A Framework for Assessing Nontraditional Maritime Threat Management Capabilities

June 2015

BANYAN ANALYTICS
An ANSER Institute
Informing Decisions that Shape the Nation’s Role in the Asia-Pacific

Banyan Analytics is an institute focused on the Asia-Pacific region. The institute uses analysis to inform decisions that shape the Nation’s role in the Asia-Pacific, aiding the U.S. government with the implementation of programs and initiatives involved in regional engagement efforts. The institute is a valuable partner to government offices and other organizations that operate in the Asia-Pacific, leveraging over five decades of ANSER experience supporting the U.S. government with objective research and analysis in addressing challenges that are inherent in coordinating and executing complex initiatives.

The research described in this report was produced by Banyan Analytics, and results from the investment of Analytic Services Inc. in research related to Informing Decisions that Shape the Nation’s Future. The views expressed herein are those of the authors and do not necessarily represent the opinions of Analytic Services Inc., or its research clients and sponsors. You may copy these materials free of charge for educational, noncommercial use if you retain all copyright notices included on them; appropriate citation of the source is requested.

In accordance with Title 17 (USC), Section 107, this material is distributed without profit or payment and is intended for nonprofit research and educational purposes only.

Analytic Services Inc. DMCA Copyright
Copyright © 2015 Banyan Analytics, Analytic Services Inc., All rights reserved.
## Contents

Executive Summary ................................................................................................................ 1  
I. Introduction ......................................................................................................................... 3  
II. Methodology ....................................................................................................................... 5  
   Scope .................................................................................................................................. 5  
   Approach .............................................................................................................................. 5  
   Data ..................................................................................................................................... 6  
III. Towards a Maritime Threat Management Framework .................................................. 9  
   Background Research for Framework Conceptualization ................................................... 9  
      Maritime Threats in WCPO ............................................................................................. 9  
   Coastal Nations’ Authority to Manage Maritime Threats.................................................... 12  
   Limitation of Countries to Manage Threats ....................................................................... 12  
   Framework Development .................................................................................................... 12  
      High-Level Goals ........................................................................................................... 13  
      Objectives ....................................................................................................................... 13  
   Capabilities .......................................................................................................................... 14  
   Activities .............................................................................................................................. 16  
IV. Framework .................................................................................................................... 19  
   General Considerations ....................................................................................................... 20  
   Framework Capability Areas ............................................................................................. 20  
      1. Risk Assessment Program ........................................................................................... 20  
      2. Infrastructure Development Guidance ........................................................................ 22  
      3. Patrol Resources ......................................................................................................... 24  
      4. Surveillance Program .................................................................................................. 25  
      5. Suspicious Activity Reporting Program ....................................................................... 29  
      6. Inspection Protocols .................................................................................................... 30  
      7. Rapid Response Guidance and Resources ................................................................... 32  
      8. Apprehension Protocol ............................................................................................... 34  
      9. Protocols and Resources to Defeat an Imminent Threat ............................................. 35  
     10. Investigation Protocols and Resources ....................................................................... 36
11. Lessons Learned Program .................................................................................................................38
12. Legislative Liaison ...........................................................................................................................38
13. Judicial System and Enforcement Entity ............................................................................................40

V. Putting the Framework into Action ..................................................................................................43
   Coastal Nation Use ...........................................................................................................................43
   Regional Organization Use ..............................................................................................................43
   Donor Country Use ..........................................................................................................................43
   Capability Development ...................................................................................................................43

VI. Conclusions .....................................................................................................................................45
This report examines the components of a coastal nation’s ability to manage nontraditional maritime threats throughout its exclusive economic zone and provides a framework that coastal nations can employ to assess their current capabilities. This study focuses on the nontraditional maritime threats of illegal, unregulated, and unreported fishing; illegal ocean dumping; human smuggling; smuggling of drugs, weapons, and people; and piracy and armed robbery at sea. The ability to manage these threats is especially important to the Pacific Island countries (PICs), which face serious risks to economic development, environmental safety, and demographic security due to the limited resources they have for managing these nontraditional maritime security threats.

First, the report examines established stances of foreign and domestic authorities on security and threat management operations in maritime environments, but also in other domains. Second, it provides a framework for assessing nontraditional maritime threat management capabilities (FANTM), grounded in the authorities presented in the first section. The framework aims to be a step towards assessing a coastal nation’s maritime threat management capabilities by helping to identify strengths, weaknesses, and gaps of its existing system. The framework is centered on 13 key capabilities spanning technology and policy, which together support maritime threat management, and supporting activities associated with each capability.

This framework is intended to assist PICs as they identify gaps in maritime threat management and work toward developing a more robust set of threat management capabilities.

Finally, the report provides recommendations on how FANTM may also be applied by regional organizations (such as the Pacific Islands Forum Fisheries Agreement and the Western and Central Pacific Fisheries Commission) and donor countries (such as Australia, New Zealand, and the United States) in the Pacific. Regional application of the framework may contribute to a shared understanding of the capabilities required throughout the region as a whole and lead to the identification of beneficial areas for development.

FANTM is a first step toward developing a standardized tool for assessing key capabilities targeted against a specific list of threats. It can be built upon to provide insights regarding the management of other maritime threats, such as terrorism and the proliferation of chemical, biological, radiological, nuclear, and explosive materials. It could also be expanded to include additional capabilities, such as licensing processes, vessel registrations, and the Port State Measures Agreement, aimed towards furthering a nation’s ability to capture and deter illicit vessels that would exploit the coastal nation’s waters. Furthermore, applying the framework to island countries may help clarify the relative contributions each of the identified capabilities...
makes to overall maritime security, ultimately allowing coastal nations to apply metrics that can inform decisions on which capabilities to prioritize, given limited resources.
I. Introduction

In 1982 the United Nations Convention on the Law of the Sea (UNCLOS) established the sovereign rights that coastal nations have over their adjacent waters. Claims over adjacent waters extended through the 12 nautical mile territorial waters to the 200 nautical mile exclusive economic zone (EEZ).\(^1\) This extended sovereignty, provided through UNCLOS, gave the coastal nations sole rights to the natural resources (fish, oil, and gas) within their EEZs.\(^2\) By becoming party to UNCLOS, small Pacific Island countries (PICs) in the Western and Central Pacific Ocean (WCPO) greatly expanded their sovereign territory, with over 98 percent of that territory now maritime in nature. This expansion, including rights over a large body of natural resources, provides PICs with great opportunities for economic development.\(^3\)

The rights allowed under UNCLOS are accompanied by strict guidance for coastal nations to secure and protect their maritime domains. Under UNCLOS, coastal nations are expected to ensure the right of innocent passage, protect against armed robbery at sea and piracy, and ensure that living marine resources in their EEZs are protected from over-exploitation, to name a few responsibilities.\(^4\) This guidance placed new pressures on PICs, as their waters are susceptible to the impacts of nontraditional maritime threats including piracy and armed robbery at sea; smuggling of drugs, weapons, and people; human trafficking; illegal ocean dumping; and, of particular concern to the PICs, illegal, unregulated, and unreported (IUU) fishing.

In an effort to comply with UNCLOS guidance, PICs have been actively seeking methods to improve their ability to detect vessels within their waters and distinguish between legitimate and illegitimate operators. While the detection capability is crucial to threat management, PICs may benefit from a more comprehensive approach to maritime threat management, including objectives such as interception, prosecution, and protection. Overall, PICs could benefit from a holistic maritime threat management framework, which would help identify key capabilities for development, allowing for not

---

only protection from current threats but prevention of future threats. Further, such a framework could expand PICs' understanding of existing capability gaps and needs.

