous monitoring
YES
Update information and Sharing
NO
End of Alert

Figure 3. Piracy and Armed Robbery flowchart

NMISC – IUU FISHING SOP

The following SOP shall be implemented by NMISC in case an IUU Fishing ALERT is received:

1. IUU Fishing alert could be received via Skylight, IORIS, SeaVision Chat, Domestic Fisheries Community, Vessel Management System (VMS), Maritime Stakeholders, Regional Fusion Centres, National Focal Points, Telephone, Fax, Emails.

2. Verify and share the information with other sources (e.g., Global Fishing Watch, Indian Ocean Tuna Commission (IOTC), Southwest Indian Ocean Fisheries Governance and Shared Growth Project (SWIOFiSH), Flag State, Skylight & IORIS) contact details as listed in the directory.

3. In case of IUU Fishing related incident, inform the NFPs. Try to get as much information about the ship and event. Inform the respective NMISC of the flag and coastal states. (List of NMISC's of the region – should be available in the National Centre.)

4. Keep monitoring the channel / frequency where the alert was received and record communication into the log Book.

5. Assist the NFP by providing on-going details of the event.

6. Assist NFPs in verifying the presence and contact details of ships in the area of the event for possible direct contact with those ships by the NFPs.

7. As soon as additional information is acquired, prepare a follow-up report to update the stakeholders on the event. Several follow-up reports can be issued related to the same IUU Fishing event.

INITIAL REPORT	
Priority	[How is priority determined and categorized?]
Ship's Name	
Call Sign	
MMSI	
IMO No.	
Details of the Owner/Operator	
SHIP'S POSITION	
Latitude	
Longitude	
Course	

Speed	
Status	
NATURE OF EVENTS	
IUU Fishing	
Suspicious Movement	
Any Other relevant Information	
Information received by	
Action taken	

Was incident reported to coastal Authority and to whom?	
LAST OBSERVED MOVEMENTS OF THE SUSPECTED VESSEL	
Date	
Time	
Position	
Course	
Speed	
ASSISTANCE REQUIRED	
Preference communication with reporting ship	
Appropriate Coast Radio Station	
VHF / MF/HF / Channel / frequency	
Date / time of report.	

*All times Local

IUU FISHING FLOWCHART

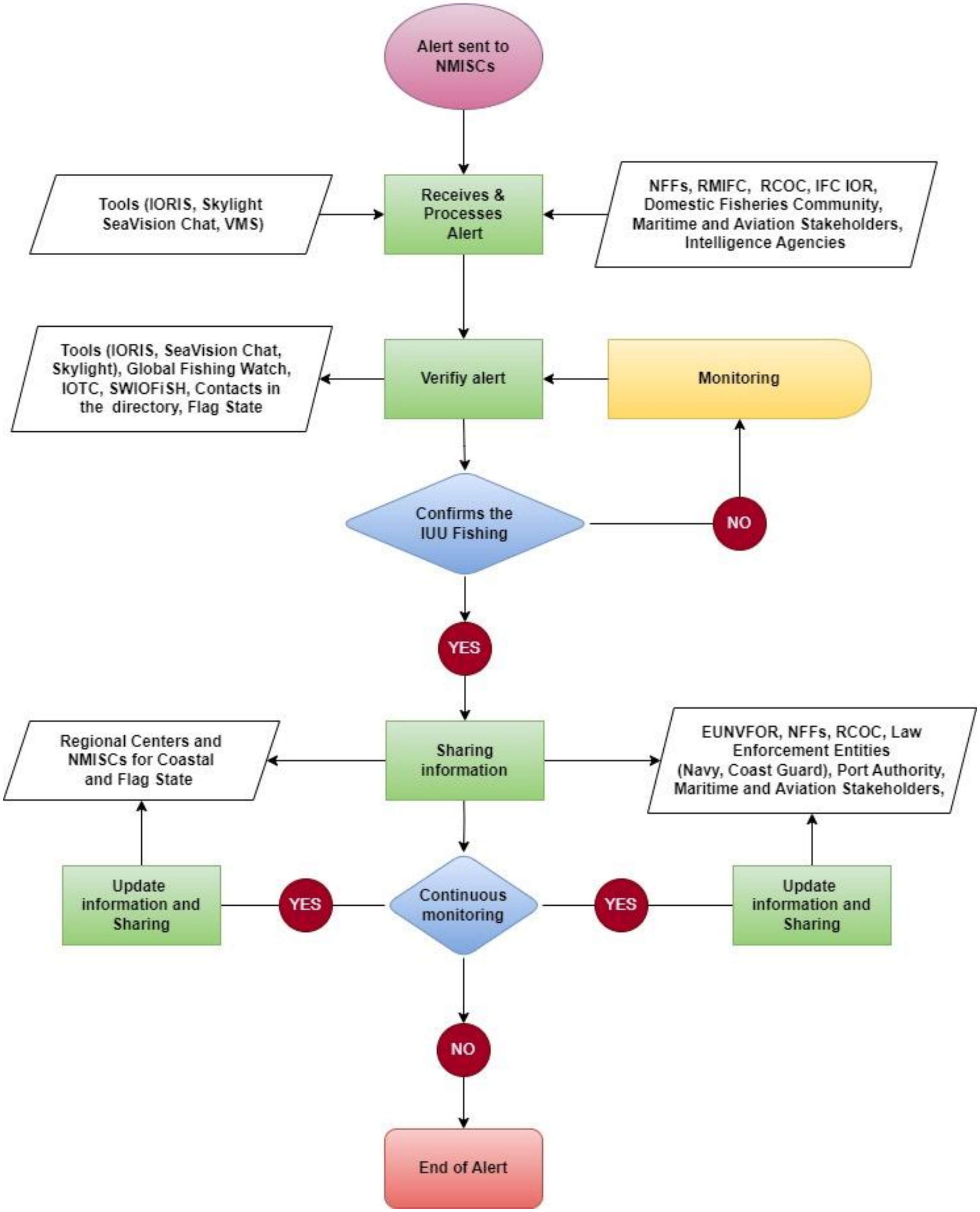

Alert sent to NMISCs
Tools (IORIS, Skylight SeaVision Chat, VMS)
Receives & Processes Alert
NFFs, RMIFC, RCOC, IFC IOR, Domestic Fisheries Community, Maritime and Aviation Stakeholders, Intelligence Agencies
Tools (IORIS, SeaVision Chat, Skylight), Global Fishing Watch, IOTC, SWIOFiSH, Contacts in the directory, Flag State
Verifiy alert
Monitoring
Confirms the IUU Fishing
NO
YES
Regional Centers and NMISCs for Coastal and Flag State
Sharing information
EUNVFOR, NFFs, RCOC, Law Enforcement Entities (Navy, Coast Guard), Port Authority, Maritime and Aviation Stakeholders,
Update information and Sharing
YES
Continuous monitoring
YES
Update information and Sharing
NO
End of Alert

Figure 4. IUU flowchart

NMISC – DRUG SMUGGLING SOP

The following SOP shall be implemented by NMISC in case a Drug Smuggling ALERT is received:

1. Drug Smuggling alerts could be received via IORIS, Sea Vision Chat, Maritime Stakeholders, Local Fisherfolk Community, International Partners (e.g., EUNAVOR, INTERPOL, UK MTO, CMF) Regional Fusion Centres, National Focal Points, Telephone, Fax, Emails.

2. Verify and share the information with other sources (e.g., INTERPOL, National Central Bureau, Drug Enforcement Agencies, UNODC, Customs) contact details as listed in the directory.

3. In case of Drug Smuggling related incident, inform the NFPs, Police, Intelligence, Anti-Narcotics Unit etc. Try to get as much information about the ship and other affiliated crafts. Inform the relevant maritime Regional Fusion Centres for more information. (List of Regional Fusion Centres – should be available in the National Centre.)

4. Keep monitoring the channel / frequency where the alert was received and record communication into the logbook.

5. Assist the leading agency (anti-narcotic unit) by providing ongoing details of the event.

6. Assist leading agency (anti-narcotic unit) in verifying the location of the vessel of interest.

7. As soon as additional information is acquired, prepare a follow-up report to update the lead agency. Several follow up reports can be issued related to the same Drug Smuggling event.

INITIAL REPORT	
Priority	[How is priority determined and categorized?]
Ship's Name (any other vessels involved)	
Call Sign	
MMSI	
IMO No.	
Details of the Owner/Operator	
SHIP'S POSITION	
Latitude	
Longitude	
Course	

Speed	
Status	
NATURE OF EVENTS	
Drug Smuggling	
Irregular Movement	
Any Other relevant Information	
Information received by	
Action taken	

Was incident reported to coastal Authority and to whom?	
LAST OBSERVED MOVEMENTS OF THE SUSPECTED VESSEL	
Date	
Time	
Position	
Course	
Speed	
ASSISTANCE REQUIRED	
Preference communication with source of information	
Appropriate Communication with the lead agency	
VHF / MF/HF / Channel / frequency	
Date / time of report.	

