

Department of Homeland Security
Department of Defense

Report on Developing an
Environment for Sharing Information
to
Combat Illegal, Unreported, and
Unregulated (IUU) Fishing

12/30/2015

Distribution A:

Approved for public release: distribution unlimited.

This report responds to one of four implementation steps called for under Recommendation #3, Maritime Domain Awareness (MDA) in the Action Plan for implementing the recommendations of the Presidential Task Force on Combating IUU Fishing and Seafood Fraud. Specifically, this document provides a report to the National Ocean Council (NOC) Committee on developing an appropriate environment for sharing information between U.S. and foreign government partner users in order to enhance threat analysis and monitoring, which would increase the awareness of decision-makers responsible for combating IUU fishing.

This page intentionally left blank

TABLE OF CONTENTS

Executive Summary 1

Introduction..... 2

Scope..... 2

Background 4

 Maritime Domain Awareness..... 4

 Illegal, Unreported, and Unregulated Fishing..... 4

 Information Sharing 5

Defining An Environment to Share Information 6

 Describe the use case being supported by the information sharing 6

 Identify the specific data elements required to support the use case 6

 Develop a standards based exchange model for the information to be shared 7

 Identify any legislative or policy driven constraints on the information 7

 Implement appropriate controls to ensure proper entitlement management 7

 Implement and monitor the sharing service 8

Recommendations to Implement an Environment for Sharing Information 9

Conclusion 11

Appendix One – Acronyms 12

This page intentionally left blank

EXECUTIVE SUMMARY

In March of 2015, the Presidential Task Force on Combating Illegal, Unreported, and Unregulated (IUU) Fishing and Seafood Fraud published its *Action Plan to Combat Illegal, Unreported, and Unregulated (IUU) Fishing*. The plan calls for the Secretaries of Homeland Security and Defense to provide a report “on developing an appropriate environment for sharing information between U.S. and foreign government partner users in order to enhance threat analysis and monitoring, which would increase the awareness of decision-makers responsible for combating IUU fishing.”

As directed in the Action Plan, and informed by the National Strategy for Information Sharing and Security (NSISS) and the National Maritime Domain Awareness Plan (NMDAP), this report identifies technical considerations and steps required to develop an environment to enable information sharing with partners nations engaged in combating IUU fishing.

Successful information sharing activities are the result of operational, informational and technological understanding achieved through a well-defined and routinely implemented process. Developing an environment to enable information sharing requires a thorough understanding of each of these factors. Cost and implementation timelines are additional drivers. Given these considerations, an environment to share information among partners should have the following goals:

- Identify a low threshold of entry from both a cost and technology perspective
- Provide, as quickly as practicable, an initial information sharing capability to build trust and confidence
- Operate in an internet based, unclassified environment
- Leverage existing policies, technologies and capabilities where possible
- Allow for growth as the technology and processes of partners mature

To facilitate the development of the environment to share information, this report recommends leveraging, where applicable, existing information exchange processes and exchange models as defined in the National MDA Architecture Plan and the Maritime Domain of the National Information Exchange Model (NIEM-M). To empower and build trust within the community, the report recommends the use of the following existing, fielded applications as initial capabilities: Maritime Safety & Security Information System (MSSIS) as well as the All Partners Access Network (APAN) and SeaVision.

This report recognizes that information sharing is about trust and understanding in support of a common goal or mission. Combating IUU fishing is important to partner nations, as well as, to the United States. Defining an environment to enable information sharing and recommending existing capabilities will allow the community to quickly implement an initial capability to build this trust and understanding.

INTRODUCTION

On June 17, 2014, the White House released a Presidential Memorandum entitled “*Establishing a Comprehensive Framework to Combat Illegal, Unreported, and Unregulated Fishing and Seafood Fraud.*” Among other actions, the Memorandum established a Presidential Task Force on Combating Illegal, Unreported, and Unregulated (IUU) Fishing and Seafood Fraud (Task Force) co-chaired by the Departments of Commerce and State, with twelve other Federal agency members.

As directed in the Presidential Memorandum, the Task Force developed a series of “recommendations for the implementation of a comprehensive framework of integrated programs to combat IUU fishing and seafood fraud...” These recommendations included one directing “The Secretaries of Defense and Homeland Security to include IUU fishing threat analysis and monitoring as a component of U.S. and international efforts to increase overall maritime domain awareness [(MDA)].” The Task Force provided those recommendations to the President via the National Ocean Council and published them in the Federal Register on December 18, 2014.