This study will examine established stances of international authorities on security and threat management operations (in maritime environments as well as other domains) and will develop a framework—grounded in these authorities—for assessing key capabilities required for maritime threat management operations. This framework can be used by PICs as they work toward development of a more robust set of threat management capabilities and will allow PICs to identify gaps in their approaches to maritime threat management.
II. Methodology

Scope

This study focuses on the management of nontraditional maritime threats (piracy and armed robbery at sea; IUU fishing; illegal ocean dumping; smuggling of drugs, weapons, and people; and human trafficking) within the EEZs of the PICs. This study is further limited to vessels that are underway and the sanctions and enforcement that follow once a suspected vessel has been apprehended.

Approach

The study team approached maritime threat management as a system, composed of actors, country goals, laws, and technologies that work together to defeat, prevent, or otherwise mitigate maritime threats. This perspective allowed the study team to understand how inputs, such as threats, must be managed, shaped, and countered to produce desired outputs (for example, safe waters that comply with UNCLOS mandates). Further, this view allowed the team a means for understanding how outputs lead to desirable outcomes, such as country prestige and economic development, which further motivate countries to invest in threat management capabilities.

Figure 1, on page 7, depicts our concept of the maritime threat management system. It illustrates how national officials, operational culture, knowledge of threats, governing documents, objectives, and capabilities (defined later in this paper) can work together to mitigate potential threats (such as IUU fishing) and produce desirable outputs and outcomes (such as reduced toxic waters and self-reliance). As noted in Figure 1, some system components (such as corrupt officials) impact the system’s ability to effectively manage threats, but changing or optimizing the performance of these components will require a longer-term effort to shift the cultural norms of lower-income island nations. In contrast to these long-term efforts, some components of the system, such as capabilities, can be improved in the near term. To that end, this study will investigate the capabilities needed for PICs to address their maritime threats.

Our study approach, which relied on the systemic view articulated above, consists of two high-level tasks:

- Background research for framework conceptualization
- Framework development

5 Outputs are those desired states that can be reached by a particular country for its waters. Outcomes are more high-level, desired end states. To achieve an outcome, one or more outputs must first be reached.
II. Methodology

Background research for framework conceptualization—To prepare the groundwork for developing a maritime threat management framework for the WCPO region, we first needed to understand a number of elements pertaining to the maritime security domain—including key threats prevalent in the WCPO, how those threats relate to UNCLOS protection mandates, the authority of coastal nations to take action, and existing limitations of the PICs to manage these threats.

Framework development—To recognize key components of threat management systems, the study team also identified principles and common practices throughout various security domains. Synthesizing these common components and subsequent analyses conducted, we identified how various maritime security principles relate to each other within a broader maritime security approach. To facilitate the resulting framework’s practical applicability, we established a scheme of hierarchical relationships facilitating logical decomposition of abstract maritime security concepts to practical maritime operations and assessments. Accordingly, we established a flow from goals to objectives, from objectives to maritime threat management capabilities, from capabilities to activities and enablers, and from these activities and enablers to practical indicators for evaluation.

Data

In support of these two high-level tasks, information was collected from a number of sources, including international laws and treaties, foreign and domestic government reports, government and agency strategic documents, conference proceedings, committee hearings, news and journal articles, and websites and reports from agencies and industry.
II. Methodology

Figure 1—Conceptual View of Maritime Threat Management System
III. Towards a Maritime Threat Management Framework

Background Research for Framework Conceptualization

Maritime Threats in WCPO

A review of maritime literature pertaining to the WCPO identified maritime threats PICs must be prepared to address, among them:

- Illegal, unregulated, and unreported fishing
- Human trafficking
- Smuggling of drugs, weapons, and people
- Illegal ocean dumping
- Piracy and armed robbery at sea

Other maritime threats exist that may benefit from the use of an approach similar to the framework developed, but within the study the focus remains on the threats identified above. Below, we will briefly discuss each threat area, including related trends and implications for PICs as well as the broader international community. Each of the threats described below is explicitly mentioned throughout international maritime law; these laws require the prevention of these threats as well as the protection of maritime operators, marine resources, and the marine environment. While some of the threats are more prevalent in the WCPO, PICs must be prepared to mitigate all possible threats in accordance with guidance provided through international maritime law.

Illegal, unregulated, and unreported fishing. The high percentage of fish stocks in the WCPO and the economic value of these stocks rank the threat of IUU fishing as one of the top concerns for island nations. The Food and Agriculture Organization of the United Nations defines IUU fishing as “either an expressly illegal activity or, at a minimum, an activity undertaken with little regard for applicable standards.” IUU fishing poses a direct threat to the conservation and management of fish stocks; left unfettered, IUU fishing could deplete stocks to an irreparable state. By failing to abide by conservation and management guidelines (for example, equipment usage and zones allowed for fishing) those involved in IUU fishing develop a competitive advantage over legitimate fishers; without proper management, IUU fishing tends to promote more IUU fishing.

In 2003, an assessment of fish stocks by the Secretariat of the Pacific Community indicated that some fish-stock exploitation rates—such as those of big-eye tuna—are unsustainable. It is not possible to say with any certainty which factor is responsible.
for these high levels of exploitation, but IUU fishing is at least a contributing factor. The WCPO is widely impacted by IUU fishing, having the second-highest rate of IUU fishing worldwide after West Africa; IUU fishing is reported to account for 34 percent of the total catch in the Western Pacific. IUU fishing has both near- and long-term implications for social opportunities and economic development and may threaten food security. However, these are not the only impacts of IUU fishing. Besides violating conservation and management standards, IUU fishers may violate regulations associated with the safety of living and working conditions on board, the safety of navigation, and maritime pollution. Depletion of fish stocks may also lead fishers to seek out other means of earning a living on the water; this could mean their involvement in smuggling or even piracy. IUU fishing does not just affect fish, the economy, or food security; it has much larger implications for the safety of all those using the oceans and the existence of other threats.

**Human trafficking.** Human trafficking, defined by the United Nations Office on Drugs and Crime as “the acquisition of people by improper means such as force, fraud or deception, with the aim of exploiting them,” has, in recent reports, been directly linked to the fishing industry in general and IUU fishing vessels in particular. The International Commission on Shipping concluded that “the worst [labor] abuses seem to be associated with fishing”; individuals forced into labor often experience labor abuses because their positions are not identified, and they therefore slip through regulatory measures. In the fishing industry these labor abuses span long working hours, poor living conditions, limited food supply, and even limited access to personal identity documents.

Besides being forced into labor in the fishing industry there are instances of human trafficking victims being sexually exploited. Within Oceania (the oceans encompassing the PICs), sexual exploitation of children by fishers on foreign fishing vessels is the main form of human trafficking. A 2006 UNICEF report pointed to seafarers from foreign fishing vessels as the main perpetrators of sexual exploitation in Kiribati. Fiji, the Solomon Islands, and Vanuatu are also reported locations of further sexual exploitation by those in the fishing industry. Limited job opportunities available to those on the islands may contribute to how readily this exploitation occurs.

**Smuggling of drugs, weapons, and people.** Fishing vessels, such as those available throughout Oceania, are regularly used as mother ships providing needed support to smaller, go-fast vessels actually carrying...
the smuggled goods. These small, often poorly maintained, fishing vessels are used by smugglers to reduce operating costs and increase profit. However, the poor maintenance can have disastrous consequences, resulting in the loss of life, when a vessel is severely overloaded.