*All times Local

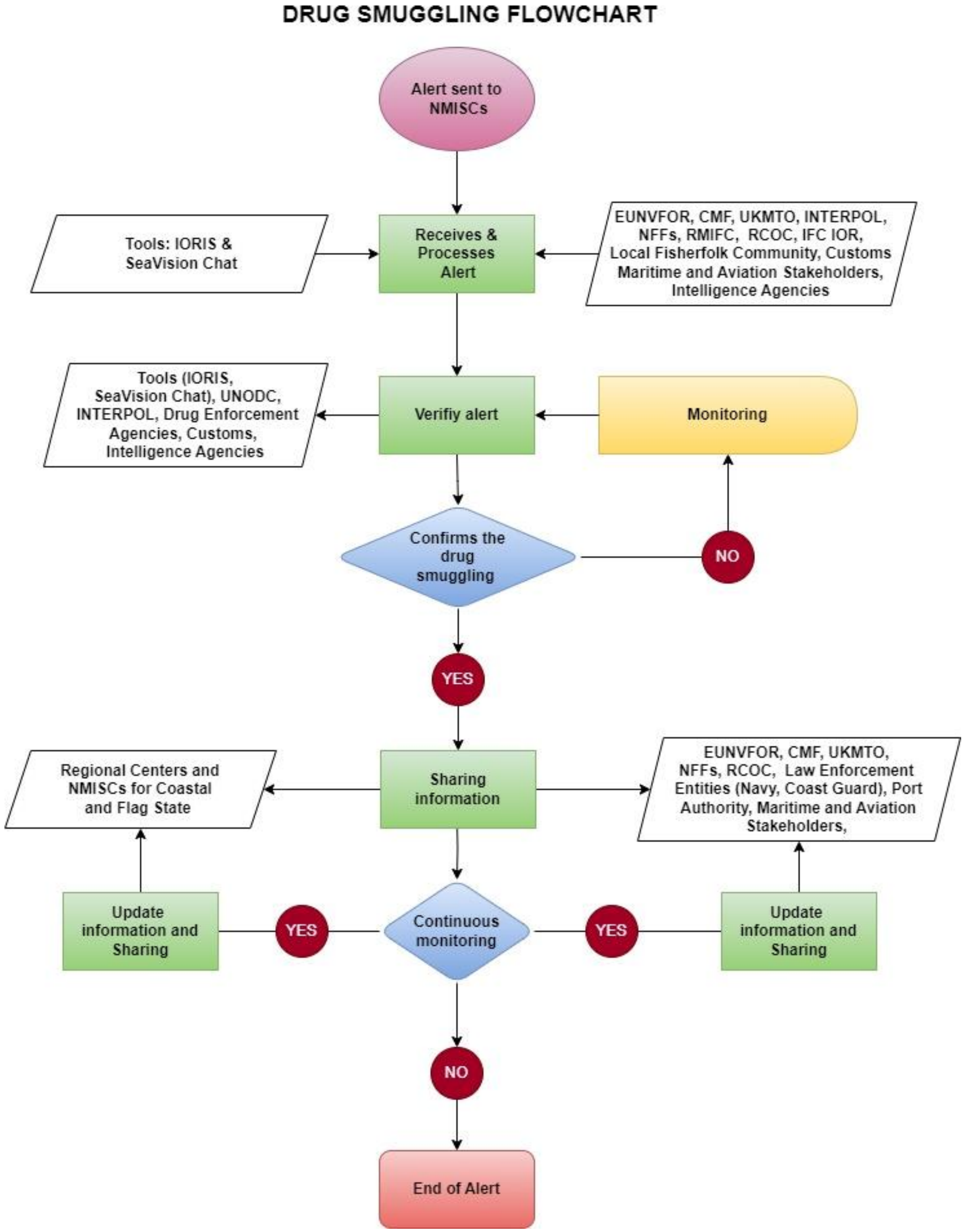

DRUG SMUGGLING FLOWCHART
Alert sent to NMISCs
Tools: IORIS & SeaVision Chat
Receives & Processes Alert
EUNVFOR, CMF, UKMTO, INTERPOL, NFFs, RMIFC, RCOC, IFC IOR, Local Fisherfolk Community, Customs Maritime and Aviation Stakeholders, Intelligence Agencies
Tools (IORIS, SeaVision Chat), UNODC, INTERPOL, Drug Enforcement Agencies, Customs, Intelligence Agencies
Verifiy alert
Monitoring
Confirms the drug smuggling
NO
YES
Regional Centers and NMISCs for Coastal and Flag State
Sharing information
EUNVFOR, CMF, UKMTO, NFFs, RCOC, Law Enforcement Entities (Navy, Coast Guard), Port Authority, Maritime and Aviation Stakeholders,
Update information and Sharing
YES
Continuous monitoring
YES
Update information and Sharing
NO
End of Alert

Figure 5. Drug Smuggling flowchart

NMISC – ENVIRONMENTAL INCIDENT SOP

The following SOP shall be implemented by NMISC in case an Environmental Incident ALERT is received:

1. Environmental Incident alert could be received via Domestic Fisheries and coastal Community, SeaVision Chat, IORIS, Vessel Traffic System, MRCC, Maritime and Aviation Stakeholders, Regional Fusion Centres, National Focal Points, Telephone, Fax, Emails.

2. Verify and share the information with other sources (e.g., Sea Vision & IORIS, MRCC, Environmental Agencies, Regional Fusion Centres, EMSA) and relevant contact details as listed in the directory.

3. In case of Environmental related incident, inform the NFPs, Port Authority, and the environmental leading agency. Try to get as much information about the environmental incident. Inform the respective Regional Centres and NMISC of the flag and coastal states. (List of NMISC's of the region – should be available in the National Centre.)

4. Keep monitoring the channel/frequency/tools where the alert was received and record communication into the log Book.

5. Monitor and update the weather forecast.

6. Assist the leading agency by providing ongoing details of the Environmental Incident.

7. Assist leading agency in verifying the presence and contact details of ships in the vicinity of the Environmental Incident.

8. Keep updating the Fishing community and local agencies about the continuous developments of the Environmental Incident.

9. Prepare a follow up report to update the stakeholders on the Environmental Incident. Several follow-up reports can be issued related to the same incident.

INITIAL REPORT	
Priority	[How is priority determined and categorized?]
Information transmitted by	
Broadcast to	
Source and cause of Environmental Incident	
Date and Time UTC of incident	
Ship's Name	

Ship Type	
Ship Manifest	
Flag	
Call Sign	
MMSI	
IMO No.	
Ship Voyage Data (Last and Next Port)	
Details of the Owner/Operator	
Insurance Details (P&I Club)	
SHIP'S CURRENT POSITION	
Latitude	
Longitude	
Course	
Bearing and Distance	
Speed	
Status (Anchorage, Moored, Drifting or Underway)	
NATURE OF EVENTS	
Nature of Environmental Incident	
Pollutant type and (estimated quantity)	
Any Other Incident (Sinking, Flooding, Fire, Grounding etc.)	
Crew List and injuries	
Any Other relevant Information	
Information received by	
Actions taken to date	
Planned actions	

WEATHER CONDITIONS (on location)	
Local Weather (Wind, Temp., Visibility)	
Sea State (Waves, Currents and Tides)	
Time (Local time and Day Light Circle)	
Charted Bathymetry	

Was the incident reported to the Domestic Coastal Authority and leading Environmental Agency? (confirm date, time, and organization)	
LAST OBSERVED MOVEMENTS OF THE POLLUTANT	
Date	
Time	
Location (lat, long)	
General Area	
Speed	
Wind and Wave (Speed and Direction)	
COMMUNICATION STRUCTURE	
Communication channel between the NMISC and the incident reporter	
Communication channel between the NMISC and vessels and aircrafts in vicinity	
Communication channel between the NMISC and leading agency	
VHF / MF/HF / UHF/ Channel / frequency	
Date / time of report.	

ASSISTANCE REQUIRED	
Search and Rescue	
Medical Evacuation	
Assets and Equipment (tugs, aerial surveillance, booms, dispersants, and skimmers)	