In March of 2015, the Task Force published an *Action Plan* to support the implementation of its recommendations. The Action Plan included a series of “implementation steps,” including one that direct the Secretaries of Homeland Security and Defense to “provide a report to the National Ocean Council (NOC)¹ on developing an appropriate environment for sharing information between U.S. and foreign government partner users in order to enhance threat analysis and monitoring, which would increase the awareness of decision-makers responsible for combating IUU fishing.”² This report responds to that direction.

SCOPE

This report identifies the steps necessary to create an environment to share MDA-related information between the U.S. and international partners to combat IUU fishing. It also discusses available information sharing environments for the short and medium term. This report concentrates on sharing information in an unclassified, non-Public Key Infrastructure (non-PKI) environment.

This report differentiates between an “environment to share information” and an “information sharing environment” as follows. An “environment to share information” is the roadmap necessary to create an application. The application itself would be the information sharing

¹ The National Ocean Council Committee on IUU Fishing and Seafood Fraud

²For continuity and completeness, Recommendation #3 of the Action Plan assigned additional implementation steps to be addressed by DoD and DHS apart from this report. These steps and their status includes: co-hosting a workshop (completed), establishing an Implementation Planning Team (completed), cataloging initiatives (completed), reporting on findings (completed) and providing an implementation plan (in progress).

environment. For example, the architecture plan for SeaVision would be the environment to share information while SeaVision would be the information sharing environment.

This report does not discuss capacity building or other concrete efforts to expand MDA capabilities for partner nations. Statues, authorities, or governance relating to MDA or information sharing are also considered to be outside the scope of this report.

BACKGROUND

Maritime Domain Awareness

Maritime Domain Awareness (MDA) is the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States.³ It enables the development of networks of information through shared goals to fight common problems, including illegal, unreported, and unregulated (IUU) fishing.

On December 31, 2013, the White House released the National Maritime Domain Awareness Plan (NMDAP) to establish “the foundation for the effective understanding of potential and actual maritime threats and challenges by promoting favorable conditions for integrating and sharing information, including intelligence, to inform decision-makers.”

As outlined in the NMDAP, information is an important national asset and, as such, requires a responsible balance between sharing and safeguarding. The NMDAP, consistent with the National Strategy for Information Sharing and Safeguarding (NSISS), promotes the development of the national maritime information sharing environment to support MDA. Such an environment is an important tool in combating IUU fishing.

Illegal, Unreported, and Unregulated Fishing

IUU fishing negatively affects economic markets, undermines the competitiveness of the seafood industry, defrauds consumers and threatens the health and sustainability of global fisheries. This global problem directly affects the lives of more than 2.5 billion people who rely on the sea for their livelihoods and as a primary source of nutrition. It is estimated that IUU fishing costs the global economy billions of dollars each year, representing approximately 20% of the global seafood catch.⁴

The National Strategy for Maritime Security (NSMS) states “Violent confrontations are on the rise as competition increases for these declining marines resources. These incidents put increasing pressure on maritime nations to undertake more aggressive actions, which have the potential to cause conflict and regional instability.”

MDA tools and services are being used to combat these issues. However, disseminating the information from these systems to IUU fishing stakeholders remains a challenge. Additional challenges exist at international government levels, as many of our foreign partners need assistance in discovering and accessing tools as well as sharing and receiving relevant data. Exposing more IUU stakeholders to these technologies and increasing information sharing with international partners will not only help combat IUU fishing, but will have positive effects in

³ National Maritime Domain Awareness Plan, Pg. 2

⁴ MRAG Ltd. And Fisheries Ecosystems Restoration Research, Fisheries Centre, University of British Columbia, “The Global Extent of Illegal Fishing” April 2008

other mission sets, such as combating terrorism, human trafficking, drug smuggling, and other transnational criminal activities.

Information Sharing

Information sharing, as an activity or action, is about improving business processes to execute defined missions to the greatest extent possible. However, “Information Sharing” is a broad term that needs to be clearly defined as it applies to a specific mission or activity. Is the “information” unprocessed sensor data or a refined analytical product? Is “sharing” providing information, no matter the definition, to a partner or is it providing access to an existing system with no information actually exchanged? Based upon the mission, objectives, constraints and partners, “information sharing” can be any or all of these definitions and each impact the recommended solution.

The community of partners combating IUU fishing is as varied as any other international mission. Some partners have mature, robust information sharing capabilities and established processes for combating IUU fishing. Others are new to both with little or no capabilities or processes. Defining an environment to share information to combat IUU fishing needs to support both ends of the spectrum.

Defining an environment to share information is also about coming to an agreement among participating partners or stakeholders about the specific mission goals to be met, the information that needs to be exchanged and the political or legal constraints that must be followed.