While the extent of activity is unclear, it is believed that smuggling of drugs, weapons, and people does occur throughout the Pacific Islands region, even if only in transit. Smuggling has implications for legitimate maritime operations and border security, and there is anecdotal evidence that foreign fishing vessels, ocean pleasure craft, and cruise liners have all been used to facilitate these activities.

Illegal ocean dumping. While some level of pollution risk is expected from legitimate maritime operations, other sources, including land sources and vessels that do not adhere to governing law, contribute pollutants as well. Pollution stemming from ocean-based activities is largely considered to be a result of fishing and aquaculture activities, with fish netting and traps the bulk of debris. This lost or discarded fishing gear threatens to entangle marine life, predominantly marine mammals, and vessels underway.

Current research on the extent of marine pollution throughout the Asia-Pacific region has been largely concentrated on the Northern Pacific and the coastlines of developed countries surrounding the ocean. With the exception of Hawaii, research on marine pollution in the waters of island territories is virtually nonexistent. With a lack of studies, the level of marine pollution that exists within the EEZs of the PICs is unknown. However, the threat’s direct impact on the maritime domain and the potential contributions of debris by IUU fishers demand recognition of this potential threat.

Piracy and armed robbery at sea. Piracy and armed robbery at sea are a distinct threat but may also be carried out by criminal organizations involved in smuggling drugs, weapons, and people. Defined in UNCLOS as “any illegal acts 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 … on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft,” piracy employs the same actions as those of armed robbery at sea; the distinction is where the action is carried out: on the high seas or within a country’s sovereign waters.

Currently, acts of piracy and armed robbery at sea are not a common threat throughout Oceania, but there is the potential for these acts to be carried out if effective law enforcement does not exist. In February of 2015, a passenger boat near Papua New Guinea was boarded by six robbers, armed with

28 Secretariat of the Pacific Regional Environment Programme, Marine Debris Pollution in the Pacific.
29 Secretariat of the Pacific Regional Environment Programme, Marine Debris Pollution in the Pacific, p. 69.
30 Secretariat of the Pacific Regional Environment Programme, Marine Debris Pollution in the Pacific, p. 69.
knives and guns, who stole cash and property from those on board. In this case, the crew on board was assaulted, but the potential for more dangerous incidents exists.\(^\text{31}\)

**Coastal Nations’ Authority to Manage Maritime Threats**

Besides requiring coastal nations to protect and manage their EEZs, UNCLOS gave nations the authority to do so.\(^\text{32}\) This authority, however, came with limitations. Through a review of international maritime law, the study team developed a comprehensive understanding of a coastal state’s authority to act in cases of suspected maritime crimes. For instance, maritime safety and security operations must be carried out by military assets or by assets clearly marked and authorized as government. Authority also varies in accordance with which threat is suspected, as well as whether the suspected vessel is flagged\(^\text{35}\) or unflagged.\(^\text{36}\)

The conditional authority to take action that is codified throughout international maritime law limits the means by which a country can manage its threats. Understanding these restrictions and requirements helped us to shape our definition of capability areas and indicators.

**Limitation of Countries to Manage Threats**

Despite recognizing the dangers posed by maritime threats, most PICs struggle to make progress in managing their impacts. The small areas of land, expansive maritime territory, and constrained funding and resources limit the nations’ ability to take action.\(^\text{37}\) As a result, many of the PICs depend on the support of donor countries (for example, the United States, Australia, New Zealand) for some portion of their security. However, with pressure to become self-sustainable, the PICs cannot rely solely on donor support.

Regional initiatives and organizations promote joint operations and sharing of information and resources to further support the capabilities of individual nations. Regional organizations, focused primarily on the conservation and management of fisheries, have been developed to promote this cooperative culture throughout the region.\(^\text{38}\) Through these regional bodies, the members have agreed upon and implemented protocols governing licensing procedures and monitoring and compliance standards. These organizations have also implemented regularly scheduled joint operations that use personnel and resources from multiple countries (both PICs and donor countries) in a concerted effort to increase maritime law enforcement presence. In spite of these initiatives, a regional approach to maritime threat management is still a challenge.\(^\text{39}\) Differences in applicable laws and regulations, large areas of ocean between the islands, and constrained domestic capabilities all challenge effective regional management.\(^\text{40}\) As a result, the nation’s EEZs continue to be the sites of illicit maritime activities throughout the Asia-Pacific.

**Framework Development**

Our Framework for Assessing Nontraditional Maritime Threat Management Capabilities (FANTM) identifies 13 key capabilities that countries should invest in to effectively manage...(the rest of the text is cut off and not fully visible.)

---


\(^{34}\) UN Convention on the Law of the Sea.

\(^{35}\) A flagged vessel is one that is registered by a particular nation. The vessels are protected by the flag state.

\(^{36}\) An unflagged vessel is a stateless vessel in that it is not registered under any nation.

---

www.anser.org/banyan_analytics

III. Towards a Maritime Threat Management Framework
threats. These capabilities pull from several domains such as technology (for example, sensors) and policy (for example, international agreements, laws, and public outreach). Coastal states should consider these key capabilities as they evaluate their current ability to manage maritime threats.

FANTM is grounded in our understanding of literature from various security sectors identifying fundamental activities related to effective threat management. The following sections describe the high-level goals, objectives, and key capabilities (identified throughout literature) that we recognize as critical to a country’s maritime threat management system.

High-Level Goals

Threat management is supported by three high-level goals:

- **Prevent**—This goal focuses on reducing the potential for a threat to occur or reducing the impact of a threat.\(^{41}\)
- **Respond**—This goal focuses on identifying and arresting suspects and aiding those affected.\(^{42}\)
- **Resolve**—This goal focuses on the enforcement of consequences\(^{43}\) and the process of continuing to improve based on previous experiences.\(^{44}\)

Objectives

High-level goals describe the desired outcome of maritime security efforts (what will be achieved).

These goals are achieved through objectives. Objectives describe actions required to achieve the goals. Maritime threat management goals are supported by seven objectives:

- **Protect**—This objective includes measures taken to reduce the vulnerabilities to, or the consequences associated with, a threat.\(^{46}\)
- **Project a force presence**—This is the overt presence of law enforcement personnel; it serves to deter potential illicit actors from conducting illegal activity and may reduce the time for officials to arrive on scene should an event occur.\(^{47}\)
- **Detect**—Detection refers to the ability to identify when a threat may exist and to track the threat to a point where action may be taken.\(^{48}\)
- **Intercept**—Interception is the ability of law enforcement officers to take action to stop adverse actors from committing a crime, either through lethal or nonlethal force. Adverse actors may be detained and await sanctions.\(^{49}\)
- **Prosecute**—Prosecution is the enforcement of sanctions against individuals involved in criminal activity; sanctions are designed to create a deterrent effect.\(^{50}\)
- **Influence maritime policy and develop agile and relevant regulations**—Both of these objectives serve to regulate and govern the actions of legitimate actors. They also provide the requirements and procedures

---


\(^{42}\)U.S. Counter Piracy and Maritime Security Action Plan.

\(^{43}\)This is an original term that the study team developed by synthesizing literature from several sources.


that should be adhered to in the management of threats.51

Each of these objectives contributes to the achievement of one or more goals. The relationships that exist between high-level goals and objectives are illustrated in Figure 2.

Capabilities

Similar to goals, objectives are achieved through supporting capabilities that are a suite of tools, personnel, procedures, etc. In this section, we identify 13 key capabilities as components of the maritime threat management system performance.