ENVIRONMENTAL INCIDENT FLOWCHART

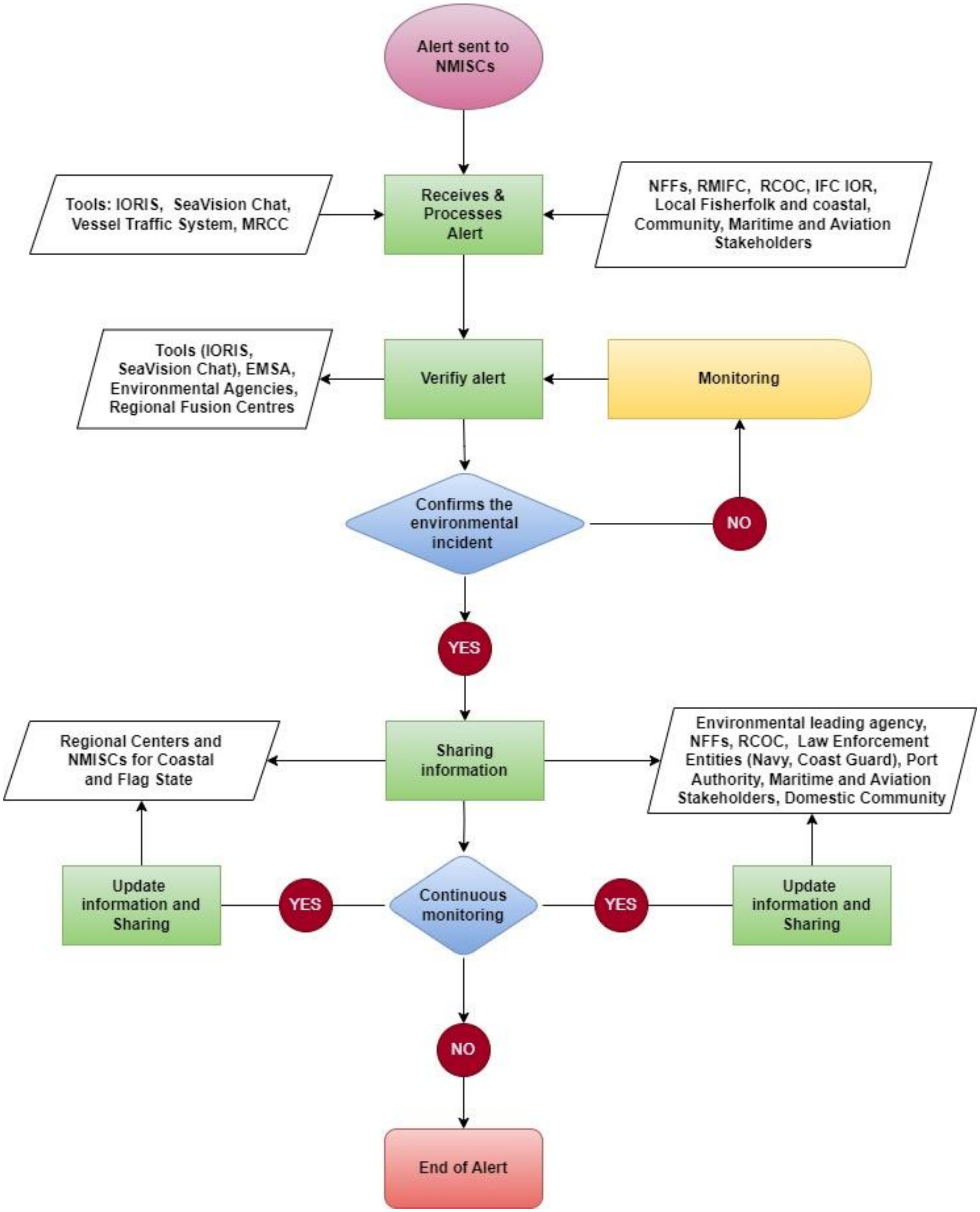

Alert sent to NMISCs
Tools: IORIS, SeaVision Chat, Vessel Traffic System, MRCC
Receives & Processes Alert
NFFs, RMIFC, RCOC, IFC IOR, Local Fisherfolk and coastal, Community, Maritime and Aviation Stakeholders
Tools (IORIS, SeaVision Chat), EMSA, Environmental Agencies, Regional Fusion Centres
Verifiy alert
Monitoring
Confirms the environmental incident
NO
YES
Regional Centers and NMISCs for Coastal and Flag State
Sharing information
Environmental leading agency, NFFs, RCOC, Law Enforcement Entities (Navy, Coast Guard), Port Authority, Maritime and Aviation Stakeholders, Domestic Community
Update information and Sharing
YES
Continuous monitoring
YES
Update information and Sharing
NO
End of Alert

Figure 6. Environmental Incident flowchart

NMISC – MARITIME SAFETY INCIDENT SOP

The following SOP shall be implemented by NMISC in case a Maritime Safety Incident ALERT is received:

1. Maritime Safety Incident alert could be received via Domestic Fisheries and Coastal Community, Sea Vision Chat, IORIS, Vessel Traffic System, **NMISC**, Mercury, Skylight, VMS, INMARSAT -C, GMDSS, DSC, Maritime and Aviation Stakeholders, Vessels in vicinity, Regional Fusion Centres, National Focal Points, Telephone, Fax, Emails.

2. Verify and share the information with other sources (e.g., Sea Vision & IORIS, Skylight, **NMISC**, Regional Fusion Centres, EMSA, Mercury, VTS, Vessels in Vicinity) and relevant contact details as listed in the directory.

3. In case of Maritime Safety related incident, inform the NFPs, Law Enforcement Entities, Health Authorities, Vessels in Vicinity and the **NMISC**. Try to get as much information about the Incident. Inform the respective Regional Centres, port authorities and NMISC of the flag and coastal states. (List of NMISC's of the region – should be available in the National Centre.)

4. Keep monitoring the channel/frequency/tools where the alert was received and record communication into the log Book.

5. Monitor and update the weather forecast.

6. Assist the **NMISC** by providing ongoing details of the Maritime Safety Incident.

7. Assist **NMISC** in verifying the presence and contact details of ships in the vicinity of the Maritime Safety Incident.

8. Keep updating the **NMISC** and local agencies about the continuous developments of the Maritime Safety Incident.

9. Prepare a follow up report to update the stakeholders on the Maritime Safety Incident. Several follow-up reports can be issued related to the same incident.

INITIAL REPORT	
Priority	[How is priority determined and categorized?]
Source of Maritime Safety Incident	
Date and Time	
Ship's Name	
Ship Type	
Ship Manifest	

Flag	
Call Sign	
MMSI	
IMO No.	
Ship Voyage Data (Last and Next Port)	
Details of the Owner/Operator	
Insurance Details	
SHIP'S POSITION	
Latitude	
Longitude	
Course	
Bearing and Distance	
Speed	
Status (Anchorage, Moored, Drifting or Underway)	
NATURE OF INCIDENT	
Nature of Maritime Safety Incident (Fire, Collision, Flooding, MOB, Grounding)	
Any Other Related Incident	
Crew List and injuries	
Any Other relevant Information	
Information received by	
Action taken	

WEATHER CONDITIONS	
Local Weather (Wind, Temp., Visibility)	
Sea State (Waves, Currents and Tides)	

Time (Local time and Day Light Circle)	
Charted Bathymetry	

Was incident reported to the MRCC?	
LAST OBSERVED LOCATION OF THE MARITIME SAFETY INCIDENT	
Date	
Time	
Position	
General Area	
Speed	
Wind and Wave (Speed and Direction)	
COMMUNICATION STRUCTURE	
Communication channel between the NMISC and the incident reporter	
Communication channel between the NMISC and vessels and aircrafts in vicinity	
Communication channel between the NMISC and leading agency	
VHF / MF/HF / UHF/ Channel / frequency	
Date / time of report.	

ASSISTANCE REQUIRED	
Search and Rescue	
Medical Evacuation	
Assets and Equipment	

MARITIME SAFETY INCIDENT FLOWCHART

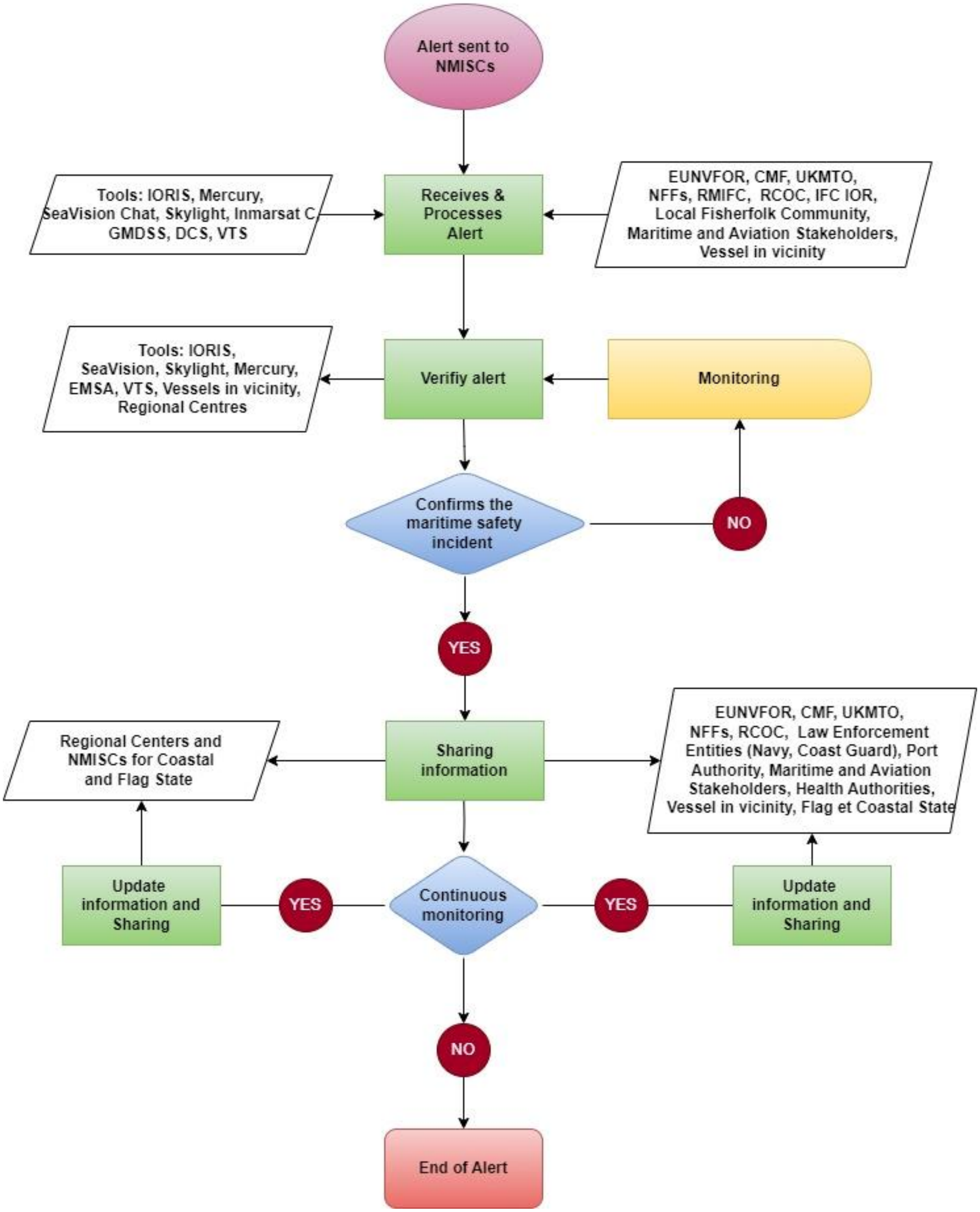

Alert sent to NMISCs
Tools: IORIS, Mercury, SeaVision Chat, Skylight, Inmarsat C, GMDSS, DCS, VTS
Receives & Processes Alert
EUNVFOR, CMF, UKMTO, NFFs, RMIFC, RCOC, IFC IOR, Local Fisherfolk Community, Maritime and Aviation Stakeholders, Vessel in vicinity
Tools: IORIS, SeaVision, Skylight, Mercury, EMSA, VTS, Vessels in vicinity, Regional Centres
Verifiy alert
Monitoring
Confirms the maritime safety incident
NO
YES
Regional Centers and NMISCs for Coastal and Flag State
Sharing information
EUNVFOR, CMF, UKMTO, NFFs, RCOC, Law Enforcement Entities (Navy, Coast Guard), Port Authority, Maritime and Aviation Stakeholders, Health Authorities, Vessel in vicinity, Flag et Coastal State
Update information and Sharing
YES
Continuous monitoring
YES
Update information and Sharing
NO
End of Alert

Figure 7. Maritime Safety Incident flowchart

NMISC – Terrorist activity against a ship SOP (Do we need one for an attack against a port and against offshore structures e.g., oil platforms?)