DEFINING AN ENVIRONMENT TO SHARE INFORMATION

The following outlines the steps to a well-defined environment to share information:

1. Describe the use case being supported by the information sharing.
2. Identify the specific data elements required to support the use case.
3. Develop a standard definition, model or product for the information to be shared.
4. Identify any legislative or policy driven constraints on the information.
5. Implement appropriate controls to ensure proper entitlement management.
6. Implement and monitor the sharing service⁵.

Each of the steps must be applied to the specific mission space or objective, taking into account all the previously mentioned considerations. The following sections address each step as applied to combating IUU fishing.

Describe the use case being supported by the information sharing

The first step to any information sharing effort is the definition of the use case; the reason why the sharing action should take place. An operational use case describes a specific mission objective to be met through an information sharing activity. A use case should provide sufficient detail to determine the data that needs to be shared and what controls or restriction should be placed on the data.

An environment for sharing information may have multiple use cases, or it may only have a single use case.

For an example of a counter IUU fishing information sharing environment, three potential use cases are offered:

1. Provide Automatic Identification System (AIS) and other position reports to any sharing partner that has the ability to receive, process, and display geo-spatially referenced vessel positions.
2. Provide access to authorized users to a geospatial display tool to visualize vessel positions.
3. Provide to partners, via email, reports about vessel activity that meets jointly developed business rules. For example: Any fishing vessel over a defined tonnage entering an identified exclusive economic zone (EEZ).

Identify the specific data elements required to support the use case

Meaningful information sharing must incorporate the specific data elements needed to support a defined use case. To ensure participants are able to work within their own legislative or policy bounds (a later consideration), understanding why the environment is using specific types of data

⁵ The National Maritime Domain Awareness Architecture Plan, pg. 4

is important. Understanding the decision point behind each data element will aid in the determination of who should share or have access to the data and support prioritizing each element. Data collection and processing takes resources; prioritizing the data elements helps to prioritize the resources.

Once the data elements have been defined, they should be depicted in an easy to understand logical data model. The logical model does not define the implementation specifics but instead, in non-technical terms, illustrates the relationship between each element.

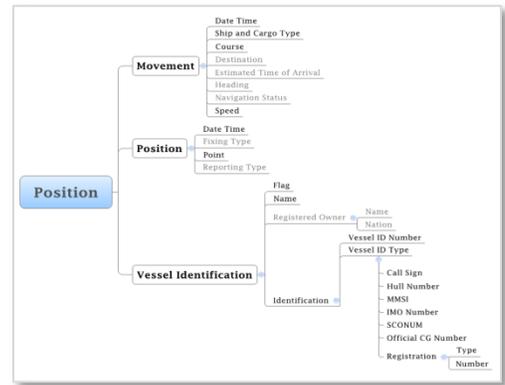


Figure 1: A Position logical model

Develop a standards based exchange model for the information to be shared

With the use case defined and the supporting data elements identified, a standards based exchange model needs to be developed. The exchange model is a technical representation of the logical model and is used by technical personnel who will implement the future environment. The technical model should reflect the elements and relationships in the logical model and should be based on a standard business modeling format like extensible markup language (XML) or Unified Modeling Language (UML).

Identify any legislative or policy driven constraints on the information

Information sharing is more than the technical movement of information between participants. Information sharing usually includes some security component to ensure the information only goes to *authorized* partners. Identifying the information sharing constraints will aid in defining what “authorized” means. Who is authorized could change, depending on the mission or exchange.

A clear understanding of the constraints and their application to each use case is required to build understanding and trust in the information sharing process.

Implement appropriate controls to ensure proper entitlement management

Based upon the understood constraints and the objective of the use case, as well as the technical maturity of the international partners, access control for the environment must be determined. The attributes or roles for the use case need to also be identified. For example, an attribute might be a country or geographic region while a role might be a law enforcement official or marine inspector.

Each role or attribute defines who would be allowed to access what information.

Implement and monitor the sharing service

Implementing an environment to share information in itself does not build trust. Partners need to be able to monitor the sharing to ensure their data is only going where it was intended. The new environment should have an auditing process where participants can verify the receipt, processing, and delivery of their data. It should also be reviewed periodically to adjust levels of data access, depending on growing or lessening maturity of the international partner.