Risk assessment program—Risk assessments are used by law enforcement agencies to establish areas and activities that are most vulnerable to particular threats.52 The results of risk assessments help to inform law enforcement agencies’ priorities and use of constrained resources.53

Infrastructure hardening guidance—Law enforcement agencies may suggest smart practices or establish standards aimed at hardening commercial vessels. Hardening can include strengthening physical structures or adding layers of infrastructure. Some examples of maritime hardening are raising the freeboard on vessels54 and adding locks to bridge55 access points.

Patrol resources—This is the capability to deploy physical resources to high-risk areas in an attempt to deter adverse actors from carrying out illicit activities.56 These assets are not constantly present; they move and can readily be applied to many areas. However, patrols need to be carefully applied, as their overtness is more recognizable and can be avoided.57

Surveillance program—Surveillance includes remote monitoring technologies that can aid in collecting and processing large amounts of data and even detect

---

54 Freeboard is the height between the waterline and the top of the gunwales (sides) or the main deck of a vessel.
55 The bridge is the area (often a room) from which a vessel is commanded.
anomalies and identify them as potential threats. Surveillance of a wide area of an EEZ allows for a more effective understanding of the vessels and activities throughout the waters.

Suspicious activity reporting program—Suspicious activity reporting programs educate the general public on suspicious activities and provide mechanisms for the public to report such activities. Suspicious activity reports, provided by stakeholders and the general public, can help to identify when a potential threat exists.

Inspection protocols—Inspections allow for the review and validation of vessel documentation and the potential to identify probable cause for further inspections and investigations. Protocols guiding inspection are key to ensuring that law enforcement operators act in accordance with international maritime laws.

Rapid response guidance and resources—Rapid response means that law enforcement personnel can respond quickly and appropriately to changing threats. This includes rapidly determining the “right” course of action and the arrival of resources on-scene.

Apprehension protocol—This capability provides guidance to law enforcement officers, including definition of probable cause. When probable cause exists, suggesting that a vessel or operator may have been involved in a criminal activity, law enforcement operators can take both the vessel and operator into custody.

Protocols and resources to defeat an imminent threat—in some cases, when a threat poses an immediate threat to life, lethal force may be required to keep the threat from being carried out. “Defeat” protocols ensure that operators and the island nations they serve have the ability, justification, and training to carry out necessarily lethal missions.

Investigation protocols and resources—This capability provides guidance on when and how a vessel can be further investigated and when and how the operator can be questioned and detained until a decision is made regarding the ability to conduct judicial proceedings. Investigation resources include tools, techniques, and methods to identify, collect, and preserve evidence in order to facilitate the prosecution of criminals.

Lessons learned program—These programs allow operators, decision makers, and policy developers to conduct a post-event analysis of the actions conducted by all stakeholders. This highlights well-executed actions and identifies areas for improvement. This feedback, known as lessons learned, shapes responses to future events.

Legislative liaison—Laws and standards must be consistently developed and refined in order to ensure that harmful actions are identified as illegal activities against which law enforcement officers may take action. Liaisons serve to represent the maritime community’s perspective on potential laws, regulations, and standards.

Judicial system and enforcement entity—An effective judicial system and enforcement entity allows for the prosecution of adverse actors who have been detained and the enforcement of consequences for those found guilty of committing an offense.

---

61“Safety, Security, and Stewardship.”
appropriate judicial system and enforcement entity can play a role in deterring future illicit operators.\textsuperscript{66}

Each of these 13 capabilities supports one or more of the 7 objectives. The relationships between objectives and capabilities are illustrated in Figure 3.

**Activities**

For each capability, the study team has identified key activities that enable its achievement. Figure 4 provides an example of how we mapped the activities to the capabilities.

Figure 3—Swim lane diagram showing relationships between objectives and capabilities
### III. Towards a Maritime Threat Management Framework

#### Figure 4—Swim lane diagrams showing relationships between capabilities and key activities
Coastal states should consider the following key capabilities as they evaluate their current maritime threat management abilities and identify areas for improvement. Each capability is achieved by conducting key activities that should also be considered when evaluating the existence and robustness of each capability. As part of this framework, we provide a series of indicators that countries can use when assessing their capabilities. Indicators are posed in the form of questions and are based on our understanding of the enabling tools, technologies, methods and sociopolitical factors that contribute to the execution of capabilities. The capability, activities, enablers, and indicators are incorporated into tables as follows:

<table>
<thead>
<tr>
<th>Key Activities</th>
<th>Enablers</th>
<th>Capability Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Activity 1</td>
<td>Enabler</td>
<td>Indicator</td>
</tr>
<tr>
<td></td>
<td>Enabler</td>
<td>Indicator</td>
</tr>
<tr>
<td></td>
<td>Enabler</td>
<td>Indicator</td>
</tr>
<tr>
<td>Key Activity 2</td>
<td>Enabler</td>
<td>Indicator</td>
</tr>
<tr>
<td></td>
<td>Enabler</td>
<td>Indicator</td>
</tr>
<tr>
<td></td>
<td>Enabler</td>
<td>Indicator</td>
</tr>
<tr>
<td>Key Activity 3</td>
<td>Enabler</td>
<td>Indicator</td>
</tr>
<tr>
<td></td>
<td>Enabler</td>
<td>Indicator</td>
</tr>
<tr>
<td></td>
<td>Enabler</td>
<td>Indicator</td>
</tr>
</tbody>
</table>

*Note: Not all enablers listed are required for the activity to be completed; the list provided is not all-inclusive; rather, it provides a sample that would require further evaluation before implementation.*
General Considerations

While each capability has distinct activities and enablers associated with it, four common enabling needs emerged. These enablers support a number of activities and their related capabilities:

a. Cooperative relationships—The interconnected nature of the maritime domain means that threats present in the waters of one country or region can easily shift to the waters of another. Therefore, maritime security operations demand cooperative relationships with not only other national law enforcement agencies and private industry, but also with regional maritime security organizations, nations with bordering maritime territories, and more widely the international community as a whole. These types of relationships will encourage the sharing of information, resources, and expertise.

b. Communications systems—These are necessary throughout threat management. They facilitate communication between vessel operators, control centers, flag states, other coastal nations, and more. Communications must be existent and reliable.

c. Information-sharing system—As cooperative relationships are cultivated, information must be shared in a way that is understandable to operators but will not overwhelm them. A common information-sharing system that incorporates relevant data in an accessible format and is available to necessary stakeholders will facilitate further integration during rapidly progressing events.

d. Trained personnel—These are necessary to carry out nearly every key activity identified throughout the framework. Personnel must be proficient in the operational and technical aspects of their position as well as interacting and communicating with stakeholders and the public. It may be recommended that individuals be trained to fill multiple positions, creating redundancy within the system.