The following SOP shall be implemented by NMISC in case a terrorist activity alert is received:

1. Terrorist activity alert could be received from an informal network (local fishers, crew member,) and intelligence source (IORIS, SeaVision, Skylight, Inmarsat C, GMDSS, DSC), International organisation (**EUNVFOR, CMF, UKMTO, INTERPOL, EMSA), VTS**, national agencies via Maritime Stakeholders, Regional Fusion Centres **(RMIFC, RCOC, IFC IOR)**, National Focal Points, Telephone, Fax, Emails.

2. Verify and share the information with the NFPs responsible for the counter terrorism, **Tools (Mercury, IORIS, SeaVision Chat, Inmarsat C, GMDSS, DSC), VTC, MRCC, Vessel in vicinities, Contacts in the directory, Ship's flag state**, Flag state of vessels involved.

3. Share the information with regional and international partners: **EUNVFOR, CMF, UKMTO, NFFs, RCOC, EMSA, MRCC, Law Enforcement Entities (Navy, Coast Guard), Port Authority, Maritime and Aviation Stakeholders, Flag state of vessels involved.**

4. Follow up with the source for any additional information.

5. Assist the NFP by providing on-going details of the activity.

As soon as additional information is acquired, prepare a follow up report to update the partners on the activity.

INITIAL REPORT	
Date and time	
Priority	[How is priority determined and categorized?]
Ship's Name	
Call Sign	
MMSI/ IMO No.	
Flag	
Details of the Owner/Operator	
SHIP'S POSITION	
Latitude	
Longitude	

Course	
Speed	
Status	
NATURE OF EVENTS	Maritime Terrorism
ANY OTHER RELEVANT INFORMATION	
INFORMATION RECEIVED BY	
ACTION TAKEN	

LAST OBSERVED MOVEMENTS OF THE SUSPECTED VESSEL	
Date	
Time	
Position	
Course	
Speed	

*All times UTC

TERRORIST ACTIVITY FLOWCHART

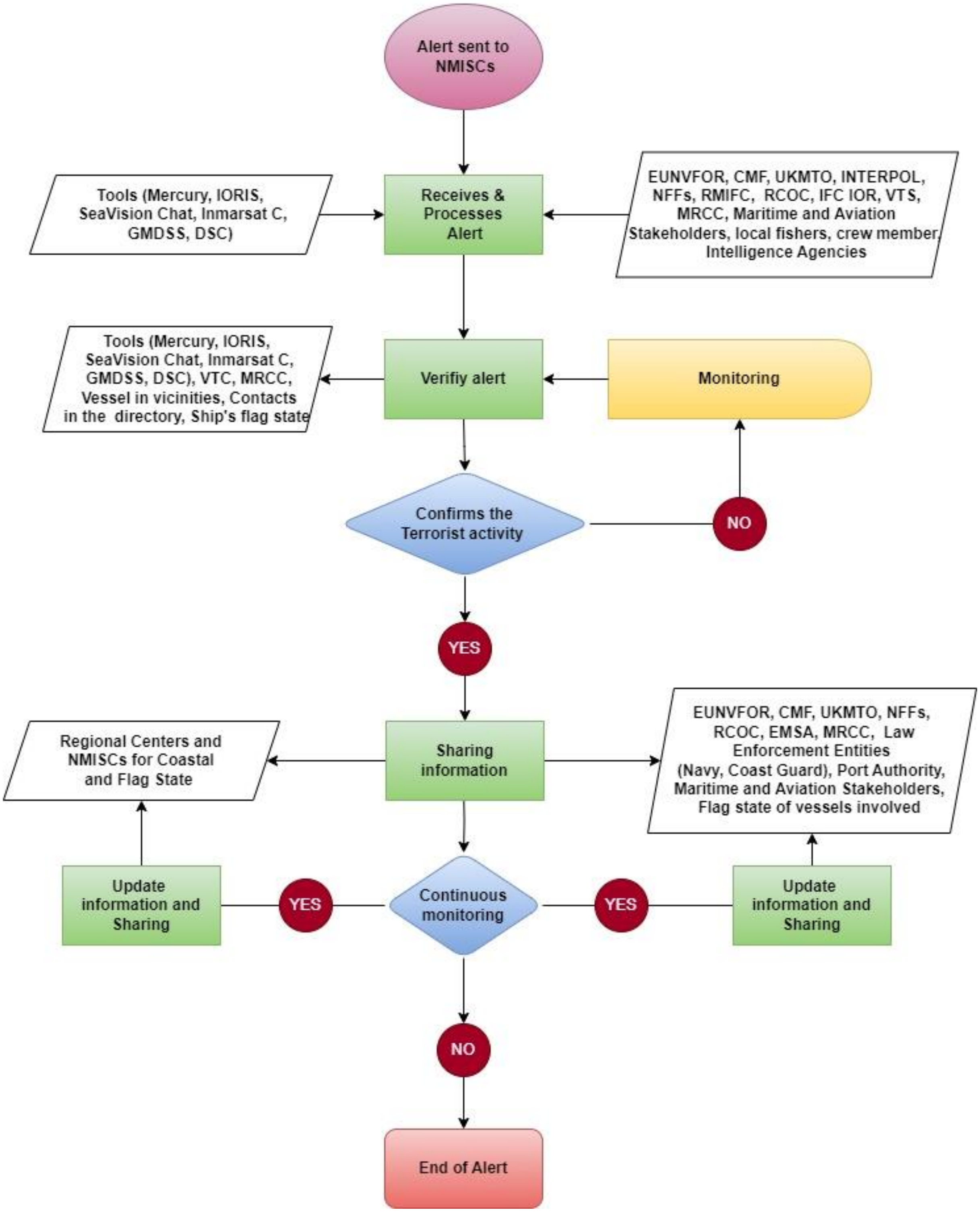

Alert sent to NMISCs
Tools (Mercury, IORIS, SeaVision Chat, Inmarsat C, GMDSS, DSC)
Receives & Processes Alert
EUNVFOR, CMF, UKMTO, INTERPOL, NFFs, RMIFC, RCOC, IFC IOR, VTS, MRCC, Maritime and Aviation Stakeholders, local fishers, crew member, Intelligence Agencies
Tools (Mercury, IORIS, SeaVision Chat, Inmarsat C, GMDSS, DSC), VTC, MRCC, Vessel in vicinities, Contacts in the directory, Ship's flag state
Verifiy alert
Monitoring
Confirms the Terrorist activity
NO
YES
Regional Centers and NMISCs for Coastal and Flag State
Sharing information
EUNVFOR, CMF, UKMTO, NFFs, RCOC, EMSA, MRCC, Law Enforcement Entities (Navy, Coast Guard), Port Authority, Maritime and Aviation Stakeholders, Flag state of vessels involved
Update information and Sharing
YES
Continuous monitoring
YES
Update information and Sharing
NO
End of Alert

Figure 8. Terrorist Activity flowchart

NMISC – irregular migration SOP

The following SOP shall be implemented by NMISC in case an Irregular Migration

activity is received:

1. Irregular Migration activity could be received from an informal network (local fishers, crew member,) and intelligence source (International organisation and national agencies) via **NFFs, MRCC, RMIFC, RCOC, IFC IOR, Immigration department Local Fisherfolk Community, Customs, Intelligence Agencies, Maritime and Aviation Stakeholders, Vessel in vicinity**, Telephone, Fax, Emails.
2. Verify and share the information with the NFPs responsible for the Irregular Migration (E.g.: Foreign Affairs Dept or immigration dept), **IORIS, SeaVision, VTS, Vessels in vicinity, MRCC, Regional Centres, Immigration department, Foreign Affairs Department, Customs.**
3. Share the information with Flag State, regional and international partners: **MRCC, NFFs, RCOC, OIM, Law Enforcement Entities (Navy, Coast Guard), Port Authority, Maritime and Aviation Stakeholders, Health Authorities, Vessel in vicinity, Foreign, Affairs Department Affairs, Embassies accredited to migrants.**
4. Follow up with the source for any additional information including safety of persons on board.
5. Assist the NFP by providing on-going details of the activity.

As soon as additional information is acquired, prepare a follow up report to update the partners on the activity.

INITIAL REPORT	
Date and time	
Priority	[How is priority determined and categorized?]
Ship's Name	
Call Sign	
MMSI/ IMO No.	
Flag	
Details of the Owner/Operator	

SHIP’S POSITION	
Latitude	
Longitude	
Course	
Speed	
Status	
NATURE OF EVENTS	Irregular Migration
ANY OTHER RELEVANT INFORMATION	
INFORMATION RECEIVED BY	
ACTION TAKEN	

LAST OBSERVED MOVEMENTS OF THE SUSPECTED VESSEL	
Date	
Time	
Position	
Course	
Speed	