RECOMMENDATIONS TO IMPLEMENT AN ENVIRONMENT FOR SHARING INFORMATION

Successful information sharing activities are the result of operational, informational and technological understanding achieved through a well-defined and routinely implemented process. Developing an environment to enable information sharing requires a thorough understanding of each factor. Cost and implementation timelines are additional drivers. Finally, within the broad community engaged in IUU fishing, political will (both domestically and internationally) must be assessed. Given these considerations, an environment to share information among partners should have the following goals:

- Identify a low threshold of entry from both a cost and technology perspective
- Provide, as quickly as practicable, an initial information sharing capability to build trust and confidence
- Operate in an internet based, unclassified environment
- Leverage existing policies, technologies and capabilities where possible
- Allow for growth as the technology and processes of the partners mature

With an eye on these goals and an understanding of the previously delineated six steps to defining an environment to share information, the following recommendations for creating an initial environment for sharing information to aid in the monitoring and analysis of IUU fishing are below:

1. Charter a working group, co-chaired by the mission owners (DHS and National Oceanic and Atmospheric Administration (NOAA)), to oversee and execute the recommendations. The working group membership should be sufficient to represent the interests of sharing partners of the technical components of the effort and may change with each step.
2. Define the use cases for information sharing to support the combating of IUU fishing. The working group should develop and refine the description of those activities, decisions or efforts that can be improved via information sharing. The product of the effort should be use cases with enough detail to identify the required data elements to share.
3. Define the specific data elements required to support the defined use cases. This activity should only be done after the use cases have been defined. The result of the effort should be logical models.
4. Develop the technical exchange models based upon the logical models. The NIEM is a standardized process used within the United States to define exchange models using XML. The MDA Executive Steering Committee (ESC) oversees the NIEM-M Domain. Working with the NIEM Maritime Domain Steward, the result of the effort will be NIEM conformant exchange models.

-
5. Identify information sharing constraints. Evaluate potential partner nations to determine the proper level of information sharing; specifically what pieces of information will be available and what pieces will not.
 6. Define the controls to ensure proper management. Using the National MDA Architecture Plan as a reference, define a set of controls to manage the data. The result of the efforts will be a detailed description of attribute, roles and controls and a technical description of the implementation.

While this roadmap will result in a well-defined environment to share information, it will not actually provide a venue to share anything. Implementation is the final and most difficult step. Effective implementation will result in an information sharing environment that will support efforts to combat IUU fishing.

However, implementation of a new environment to share information is a long and laborious process. With the current state of IUU fishing, a parallel goal should also be to put something into operation as soon as possible to engage partners and show immediate results for their efforts. Therefore, there should also be consideration of existing operational technologies and how they may be used to provide an environment to share information to combat IUU fishing. A three pronged approach to implementing currently available technology is also recommended:

1. **Maritime Safety and Security Information System (MSSIS):** MSSIS is a freely-shared, unclassified, near real-time data collection and distribution network for sharing AIS information. New partners could become members of MSSIS and begin sharing basic information in a few days.
2. **SeaVision:** SeaVision is an unclassified, maritime web-based tool that is used to view and share a broad range of maritime information. SeaVision is currently in use by national and international maritime information sharing partners. SeaVision uses NIEM conformant exchanges, and supports controls to manage information access.
3. **All Partners Access Network (APAN):** APAN is an unclassified information sharing and collaboration service created by Defense Information Security Agency (DISA) for use by those organizations and individuals that do not have access to traditional DOD systems and networks. APAN is a free service that requires only an internet connection and an email address to use. There are also already existing IUU fishing groups that can be easily expanded to include additional partner groups.

The cost and knowledge threshold for partner nations to start with any of these applications is low. These initial applications would also enable partners to contribute information from existing coastal surveillance radars and other national sensors to enhance overall maritime awareness.

CONCLUSION

This report identifies technical considerations and steps required to develop an environment to enable information sharing with partners nations engaged in combating IUU fishing. Also, this report highlights several available no/low-cost initial, applications already fielded that could provide partners with an initial capability to aid their efforts in enhancing MDA and combating IUU fishing. The primary challenge, though, remains the ability of international partners to prioritize the establishment of such an environment and the persistent use of available applications. Overcoming this challenge needs to be recognized as a prerequisite, in all cases, to achieve success in any mission, including combating illegal, unreported, and unregulated fishing.

APPENDIX ONE – ACRONYMS

AIS - Automatic Identification System
APAN - All Partners Access Network
COCOM - Combatant Command
DHS - Department of Homeland Security
DISA - Defense Information Systems Agency
DOD - Department of Defense
EA - Executive Agent
IPT - Implementation Planning Team
IT - Information Technology
IUU - Illegal, Unreported and Unregulated
MDA - Maritime Domain Awareness
MSSIS - Maritime Safety and Security Information System
NGO - Non Governmental Organization
NIEM - National Information Exchange Model
NMDAP - National Maritime Domain Awareness Plan
NOAA - National Oceanic and Atmospheric Administration
NOC - National Ocean Council
NSISS - National Strategy for Information Sharing and Security
NSMS - National Strategy for Maritime Security
PKI - Public Key Infrastructure
UML - Unified Modeling Language
USCG - United States Coast Guard
USG - United States Government
XML - Extensible markup language