Framework Capability Areas

1. Risk Assessment Program

Risk assessments are used by law enforcement agencies to establish areas and activities that are most vulnerable to particular threats. Risk assessments depend on the accurate identification of the threats, vulnerabilities, and consequences associated with the areas and activities of interest. Accurate identification relies on close cooperation with the stakeholders responsible for daily operations and security. The likelihood of these threats hitting vulnerable areas and the relative impact of the consequences are used to assess the total risk of an area.
### IV. Framework

#### Capability 1: Risk Assessment Program

**1. Identify threats, vulnerabilities, and consequences**

- **Enablers**
  - Trained personnel
    - Are maritime law enforcement personnel trained to interact with the private sector to accurately and confidently identify vulnerabilities?
    - Are personnel trained to identify vulnerabilities during the course of inspections?
    - Are personnel trained to identify threat trends based on available information?
    - Are personnel encouraged to share information regarding threats with other agencies as appropriate?
  - Cooperative relationships
    - Does the maritime law enforcement agency regularly interact with regional organizations, law enforcement agencies from other countries, and operators within the private sector (ports, marinas, etc.)?
    - Is information regarding threats shared across these relationships?
    - Is threat information provided through a shared enterprise-level system? Phone calls? Threat bulletin?
    - Are threat trends shared or knowledge of specific threats?
  - Enterprise-level access to shared information
    - Does a system exist that can readily incorporate information from a number of sources from different agencies and/or countries?
    - Given proper authority, can officials from various agencies and/or countries use this system to provide information and to access information provided by others?
    - Are data and information provided by different agencies readily integrated within this system to provide operators with an appropriate understanding of existing threat and vulnerability conditions?
    - Is this information consistently backed up to allow for review of trends, threat information, or areas that are vulnerable?
    - Do personnel receive training on the available system and use the system regularly to maintain the ability to leverage available information?
  - Evaluation methodology
    - Is there a standardized, consistent approach used to elicit responses from the private sector regarding threats, vulnerabilities, and consequences associated with their industry?
    - Is there an established methodology used to identify threats, vulnerabilities, and consequences throughout the inspection process?

- **Capability Indicators**
  - Are personnel trained in the potential ways to evaluate a threat, vulnerability, and consequence?
  - Do personnel participate in or evaluate exercises geared towards identifying vulnerabilities?
  - Are personnel trained in methods of understanding which threats, vulnerabilities, and consequences may be mitigated?
  - Are there standardized approaches to evaluate both the first- and second-order consequences should an event occur?
  - Are exercises conducted to evaluate the vulnerability of a location?
  - Are stakeholder perspectives regarding vulnerabilities and consequences acknowledged and taken into account during the assessment?
  - Are there guidelines regarding which stakeholders or partnering agencies and/or countries should be included in the process and any exercises conducted?

**2. Consider and analyze threats, vulnerabilities, and consequences**

- **Enablers**
  - Trained personnel
    - Are stakeholders and/or the public included in the risk assessment process?
    - Are one-on-one sessions with private-sector stakeholders conducted to identify vulnerabilities without allowing proprietary information to be shared inappropriately?
    - Do law enforcement personnel provide private-sector stakeholders with assurances that any proprietary or law enforcement-sensitive information will not be accessible by others?
    - Do law enforcement officials know what questions to ask to understand the downstream consequences associated with an event at a stakeholder’s location?
    - Do law enforcement partners hold general body meetings with the public to elicit open feedback regarding which consequences (financial, psychological, access to imports and resources) may be the most detrimental?
    - Are requests for information regarding consequences asked in such a way as to minimize panic while eliciting appropriate responses?
  - Outreach mechanism
    - Are stakeholders and/or the public able to provide input regarding the threats that they are most concerned about?
    - Can private-sector stakeholders provide input regarding vulnerabilities through one-on-one sessions?
    - Can input regarding vulnerabilities be readily updated as the private sector implements new security protocols?
    - Can stakeholders and/or the public provide input regarding the consequences considered the most detrimental (financial, psychological, access to imports and resources)?
    - Is this input provided through one-on-one sessions, general body meetings, email or phone repositories, or other methods?

- **Capability Indicators**
  - Do systems exist to facilitate communication within the law enforcement agency itself and between the law enforcement agency and stakeholders and the public?
  - Are law enforcement personnel trained on these systems?
  - Are law enforcement personnel required to maintain a level of proficiency in the operation or maintenance of these systems?
  - Are there standard protocols regarding the involvement of stakeholders and/or the public in the risk assessment?
  - Does this protocol govern how these individuals are involved?
  - Is there a required procedure for how stakeholders and/or the public are included?
  - Is a stakeholder and public input reduced in the risk assessment process?
  - Are there procedures in place to explain why input was not included?

**3. Involve stakeholders and/or the general public**

- **Enablers**
  - Trained personnel
    - Are personnel trained to communicate the importance of conducting an appropriate risk assessment?
    - Are personnel trained to identify the appropriate venue for discussion with individual stakeholders as necessary?
    - Can personnel elicit input from a wide range of stakeholders?
2. *Infrastructure Development Guidance*

Law enforcement agencies may suggest smart practices or establish standards aimed at improving the physical security of commercial vessels. By applying these hardening measures, commercial vessels may deter illicit actors, reducing the demand on law enforcement prevention and response measures. Effective hardening depends on the appropriate identification of high-risk areas and activities, maintaining a balance between security and functionality, and the consideration and analysis of alternatives in order to determine the appropriate mitigating capabilities to employ. Areas identified for hardening must also be prioritized for action as resource constraints will limit long-term development projects. Close relationships with relevant stakeholders and the public are key to ensure that proposed hardening measures align with functionality requirements and will receive support for implementation.
### Capability 2: Infrastructure Development Guidance

#### IV. Framework

<table>
<thead>
<tr>
<th>Key Activities</th>
<th>Enablers</th>
<th>Capability Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outreach mechanism</td>
<td>• Are stakeholders and/or the public included in the process of evaluating hardening alternatives?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Do law enforcement personnel use one-on-one sessions with individual stakeholders to identify existing security needs while limiting the open communication of this information?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Do law enforcement personnel provide individual stakeholders with assurances that access to information regarding security needs will be limited to law enforcement personnel?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Are general body meetings held with stakeholders and the public to elicit requirements regarding access to the maritime domain, the functionality of vessels and landside structures, and the protection and preservation of the environment?</td>
<td></td>
</tr>
<tr>
<td>Input mechanisms</td>
<td>• Do individual stakeholders inform law enforcement personnel of what their security must be able to do, rather than what is needed to improve security?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Are law enforcement officials trained to adjust how questions are asked to elicit the appropriate type of information?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Can stakeholders and/or the public provide input on requirements to access the maritime domain and protect the maritime domain?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Is this input provided through one-on-one sessions, general body meetings, email or phone repositories, or other methods?</td>
<td></td>
</tr>
<tr>
<td>Communication systems</td>
<td>• Do systems exist to facilitate communication within the law enforcement agency itself and between the law enforcement agency and stakeholders and the public?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Are law enforcement personnel trained on these systems?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Are law enforcement personnel required to maintain a level of proficiency in the operation or maintenance of these systems?</td>
<td></td>
</tr>
<tr>
<td>Standard operating procedures</td>
<td>• Is there a standard protocol regarding the involvement of stakeholders and/or the public in the evaluation of hardening alternatives?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Does this protocol govern how these individuals are involved?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Is there a standard procedure used to differentiate relevant information from other information that may be provided?</td>
<td></td>
</tr>
<tr>
<td>Trained personnel</td>
<td>• Are personnel trained in communicating the value of implementing hardening measures?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Are personnel trained to guide conversations with stakeholders and the public to elicit the information required?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Are law enforcement officials trained to identify the pertinent information from all information that may be provided?</td>
<td></td>
</tr>
<tr>
<td>Knowledge of high-risk areas and activities</td>
<td>• Are the same personnel who identified high-risk areas and activities involved in the development of priorities for action?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If not, do the new personnel have knowledge of these areas and activities?</td>
<td></td>
</tr>
<tr>
<td>Knowledge of stakeholder perspectives</td>
<td>• Are stakeholder perspectives regarding high-risk areas and activities acknowledged throughout the process and given consideration during evaluation?</td>
<td></td>
</tr>
<tr>
<td>Trained personnel</td>
<td>• Are personnel trained to consider all high-risk areas and activities and potential threats while determining priorities for action?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Are personnel trained to interact with stakeholders to effectively communicate the priorities for action and manage differences in opinion?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Are personnel trained to conduct the analysis required to prioritize areas and activities for the implementation of hardening measures?</td>
<td></td>
</tr>
<tr>
<td>Evaluation methodology</td>
<td>• Is there an established methodology used when determining areas and resources that should be prioritized for action?</td>
<td></td>
</tr>
<tr>
<td>Material</td>
<td>• Are the materials required for these hardening measures available?</td>
<td></td>
</tr>
<tr>
<td>Funds</td>
<td>• Are there funds available to support the implementation of these hardening measures as needed?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Can incentives be used to encourage stakeholders to implement changes on their own?</td>
<td></td>
</tr>
<tr>
<td>Trained personnel</td>
<td>• Are personnel trained to communicate the value and importance of hardening when stakeholder participation is required?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Are personnel trained and allowed to review with stakeholders why the identified hardening alternative best meets the security needs?</td>
<td></td>
</tr>
<tr>
<td>Stakeholder participation</td>
<td>• Are stakeholders provided the information necessary to ensure their participation in hardening key areas and resources?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Are stakeholders rewarded for their participation in implementing hardening measures?</td>
<td></td>
</tr>
</tbody>
</table>
3. **Patrol Resources**