*All times in UTC

IRREGULAR MIGRATION FLOWCHART

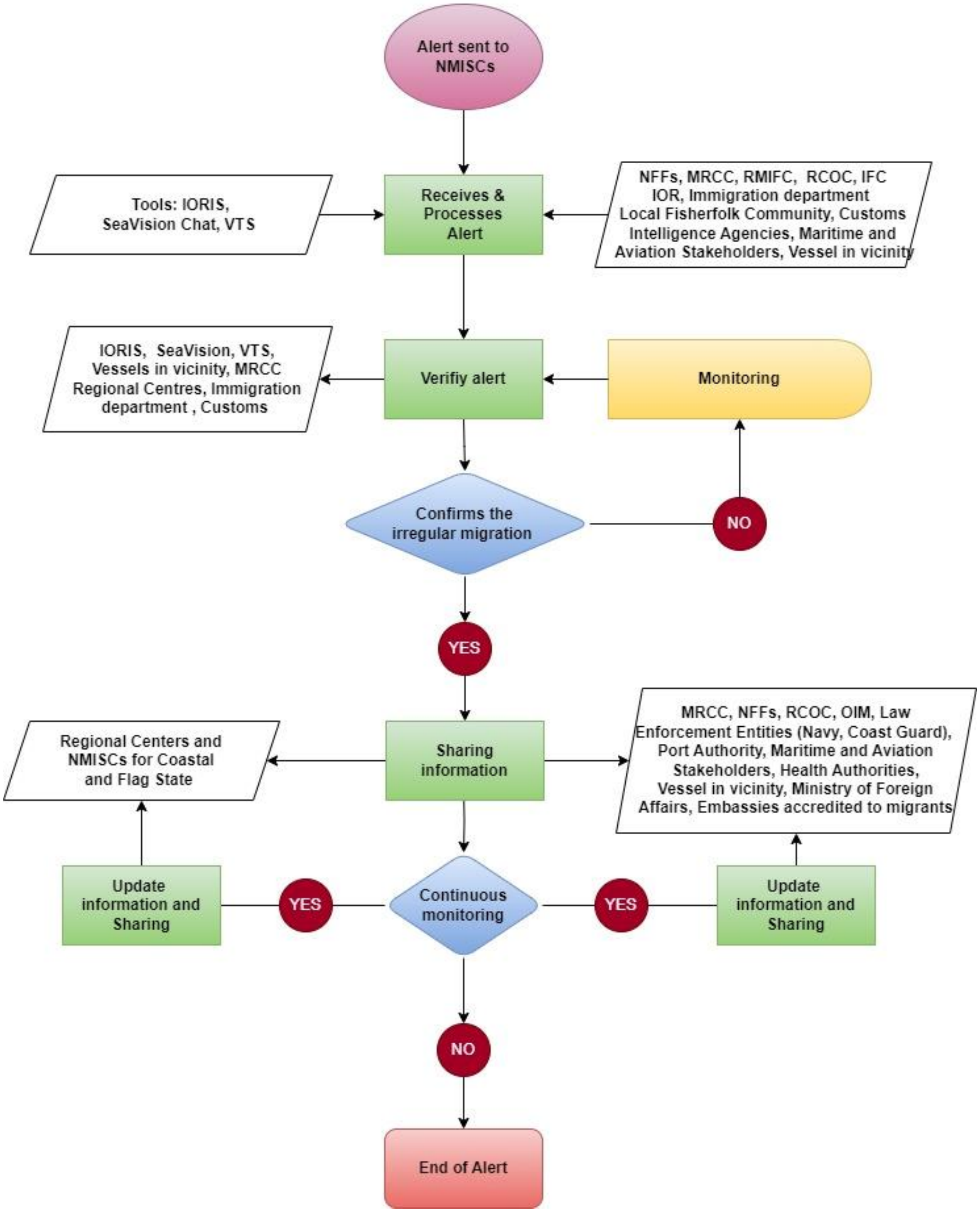

Alert sent to NMISCs
Tools: IORIS, SeaVision Chat, VTS
Receives & Processes Alert
NFFs, MRCC, RMIFC, RCOC, IFC IOR, Immigration department Local Fisherfolk Community, Customs Intelligence Agencies, Maritime and Aviation Stakeholders, Vessel in vicinity
IORIS, SeaVision, VTS, Vessels in vicinity, MRCC Regional Centres, Immigration department , Customs
Verifiy alert
Monitoring
Confirms the irregular migration
NO
YES
Regional Centers and NMISCs for Coastal and Flag State
Sharing information
MRCC, NFFs, RCOC, OIM, Law Enforcement Entities (Navy, Coast Guard), Port Authority, Maritime and Aviation Stakeholders, Health Authorities, Vessel in vicinity, Ministry of Foreign Affairs, Embassies accredited to migrants
Update information and Sharing
YES
Continuous monitoring
YES
Update information and Sharing
NO
End of Alert

Figure 9. Irregular Migration flowchart

NMISC - TRAFFICKING AND CONTRABAND SMUGGLING SOP

The following SOP shall be implemented by the NMISC in case a Contraband Smuggling ALERT is received:

1. Contraband Smuggling alert could be received via IORIS, SeaVision chat, Mercury Chat, VMS, VTS, SKYLIGHT, INMARSAT C, GMDSS, National Focal Points, INTERPOL, Customs, Intelligence agencies, Regional Fusion Centres, Maritime and Aviation Stakeholders, UNODC through Telephone, Fax, Emails.

2. Verify and share the information with other sources (e.g., RMIFC/ RCOC/ IFC IOR/ EMSA/ VTS/ INTERPOL/ MRCC) and contact details as listed in the directory.

3. In case of a Trafficking and Contraband Smuggling related incident, inform the NFPs, RCOC, Law Enforcement Entities (Navy, Coast Guard), Port Authority, Maritime and Aviation Stakeholders. Try to get as much information about the ship and event. Inform the respective Lead agencies and supporting agencies.

4. Keep monitoring the channel / frequency where the alert was received and record communication into the logbook.

5. Assist the NFP / lead agency by providing on-going details of the event.

6. Issue updates to other interested parties.

7. Assist NFPs/ lead law enforcement agency in verifying the presence and contact details of ships in the area of the event for possible direct contact with those ships by the lead agency.

8. As soon as additional information is acquired, prepare a follow-up report to update the stakeholders on the event. Several follow up reports can be issued related to the same trafficking / contraband smuggling event.

TRAFFICKING AND CONTRABAND SMUGGLING

(REF NO)

□ Goods □ Arms □ Drugs □ Wildlife □ Human

Subject: Watchstander/ Operator: Date/Time:

AWARENESS/INFORMATION GATHERING

REPORTING SOURCE INFORMATION

Name: Phone: *(If Vessel on Ground is Source)* Vessel Name /GPSIMO/MMSI/SSEN#: Position

Incident Description:

Items On-board:

Suspected Smuggler: Nationality:

Armed: (Specify) Yes / No

Vessel Name/Type:

IMO/MMSI:

Estimated Number of Crew:

Notes:

(For urgent verification and monitoring of all actions taken. Brief appropriate supervisors for any updates.)

LPOC: NPOC:

Status of Suspected Smuggler:

Date/Time Observed:

Flag of Registry: Nationality:

Geographic Location: GPS Coordinates:

Speed/Course:

Weather/Sea Condition: Wind Speed/Direction: Wave Height:

Storage Location:

Agencies to be Notified:

UPDATES:

(Describe any updates.)

INITIAL ACTIONS: WATCHSTANDER/ OPERATOR	
Notification: 1. Assistant Duty Officer 2. Analysts 3. Duty Officer 4. Director of Operations 5. Director	Remarks: 1. Lateral Coordination to concerned agencies. 2. Draft Maritime Information Report 3. Others (Specify):
Supporting Agencies to be Notified:	

Status: Maritime Information Report	Remarks:
Agency Notifications Received by/Date/Time	Remarks:
o (Main Agency concerned):	
o (Other Agency concerned 1):	
o (Other Agency concerned 2):	
o Others (Specify):	
OTHER INITIAL ACTIONS	
1. Complete information 2. Verify the received information from all possible sources: 1) Open-source intelligence 2) Counterparts from concerned local agencies. 3) Counterparts from concerned foreign entities. 3. Assess verified information: 1) Consult with Analysts. 2) Identify applicable international and domestic laws.	Remarks:

3) Identify the lead and supporting agencies. 4. Recommend appropriate action: 1) Continuous monitoring. 2) For archiving. 3) Maritime Intelligence, Surveillance, and Reconnaissance. 4) Interagency maritime security operation.	
FOLLOW UP ACTIONS	
Agency Action Taken	Incident Status
Remarks:	Remarks:
Make a Chronological of Events:	
Progress Report: 1 2 3 4 5	Remarks:
Request For Information	Additional Information
Remarks:	Remarks: *(Provided updates to concerned agencies)*

Final Report:	Remarks:
Status Update/Brief: 1. Assistant Duty Officer 2. Analysts 3. Duty Officer 4. Director of Operations 5. Director	Remarks:

CONCLUSION	
Include in Daily Report	
Daily Brief	
Incident Logbook	
Accomplishment Report	
NMISC Final Incident Report	

POLICY INFORMATION

1. DRUG TRAFFICKING LAWS
    1. INTERNATIONAL
        1. Single Convention on Narcotic Drugs of 1961 (as amended in 1972)
        2. Convention on Psychotropic Substances of 1971
        3. United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988
        4. Etc.
    2. DOMESTIC LAWS

1. *(enumerate)*

1. HUMAN TRAFFICKING
    1. INTERNATIONAL LAWS
        1. 2000 Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children Act (Palermo Protocol)
        2. United Nations Convention against Transnational Organized Crime (Trafficking Protocol)
        3. Etc.
    2. DOMESTIC LAWS
        1. *(enumerate)*

2. GOODS SMUGGLING

    1. INTERNATIONAL LAWS

        1. (enumerate)

    2. DOMESTIC LAWS

        1. (enumerate)