Patrols task physical resources to high-risk areas in an attempt to deter adverse actors from carrying out illicit activities. Similar to hardening, the ability to patrol requires the identification of high-risk areas and activities, balancing the need for a persistent law enforcement presence with the costs of use, while considering and analyzing which assets may provide the required patrols. The finite number of resources that may be used to patrol, as well as the cost of operating these assets, demands that patrols be prioritized and tasked in accordance with the law enforcement agency’s goals. Assets underway conducting a patrol are responsible not only for reducing the probability that a threat will occur in the high-risk area, but also for monitoring other vessels in the area, collecting information on vessels underway, and taking action against suspicious vessels as requested by navigating to the location of the event.

<table>
<thead>
<tr>
<th>Key Activities</th>
<th>Enablers</th>
<th>Capability Indicators</th>
</tr>
</thead>
</table>
| 1. Identify high-risk areas and activities | Knowledge of threats, vulnerabilities, and consequences | • Are the same personnel who identified threats, vulnerabilities, and consequences responsible for identifying high-risk areas and activities?  
• If not, do the new personnel have knowledge of the threats, vulnerabilities, and consequences previously identified? |
| | Trained personnel | • Are personnel aware of the available methods to analyze the individual threats, vulnerabilities, and consequences?  
• Do personnel understand the benefits and drawbacks of each available method?  
• Are personnel trained to identify whether a different methodology is required?  
• Are personnel trained to conduct the analysis to distinguish the high-risk areas and activities from the individual threats, vulnerabilities, and consequences? |
| | Evaluation methodology | • Is there an established set of methodologies used by personnel to identify high-risk areas and activities?  
• Does a standard approach exist to identify which methodology applies to specific cases? |
| | Knowledge of stakeholder perspectives | • Are stakeholder perspectives regarding high-risk areas and activities acknowledged throughout the process and given consideration during evaluation? |
| 2. Consider and analyze patrol alternatives | Trained personnel | • Are personnel aware of the various alternatives that may be applied to improve security?  
• Are personnel trained to analyze the benefits and implications of each available alternative and identify the next course of action?  
• Are personnel aware of the various resource alternatives that may be used to patrol?  
• Are personnel trained to analyze the benefits and implications of resource alternatives for security patrols and identify potential courses of action? |
| | Evaluation methodology | • Is there a standardized approach to identify the benefits and implications of patrols and other security alternatives?  
• Is there a standardized approach used to evaluate the available security alternatives?  
• Is there a standardized approach to identify the benefits and implications of individual patrolling alternatives?  
• Is there a standardized, consistent approach used to evaluate available patrol alternatives? |
| | Knowledge of stakeholder perspectives | • Are stakeholder perspectives regarding a balance between security and functionality acknowledged and taken into account throughout the assessment? |
| | Standard operating procedure | • Are there standards regarding the level of law enforcement operator safety that must be ensured for patrols to be utilized?  
• Are environmental implications and the demand for use of and access to the maritime domain taken into account while considering patrol alternatives?  
• Is there a standard protocol in place to assess the availability of resources? |
| 3. Prioritize actions | Knowledge of high-risk areas and activities | • Are the same personnel who identified high-risk areas and activities involved in developing priorities for action?  
• If not, do the new personnel have knowledge of these areas and activities? |
| | Knowledge of stakeholder perspectives | • Are stakeholder perspectives regarding high-risk areas and activities acknowledged throughout the process and given consideration during evaluation? |
| | Trained personnel | • Are personnel trained to consider all high-risk areas and activities, potential threats, operator safety, and operational costs of resources while determining priorities for action?  
• Are personnel trained to communicate to stakeholders the rationale associated with the implementation of patrols? |
| | Evaluation methodology | • Is there an established methodology used when determining priorities for patrols?  
• Does this methodology account for hardening measures in place as well? |
4. Surveillance Program

Surveillance of a wide area of an EEZ allows for a more effective understanding of the vessels and activities in EEZ waters than that provided by patrols. Remote monitoring technologies used for surveillance collect information on all licensed vessels as well as all vessels underway within sovereign waters. Advanced monitoring and surveillance technologies can use this information to differentiate between legitimate and suspicious vessels. When a suspicious vessel is identified, the vessel is reported and appropriate action is taken.
<table>
<thead>
<tr>
<th>Capability 4 - Surveillance Program</th>
<th>Key Activities</th>
<th>Enablers</th>
<th>Capability Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Collect information on all licensed vessels</td>
<td>Access to vessel registries</td>
<td>• Does the maritime law enforcement agency have access to current national and regional vessel registries?</td>
<td>• Are law enforcement personnel trained to identify the information provided through those registries?</td>
</tr>
<tr>
<td></td>
<td>Enterprise-level access to shared information</td>
<td>• Does an enterprise-level, shared information system exist?</td>
<td>• Is vessel registry information incorporated into an enterprise-level, shared information system?</td>
</tr>
<tr>
<td></td>
<td>Access to compliance inspection reports</td>
<td>• Does the maritime law enforcement agency have access to historical reports associated with compliance inspections?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vessel monitoring service (VMS) and automatic location communicator (ALC)</td>
<td>• Are long-range receivers used to access information provided through an ALC or VMS?</td>
<td>• Are the limitations of an ALC or VMS understood and considered in implementation?</td>
</tr>
<tr>
<td></td>
<td>Automatic identification system</td>
<td>• Are AIS receivers used to access information provided by vessels?</td>
<td>• Is AIS information incorporated into an enterprise-level, shared information system?</td>
</tr>
<tr>
<td></td>
<td>Long-range identifying and tracking (LRIT)</td>
<td>• Are vessels flagged by the country required to carry an LRIT system on board?</td>
<td>• Are there agreements in place allowing the maritime law enforcement agency access to other nations’ LRIT information?</td>
</tr>
<tr>
<td></td>
<td>Vessel traffic service (VTS)</td>
<td>• Are LRIT information incorporated into an enterprise-level, shared information system?</td>
<td>• Is LRIT information incorporated into an enterprise-level, shared information system?</td>
</tr>
<tr>
<td></td>
<td>Observers</td>
<td>• Are observers deployed aboard licensed fishing vessels?</td>
<td>• Are observers trained to look for suspicious behavior and activities?</td>
</tr>
<tr>
<td></td>
<td>Cooperative relationships</td>
<td>• Does the maritime law enforcement agency regularly interact with regional organizations, other national and international law enforcement agencies, and maritime operators?</td>
<td>• Is information regarding vessels underway within the nation’s sovereign waters, or the waters adjacent to the sovereign waters (another nation’s EEZ or the high seas), shared across these relationships?</td>
</tr>
<tr>
<td></td>
<td>Enterprise-level access to shared information</td>
<td>• Is vessel information provided through a shared enterprise-level system?</td>
<td>• Is information available in real time to allow for action to be taken?</td>
</tr>
<tr>
<td></td>
<td>Electro-optic cameras</td>
<td>• Are electro-optic cameras used to monitor key areas and activities underway?</td>
<td>• Is this information stored to allow for possible use during investigations and judicial proceedings?</td>
</tr>
</tbody>
</table>
### IV. Framework

#### Capability 4: Surveillance Program

**Key Activities**

- Collect information on all vessels underway within sovereign waters.

**Enablers**

- Infrared cameras
  - Are there occasions (nights, bad weather, etc.) when an electro-optic camera is unable to provide necessary information?
  - Are infrared cameras used to monitor key areas and activities underway?
  - Is this information provided in real time to personnel for observation and action as necessary?
  - Are camera feeds incorporated into an enterprise-level, shared information system? Patched into the command center?
  - Is this information stored to allow for possible use during investigations and judicial proceedings?

- Automatic identification system
  - Are land-based AIS receivers used to access information provided by vessels?
  - Is AIS information incorporated into an information-sharing network?
  - Do law enforcement officers understand the limitations of information provided through an AIS?

- Vessel monitoring service and automatic location communicator
  - Are land-based receivers used to access information provided through an ALC or VMS?
  - Can information provided through a VMS be incorporated into an information-sharing network?
  - Are the limitations of an ALC or VMS understood and considered in implementation?

- Vessel monitoring service (VMS) and automatic location communicator (ALC)
  - Are land-based receivers used to access information provided through an ALC or VMS?
  - Are the limitations of an ALC or VMS understood and considered in implementation?
  - Can information provided through a VMS be incorporated into an enterprise-level, shared information system?
  - Is data provided through radar incorporated into an enterprise-level, shared information system?

- Radar
  - Is maritime radar used to identify vessels in the area that are not otherwise transmitting their location?
  - Are law enforcement personnel trained to understand the information provided by maritime radar?
  - Are personnel aware of the limitations of radar data?

- Passive acoustics
  - Are there vessels that do not transmit their location and are too small to be identified using radar?
  - Are there environmental concerns that restrict or prohibit the use of active sonar (for example, marine mammals)?
  - Are passive acoustic systems used to identify the presence of these small vessels in restricted areas?
  - Do law enforcement officers receive training in order to understand information provided by passive acoustics?
  - Can passive acoustic data be incorporated into an enterprise-level, shared information system?

- Active sonar
  - Are there vessels that do not transmit their location and are too small to be identified using radar?
  - Are active sonar systems used to identify the presence of these small vessels in restricted areas?
  - Are law enforcement personnel trained to readily understand information provided through sonar?
  - Can this information be incorporated into an information-sharing system?

- Social media
  - Are social media outlets monitored to identify suspicious activities or events requiring the assistance of maritime law enforcement?

- Suspicious activity reporting system
  - Is there a system available for the public and stakeholders to report suspicious activity?
  - Is this information integrated into an information-sharing network?
  - Is this system otherwise monitored for reports of activity?

- Satellite
  - Does the maritime law enforcement agency have access to satellite data for a portion of or the entire sovereign waters?
  - Is this data at a resolution that allows for identification of vessels of varying size?
  - Are law enforcement personnel trained to understand the information provided by satellite images?
  - Is satellite data incorporated into an enterprise-level, shared information system?

- Unmanned aerial vehicle (UAV)
  - Are UAVs used to conduct regular surveillance operations?
  - Is the information from the UAV readily accessible by all personnel or by the operator?
  - Is the information provided in real time to personnel for observation and action as necessary?
  - Is this information stored to allow for possible use during investigations and judicial proceedings?
  - Are law enforcement officers trained to operate a UAV?

- Unmanned underwater vehicle (UUV)
  - Are UUVs used to conduct regular surveillance operations?
  - Is the information from the UUV readily accessible by all personnel or by the operator?
  - Is the information provided in real time to personnel for observation and action as necessary?
  - Is this information stored to allow for possible use during investigations and judicial proceedings?
  - Are law enforcement officers trained to operate a UUV?
### IV. Framework

**Capability 4: Surveillance Program**

#### 3. Differentiate between legitimate and suspicious vessels

**Key Activities**
- 3.

**Enablers**
- Trained personnel
  - Are personnel trained to use information from disparate sources to verify and validate a vessel's status and location?
  - Do personnel know what information is available for this analysis and how to gain access to that information?
  - Are personnel trained to identify key operations (slow transit speed, proximity to another vessel, etc.) that may be suspicious?
  - Are personnel able to identify vessels with restrictions, as well as violations of those restrictions (areas that are restricted, operating speeds that may suggest certain actions)?
  - Can personnel identify when enough information is not available to verify a vessel and suggest action to remedy this gap?

**Capability Indicators**
- Enterprise-level access to shared information
  - Does an enterprise-level, shared information system exist?
  - Given proper authority, can law enforcement officers from various agencies and/or countries provide and access data and information available through the system?
  - Are data and information readily integrated and visualized in an understandable manner for law enforcement personnel of various backgrounds?
  - Are law enforcement officials trained to access, use, and understand the information available through the system?
  - Are law enforcement officials able to manually adjust what information is viewed on screen?
  - Is the information available in real time to allow for action to be taken?
  - Is this information consistently backed up to allow for possible use during investigations and judicial proceedings?

- Anomaly detection software
  - Is software used to rapidly evaluate available data and identify anomalies and irregularities?
  - Do law enforcement personnel understand when the use of this software may be worthwhile?

#### 4. Report suspicious vessels

**Key Activities**
- 4.

**Enablers**
- Enterprise-level access to shared information
  - Does an enterprise-level, shared information system exist?
  - Can this system be used to push information regarding potentially suspicious vessels to law enforcement personnel responsible for taking further action and to those deployed aboard law enforcement resources?
  - Is the information available in real time to allow for action to be taken?
  - Is this information consistently backed up to allow for possible use during investigations and judicial proceedings?

**Capability Indicators**
- Communication systems
  - Does a system exist to allow law enforcement personnel to notify and communicate with others within the agency when a vessel is suspected of suspicious activity?
  - Are there multiple systems that can be used to provide the same information, creating redundancy and improving the ability of communications to continue despite events that may affect the operation of some systems?
  - Are personnel trained on all the systems available for use?
  - Are personnel expected to maintain a certain level of proficiency on each system?
  - Do these systems allow rapid communication with multiple officials simultaneously?

#### 5. Identify need for action

**Key Activities**
- 5.

**Enablers**
- Knowledge of potential suspicious activity
  - Has a potentially suspicious activity been identified?
  - Does available information support this suspicion?

**Capability Indicators**
- Trained personnel
  - Are personnel trained to identify potentially suspicious activities that require further review?
  - Can personnel identify when enough information is not available to verify a vessel?
  - Are law enforcement officials aware of the alternatives that can be employed to collect further information on a suspicious vessel?
  - Can personnel suggest which alternative may be employed?