TRAFFICKING AND CONTRABAND SMUGGLINGFLOWCHART

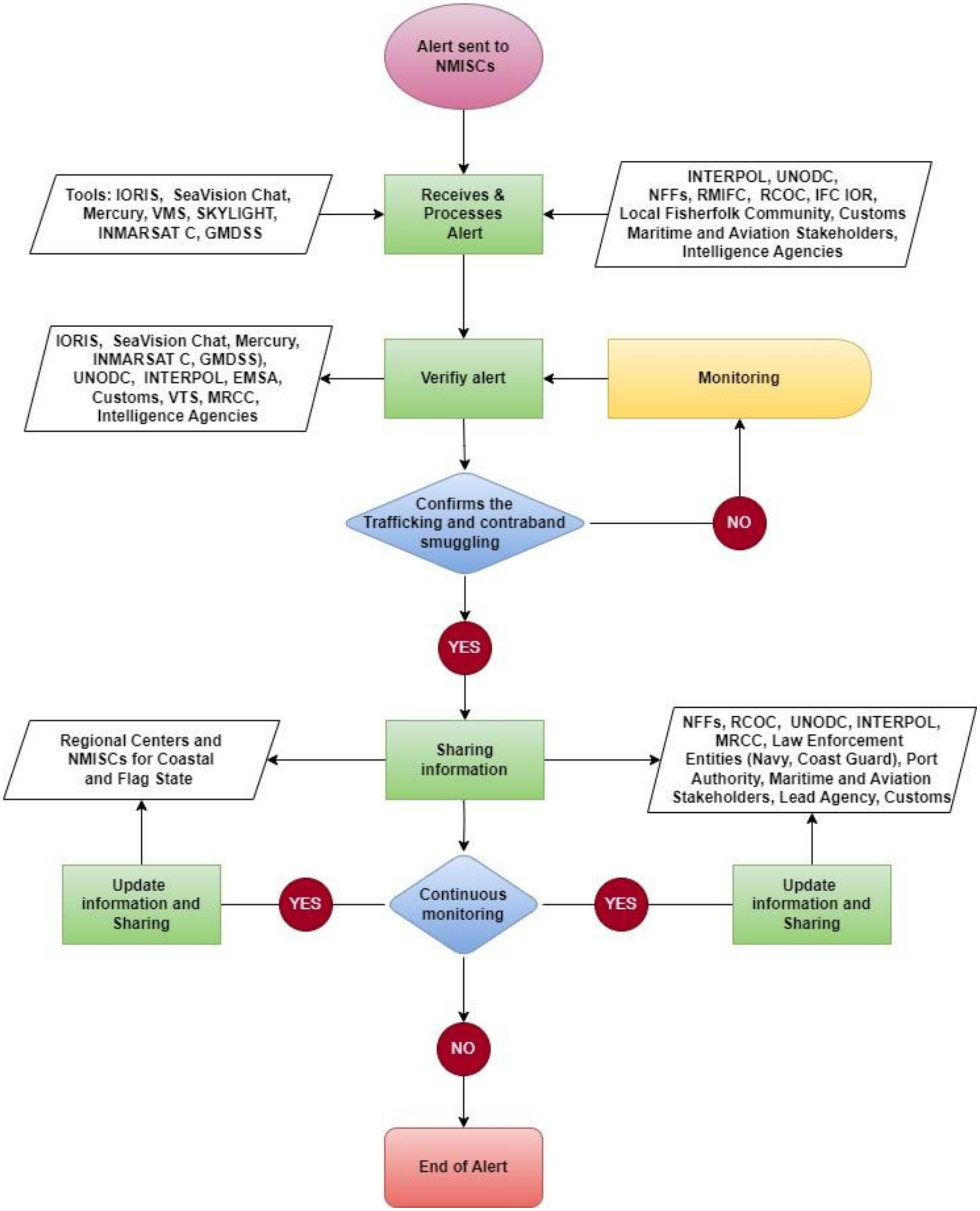

Alert sent to NMISCs
Tools: IORIS, SeaVision Chat, Mercury, VMS, SKYLIGHT, INMARSAT C, GMDSS
Receives & Processes Alert
INTERPOL, UNODC, NFFs, RMIFC, RCOC, IFC IOR, Local Fisherfolk Community, Customs Maritime and Aviation Stakeholders, Intelligence Agencies
IORIS, SeaVision Chat, Mercury, INMARSAT C, GMDSS), UNODC, INTERPOL, EMSA, Customs, VTS, MRCC, Intelligence Agencies
Verifiy alert
Monitoring
Confirms the Trafficking and contraband smuggling
NO
YES
Regional Centers and NMISCs for Coastal and Flag State
Sharing information
NFFs, RCOC, UNODC, INTERPOL, MRCC, Law Enforcement Entities (Navy, Coast Guard), Port Authority, Maritime and Aviation Stakeholders, Lead Agency, Customs
Update information and Sharing
YES
Continuous monitoring
YES
Update information and Sharing
NO
End of Alert

Figure 10. Trafficking and Contraband Smuggling flowchart

NMISC - MARITIME SECURITY THREATS (HYBRID) SOP

The following SOP shall be implemented by the NMISC in case a Maritime Security Threats (Hybrid) ALERT is received:

1. Maritime Security Threats (Hybrid) alert could be received via Mercury Chat, Customs, INTERPOL, UNODC, Anti-Drug Agencies, Intelligence Services, Air and Border Police, Sea Vision, Ioris, Skylight, VTS, NATIONAL Focal Points, Telephone, Fax, Emails.

2. Verify and share the information with other sources (e.g., INTERPOL, UNODC, European Maritime Safety Agency (EMSA), UKMTO – MSCHOA – EUNAVFOR – NATO Shipping Centre, CMF) and other relevant contact details as listed in the directory.

3. In case of Maritime Security Threats (Hybrid) related incident, inform the NFPs / lead agencies. Try to get as much information about the ship and event. Inform the respective Navy, Coast-Guard, MRCC, Customs, Port authorities and other Law Enforcement Agencies.

4. Keep monitoring the channel / frequency where the alert was received and record communication into the log Book.

5. Assist the Lead agencies, Navy, Coast Guard, Customs, Port authority, Air and Border Police, by providing on-going details of the event.

6. Assist NFPs / lead agencies in verifying the presence and contact details of ships in the area of the event for possible direct contact with those ships by the lead agencies.

7. As soon as additional information is acquired, prepare a follow-up report to update the stakeholders on the event. Several follow-up reports can be issued related to the same Maritime Security Hybrid Event.

INITIAL REPORT	
Priority	[How is priority determined and categorized?]
Source of Maritime Security Threats (Hybrid) Incident	
Date and Time	
Ship's Name	
Ship's Type	
Ship Manifest	
Flag	
Call Sign	

MMSI	
IMO Number.	
Ship Voyage Data	
Details of Owner/Operator	
Insurance Details	
SHIP'S POSITION	
Latitude	
Longitude	
Course	
Bearing and Distance	
Speed	
Status	
NATURE OF EVENTS	
Any Other relevant Information	
Information received by	
Action taken	

POSITION OF INCIDENT	
Latitude	
Longitude	
Course	
Bearing and Distance	
Speed	
Status	
Name of the area	

DETAILS OF INCIDENT	
Sailing	
At the anchor	
At berth	
Method of attack	
Description of suspected craft	
Any other relevant information (language spoken)	
Injures to crew and passengers	
Damage to ship (Which part of the ship was attacked)	
Brief details of stolen property / cargo	
Action Taken by the master/ crew	
Was incident reported to coastal Authority and to whom?	
COMMUNICATION STRUCTURE	
Communication channel between the NMISC and the incident reporter	
Communication channel between the NMISC and vessels and aircrafts in vicinity	
Communication channel between the NMISC and leading agency	
Appropriate Coast Radio Station	
VHF / MF/HF / Channel / frequency	
INMARSAT Ld. (plus Ocean Region Code)	
Date / time of report.	
ASSISTANCE REQUIRED	
Search and Rescue	
Medical Evacuation	

Assets and Equipment	

MARITIME SECURITY THREATS (HYBRID) FLOWCHART

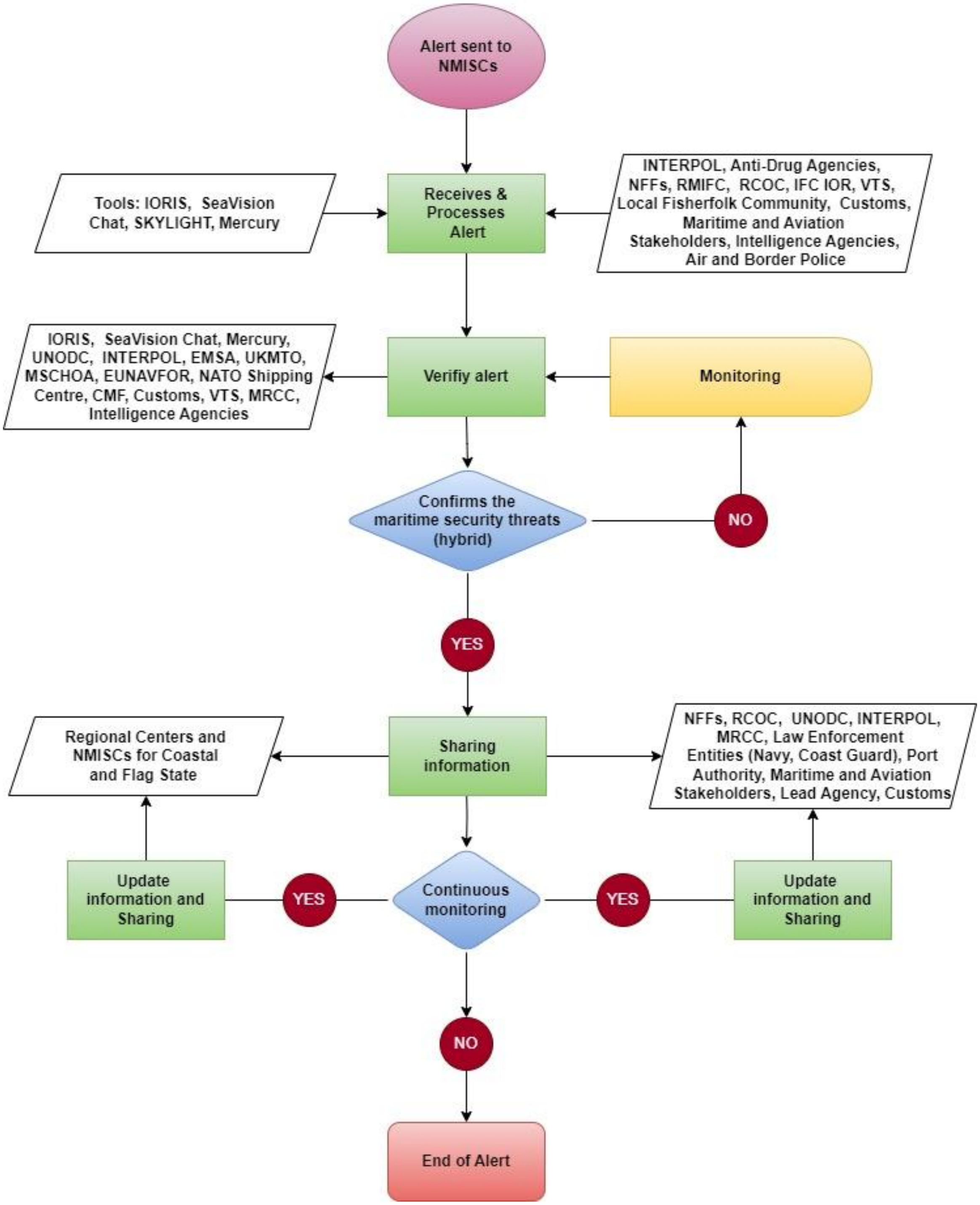

Alert sent to NMISCs
Tools: IORIS, SeaVision Chat, SKYLIGHT, Mercury
Receives & Processes Alert
INTERPOL, Anti-Drug Agencies, NFFs, RMIFC, RCOC, IFC IOR, VTS, Local Fisherfolk Community, Customs, Maritime and Aviation Stakeholders, Intelligence Agencies, Air and Border Police
IORIS, SeaVision Chat, Mercury, UNODC, INTERPOL, EMSA, UKMTO, MSCHOA, EUNAVFOR, NATO Shipping Centre, CMF, Customs, VTS, MRCC, Intelligence Agencies
Verifiy alert
Monitoring
Confirms the maritime security threats (hybrid)
NO
YES
Regional Centers and NMISCs for Coastal and Flag State
Sharing information
NFFs, RCOC, UNODC, INTERPOL, MRCC, Law Enforcement Entities (Navy, Coast Guard), Port Authority, Maritime and Aviation Stakeholders, Lead Agency, Customs
Update information and Sharing
YES
Continuous monitoring
YES
Update information and Sharing
NO
End of Alert

Figure 11. Maritime Security Threats (Hybrid) flowchart

NMISC SEARCH AND RESCUE SOP

1. PURPOSE

The purpose of this procedure is to ensure that appropriate steps and actions are taken during coordination of marine SAR operations.

2. DESCRIPTION OF ACTIVITIES

1. The **NMISC** receives alert and message for SAR assistance from a vessel under distress.

2. The **NMISC** analyses the message.

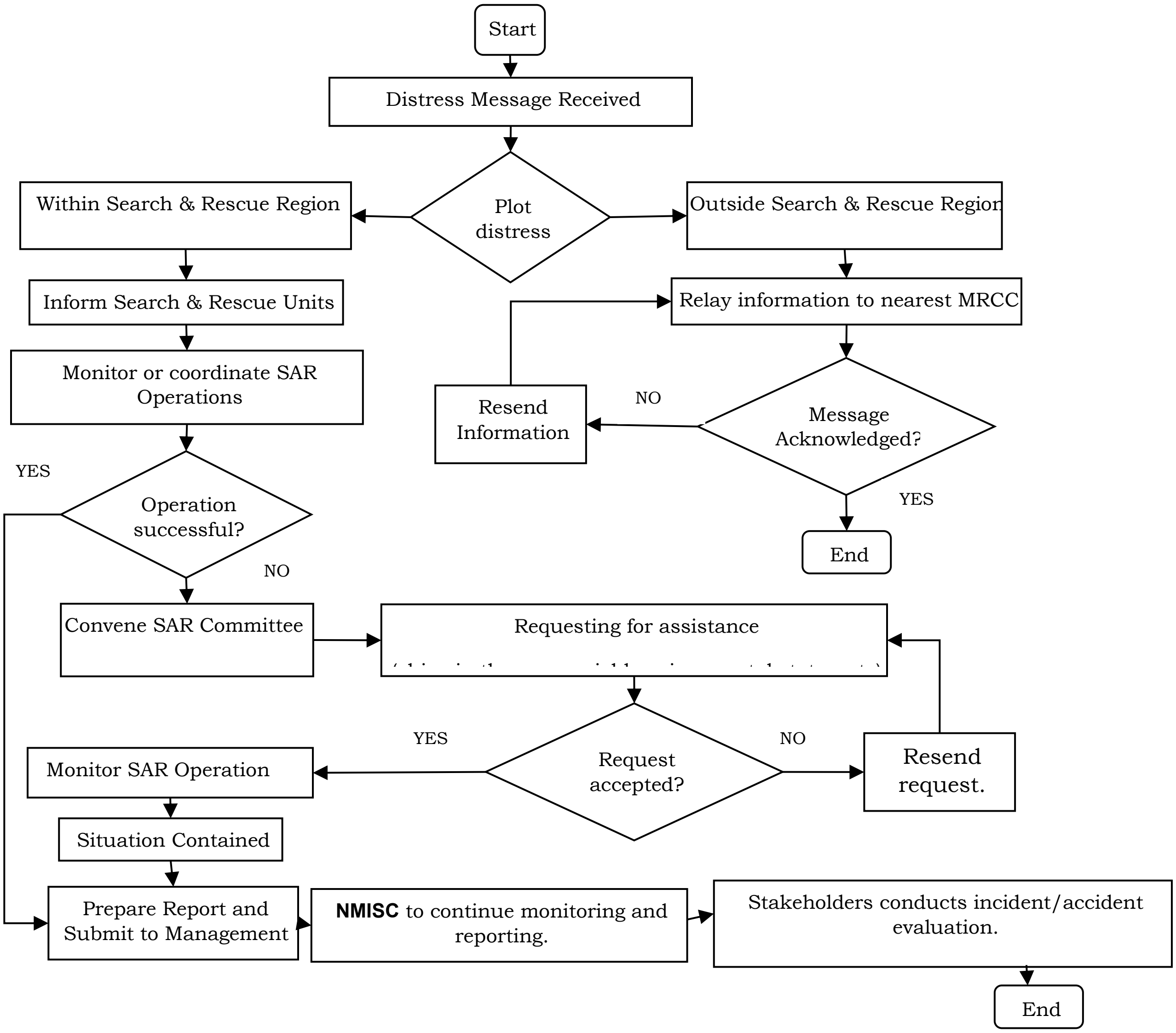
    1. If the distress message received is outside the SAR region, the MRCC will relay it to the nearest **NMISC** until it is acknowledged that it has been received.

    2. If the distress message received is within the SAR region, the **NMISC** will inform the maritime SAR response units.

1. The **NMISC** will continue to monitor the SAR operation and upon completion, the **NMISC** will prepare a report and submit it to the Management.

2. SAR stakeholders to conduct an evaluation and implement lessons learnt.

SAR FLOWCHART


Start
Distress Message Received
Plot distress
Within Search & Rescue Region
Outside Search & Rescue Region
Inform Search & Rescue Units
Relay information to nearest MRCC
Monitor or coordinate SAR Operations
Resend Information
NO
Message Acknowledged?
YES
Operation successful?
YES
NO
End
Convene SAR Committee
Requesting for assistance
YES
Request accepted?
NO
Resend request.
Monitor SAR Operation
Situation Contained
Prepare Report and Submit to Management
NMISC to continue monitoring and reporting.
Stakeholders conducts incident/accident evaluation.
End

10. **DAILY PROCEDURAL SOPS AND BATTLE RHYTHM**

NMISC WATCH LOG SOP

NMISC WATCH LOG SOP	SOP# 001
Watch Log	PAGE 1 OF 1
The watch log shall be a complete daily record, by watches, which shall describe every occurrence of importance concerning the watch and the command and control of the NMISC or items of historical value.	
The following items should be logged in the watch log, including time of occurrence. This is by no means a complete listing of all items to be logged.	
	-Assuming the watch; list all watchstanders for the shift. -Release of any messages or official notifications. -The entry and exit of any distinguished/ official visitor in the NMISC. -Any execution of a drill. -Any event that activates a Management Critical Information Requirement or DCoC Regional response Information Requirement -Any degradation in systems or ability to conduct operations. -Significant events pertaining to forces (HQ and AOR), operations, or readiness. -Emergencies in the Maritime Operations Center complex. -All conferences. - NMISC shall obtain weather reports and share with relevant stakeholders -Changes in status of watch or defense conditions. -Event requiring notification of the Management -Any entry or exit of VOIs into the AOR. -Events that require the activation of the Crisis Action Team. -Changes and turnovers of watch personnel during the watch. -Relief of the watch. (Final entry)

SAMPLE WATCH LOG SHEET

S/NO.	DATE & TIME	STN FROM	STN TO	MODE OF COM	DETAILS	SIGN

MANAGER SIGNATURE ……………… DATE: …………………

WATCH HANDOVER PROCEDURES AND CHECK LIST

1. EQUIPMENT OPERATIONAL STATUS

EQUIPMENT	STATUS WORKING? (Y/N)	COMMENTS
ISDN TELEPHONE LINES		
LANDLINE TELEPHONE		
MOBILE TELEPHONE (Airtime + Connectivity)		
PRINTER (		
AIRCONDITIONING		
INTERNET		
OUTLOOK WEBSITE		
REMISC		
MERCURY		
AIS		
LRIT		
FLEET 77		
VHF		
MF/ HF		
INMARSAT C		

2. SHIFT SUMMARY:

TIME	INCIDENT(S)/OPERATION(S)/ EVENT(S)	REPORT (details of the incident /operation(s)/ event(s))	ACTION TAKEN (In brief) (Full details already entered in the Centre Log)
			.

3. ONGOING ASSIGNMENT/ WORK IN PROGRESS:

ASSIGNMENT DETAILS		TASKED BY	PENDING TASKS/ FOLLOW-UP CASES.
HANDING OVER		TAKING OVER	
SIGN		SIGN	

COMMUNICATION CHECK SOP

NMISC/COMMS CHECK SOP	SOP# 003
Communications checks to all DCoC ISC network to be done every morning	PAGE 1 OF 2
The SOP provides additional guidance and actions for conducting a communication check in the following systems and equipment	
Email	
Telephone VOIP	
MF/HF	
Platform such as IORIS	

DCOC
DJIBOUTI CODE OF CONDUCT

REQUEST FOR INFORMATION

RFI No.	Registration Number	Vessel Name	Flag State	Port of Registration	Type of Vessel	Course, Speed	IMO Number	MMSI

From:	To:
Date:	Deadline:
Subject:	
Background Information:	
Detailed Request: Additional Request:	
Format: Email requested	
Confidentiality: Official / Unclassified **NOTE: Please indicate if the RFI is above Official / Unclassified. If so, the RFI response requires alternative channels of communication.*	
Transmission:	

Point of Contact Name ______________________________

Telephone Number ______________________________

Email Address ______________________________

CONTACT HANDOVER SOP

NMISC SOP	SOP# 002
Contact Handover	
The SOP provides additional guidance and actions for conducting a contact handover to another / NMISC/MOC.	
In the event that a contact of interest is exiting AOR/entering neighbor AOR the below report will assist in transferring tracking responsibilities until contact is deemed not to be a contact of interest.	
From	To:
Line 1:	Contact type/ Name
Line 2:	Track Number (per established procedure / logs)
Line 3:	IMO No. /MMSI/ ID
Line 4:	Sensor Type (Radar / AIS / Visual)
Line 5:	Contact Posit (Lat / Long)
Line 6:	Contact Course / Speed
Line 7:	DTG of Position
Line 8:	Narrative / Intentions / Amplifying Information

DCOC
DJIBOUTI CODE OF CONDUCT

Maritime Incident Reporting and Analysis (MIRA)

Name of MARSEC Agency	
MIRA Reference Number	
Incident Reported by	
Date and Time of Report	

Incident Details

1. **Incident Type: -**

a) Piracy And Armed Robbery
b) Contraband Smuggling
c) IUU Fishing
d) Irregular Human Migration
e) Maritime Incident
f) Maritime Security
g) Cyber Security
h) Maritime Environmental Pollution
j) Others, Please Specify ________________________________

2. **Date and Time of Incident: -**

a) Date ____
b) Time (GMT & Local) __________________________________

3. **Location of Incident: -**

a) Latitude _______________________________
b) Longitude __________________________________
c) Nearest Port or Landmark ____________________________

4. **Vessel Information (If Applicable): -**

a) Vessel Name ______________________________
b) Flag State ______________________________
c) Type of Vessel _________________________________
d) Vessel Identification Number/IMO Number ____________________
e) Any other identifying information ________________________

5. **Description of Incident: -**
Provide a detailed account of the incident, including circumstances, events, and any damage or injuries sustained.

6. **Reporting Entity: -**
MARSEC Centre, Intelligence Agency, Maritime Patrol Aircraft or Others (Specify name)

7. **Reporting Person Details: -**

a) Name
b) Designation
c) Contact Info (Phone no., email)

Supporting Information

8. **Source of Information: -**

a) Visual Observation
b) Radar
c) Aerial Surveillance
d) Satellite Imagery
e) Other (Specify Source) ___________________

9. **Additional Witnesses: -** □ Yes □ No
If yes, provide witness details (Names, contact info or identifying details)

10. **Corroborating Documents: -**

□ Photos □ Videos □ Radar Images □ Satellite Images

□ Other (Specify) ______________________________________

Assessment

11. **Credibility of Incident: -**

□ High □ Medium □ Low

Justification of Assessment

12. **Potential Threat Level: -**

□ High □ Medium □ Low

Justification of Assessment

13. **Previous Incidents in the Area: -**

□ Yes □ No

If yes, provide nature and details of previous incidents

Incident (Type, Date, Time)	Incident Details

14. **Legal Provisions related to the Incident: -**

Level	Legal Provisions
National	
Regional	
International	

Level	Legal Provisions
Others	

15. **Agencies relevant to the Incident: -**

Agency & Type	Rationale

16. **Possible actions for further management of the Incident: -**

Please fill possible actions first and decide priority thereafter

Possible Actions	**Priority**

Actions Taken

17. **Communication with Vessel (if applicable): -**

□ Attempted □ Not Attempted

If Attempted

□ Successful □ Unsuccessful

18. **Contact with Flag State (if applicable):**

□ Attempted □ Not Attempted

If, not attempted (Reason) ___________________________________

If, attempted

□ Successful □ Unsuccessful

19. **Coordination with Other Agencies: -**

a) Information passed and details

Agency	Information Passed

b) Request for Information made and details

RFI No & Agency	Information Sought

20. **Surveillance and Response Activities: -**

a) Surveillance Ongoing

b) Boarding/Inspection Conducted

c) Pursuit or Apprehension

d) Search and Rescue Operations

e) Arrests Made (if applicable)

21. **Additional Information Gathered: -**

□ Yes □ No

If yes, provide details:

Date **Signature**

This comprehensive Maritime Incident Reporting and Analysis (MIRA) form provides a structured approach for maritime security agencies to document and assess MARSEC incidents and aids in the collection of critical information and supports effective response and analysis to ensure the safety and security of maritime traffic and mariners.

APPENDICES

11. CONTACT DETAILS OF DCoC NMISCs

NO	SIGNATORY STATES	CONTACTS
1.	Comoros	Maritime Operations Centre – Moroni Located at the CG HQ POC: Capt. Fahmy EL Nassib – Director of the MOC Email; comorosmoc@gmail.com Tel No; +2693217913
2.	Djibouti	
3.	Egypt	
4.	Eritrea	
5.	Ethiopia	Ethiopian Maritime Affairs Authority, Contact: Capt. Getinet Abay Gebru CEO, Maritime Administration wing Email: maraddirector@etmaritime.com getinet.esl@gmail.com Tel: +251 11503640 (land line - office hrs.) +251 911231115 (Mobile 24/7)
6.	France	
7.	Jordan	Jordan Maritime Commission Tel No +96232015858 Email: jma@jma.gov.jo
8.	Kenya	Joint Operation Centre Port of Mombasa Email; joc@kpa.co.ke Tel; +254743430430
9.	**Madagascar**	National Maritime Information Fusion Centre (NMIFC)

		P.O. Box 3965, Ankaditoho, Antananarivo (101), Madagascar. Emails: To: directeur.general@cfimmadagascar.org Cc: watchfloor@cfimmadagascar.org Phones: Front desk: + 261 020 22 24 393; +261 34 57 687 50.
10.	**Maldives**	
11.	**Mauritius**	Mauritius Maritime Information Sharing Centre The Commandant National Coast Guard NCG OPS Room Telephone: +230 2083935 / 2088317 / 2187472 Email: ncgops.mpf@govmu.org ccncg.mpf@govmu.org
12.	**Mozambique**	
13.	**Oman**	Maritime Security Center Located At Muscat – Mam Camp Email: Omsc@Mod.Gov.Om 24303111 24303999 24303030
14.	**Saudi Arabia**	Jeddah Maritime Information Sharing Centre (JMISC) Cdr. Hassan Alasmari +966547632701

		Email: jmisc@fg.gov.sa +966126500323
15.	**Somalia**	Ministry of Ports and Marine Transport National Maritime Information Center (NMISC) Contact Name: Mr. Yonis Adan Adan Phone: +252625157572 24/7 Cellphone: +252615157572 Email: maritime.advisor@mpmt.gov.so Sea vision: NMISC-Somalia Watch Keeper 1 IORIS: NMISC-Somalia Watch Keeper 1 C/o: Mogadishu seaport Hamarjajab District
16.	**South Africa**	South Africa Maritime Rescue Coordination Centre Tygerberg Park, Plattekloof, Cape Town 7500 Capt. Ravi Naicker: Rnaicker@samsa.org.za/ imorg@samsa.org.za +27 21 938 3300 mrcc.ct@samsa.org.za
17.	**Seychelles**	National Information Sharing and Coordination Centre Bois De Rose Email: Director@niscc.gov.sc Tel; +2484385657
18.	**Sudan**	Regional Maritime Information Sharing Centre (ReMISC), in Sudan Maritime Controlling Capt. Islam Babkir Abudarag.

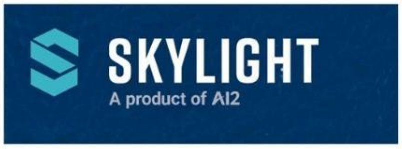
		Tel: 00249912341776 Email: abudaragoes@gmail.com
19.	**UAE**	
20.	**Tanzania**	MRCC Dar Es Salaam TPA Control Tower 13th Floor Email: mrccdar@tasac.go.tz Mob: +255 715 886295 +255 767 886295
21.	**Yemen**	Regional Maritime Information Sharing Center Cc: 1- Mohammed Al- Majashi 2-Adeeb Ahmed Abdulsattar Email: Regional Maritime Information Sharing Center (ReMISC) remisc@maa-yemen.com Yemen Maritime Rescue Coordinating Centre (MRCC) mrcc@maa-yemen.com +44 7404 550899/ +967 777810392

Contact information for every RCC and MRCC around the world:
SAR Contacts - Search and Rescue Contacts World-Wide

DCOC
DJIBOUTI CODE OF CONDUCT

ACKNOWLEDGEMENT

The Regional Workshop on Development of Standard Operating Procedures (SOPs) for the DCoC/JA Information Sharing Network held at the Jeddah Academy for Maritime Science and Security Studies, Jeddah, Kingdom of Saudi Arabia from July 30 to August 10, 2023, was made possible by the excellent facilitation and support of the following partner organizations and countries:



DCOC
DJIBOUTI CODE OF CONDUCT

CONTACT US

Write to us:
The DCoC Team,
IMO Regional Presence Office,
United Nations Complex Gigiri,
Block P – Middle Level,
P.O. Box 30218 (00100) Nairobi, Kenya.

Email Us:

dcoc@imo.org

Visit us on the web at:

www.dcoc.org

~ENDS~