**Capability Indicators**
- Communication systems
  - Does a system exist to allow law enforcement personnel to notify and communicate with others within the agency when a vessel is suspected of suspicious activity, and what action is to be taken?
  - Are there multiple systems that can be used to provide the same information, creating redundancy and improving the ability of communications to continue despite events that may affect the operation of some systems?
  - Are personnel trained on all of the systems available for use?
  - Are personnel expected to maintain a certain level of proficiency on each system?
  - Do these systems allow rapid communication with all law enforcement personnel simultaneously?
5. Suspicious Activity Reporting Program

Reports of suspicious activities, provided by stakeholders and the general public, can help to identify when a potential threat exists. For the general public to report suspicious maritime activities, they must be educated and involved in the threat management process. Maritime security officials must monitor reports and social media outlets for potential events reported by the public. The report of a suspicious activity should be passed along the chain of command to identify action needed.
6. Inspection Protocols

Protocols guiding inspection are key to ensuring that law enforcement operators act in accordance with international maritime laws. Inspections allow for the review and validation of vessel documentation and the potential to identify probable cause for further inspections and investigations. Law enforcement officers review documents carried aboard vessels and compare the data to information collected on all licensed vessels as well as basic ship information. In the event that discrepancies are identified, law enforcement officers conduct a preliminary inspection of vessel compartments, search for drugs, and use biometric data to identify vessel operators.
### IV. Framework

<table>
<thead>
<tr>
<th>Capability 6</th>
<th>Inspection Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Collect information on all licensed vessels</td>
<td></td>
</tr>
<tr>
<td><strong>Key Activities</strong></td>
<td><strong>Enablers</strong></td>
</tr>
<tr>
<td>Access to vessel registries</td>
<td>• Does the maritime law enforcement agency have access to current national and regional vessel registries?</td>
</tr>
<tr>
<td>Enterprise-level access to shared information</td>
<td>• Are law enforcement personnel trained to identify the information provided through these registries?</td>
</tr>
<tr>
<td>Compliance inspection reports</td>
<td>• Is vessel registry information incorporated into an enterprise-level, shared information system?</td>
</tr>
<tr>
<td>Observers</td>
<td>• Is vessel registry information updated to remain current?</td>
</tr>
<tr>
<td>On-scene, trained personnel</td>
<td>• Are law enforcement personnel trained to identify when a vessel’s information requires updates?</td>
</tr>
<tr>
<td>Interpreter or translator</td>
<td>• Does an enterprise-level information-sharing system exist?</td>
</tr>
<tr>
<td>Standard operating procedure</td>
<td>• Given proper authority, can law enforcement officers from various agencies and/or countries provide and access data and information available through the system?</td>
</tr>
<tr>
<td>Established standards</td>
<td>• Are data and information readily integrated and visualized in an understandable manner for law enforcement personnel of various backgrounds?</td>
</tr>
<tr>
<td>Public knowledge of standards</td>
<td>• Is the information available in real time to law enforcement officials conducting inspections?</td>
</tr>
<tr>
<td>Vessel compartment inspection technology</td>
<td>• Is this information consistently backed up to allow for possible use during investigations and judicial proceedings?</td>
</tr>
<tr>
<td>Ranging and/or length assessment technology</td>
<td>• Does the maritime law enforcement agency conduct regular compliance inspections?</td>
</tr>
<tr>
<td>Radiation detectors</td>
<td>• Are these reports incorporated into an enterprise-level information-sharing system in a manner that allows law enforcement officials to access the historical compliance inspection reports associated with a particular vessel?</td>
</tr>
<tr>
<td>At-sea access to a database of types of radiation and legitimate emitters of that type of radiation</td>
<td>• Are law enforcement officials aware of the information provided within a compliance inspection report and the frequency with which these inspections are conducted?</td>
</tr>
<tr>
<td>• Are observers deployed aboard licensed fishing vessels? How often?</td>
<td></td>
</tr>
<tr>
<td>• Are observers trained to look for suspicious behavior and activities?</td>
<td></td>
</tr>
<tr>
<td>• Can observers regularly provide information on a vessel’s operations, or the operations of another vessel in proximity, to their command center?</td>
<td></td>
</tr>
<tr>
<td>• Does a communication system exist to facilitate this information sharing?</td>
<td></td>
</tr>
</tbody>
</table>

www.anser.org/banyan_analytics
### 7. Rapid Response Guidance and Resources

Rapid response means that law enforcement personnel can respond quickly and appropriately to changing threats. Rapid response demands the consideration of the options available to a law enforcement agency to take action related to suspicious vessels, determination of the appropriate response, prioritization of these as-needed events against enduring patrols, and navigation of resources to the event’s location.
### IV. Framework

<table>
<thead>
<tr>
<th>Capability 7</th>
<th>Rapid Response Guidance and Resources</th>
</tr>
</thead>
</table>

#### 1. Identify need for action

**Key Activities**
- Knowledge of potential suspicious activity
- Trained personnel
- Communication systems

**Enablers**
- Has a potentially suspicious activity been identified?
- Does available information support this suspicion?
- Are personnel trained to identify potentially suspicious activities that require further review?

**Capability Indicators**
- How do maritime law enforcement personnel notify others within the agency of a vessel they consider suspicious?
- Are there systems that allow rapid communication with all personnel simultaneously?

#### 2. Consider and analyze response alternatives

**Key Activities**
- Knowledge of potential suspicious activity
- Trained personnel
- Real-time knowledge of asset status, type, and location

**Enablers**
- Is there a known suspicious vessel (or known suspicious activity) within sovereign waters?
- Are personnel trained to differentiate between situations that require on-scene law enforcement personnel and those that require more information?
- Are personnel aware of the various alternatives that may be employed to respond to a report of suspicious activity in order to collect more information?
- Are personnel aware of the situations in which these alternatives may apply?
- Are personnel trained to account for law enforcement safety implications when considering on-scene personnel alternatives?

**Capability Indicators**
- Are the personnel deploying assets for patrols aware of the varying location and status of potential resources?
- Do personnel know what resources can provide the on-scene presence required? Manned surface vessels? Manned aircraft?
- Do personnel know what resources can be tasked to collect more information? UAS? UUV? Satellites?

#### 3. Prioritize actions

**Key Activities**
- Knowledge of potential suspicious activity
- Standard operating procedures

**Enablers**
- Does procedure dictate which alternatives should be considered based on the situation (type of vessel, reported suspicious activity)?
- Has procedure established a consistent method for quickly evaluating and selecting the alternative to be implemented?
- Are certain law enforcement personnel required to be involved in the consideration of alternatives?

**Capability Indicators**
- Has a potentially suspicious activity been identified?
- Do all personnel have knowledge of a potential suspicious activity?
- Does available information support this suspicion?

#### 4. Task resources

**Key Activities**
- Knowledge of potential suspicious activity
- Standard operating procedures
- Real-time knowledge of resource status, type, and location

**Enablers**
- Does procedure dictate that certain security patrols continue regardless of suspected criminal activities or suspicious vessels?
- Are certain criminal activities considered more egregious than others?
- Are certain law enforcement personnel required to be involved in prioritizing actions?
- Are certain suspicious activities considered better indicators of a threat?
- Is there a specified methodology applied when determining priorities for action?

**Capability Indicators**
- Are stakeholder perspectives regarding suspicious activities considered in determining appropriate action?

#### 5. Navigate to event location

**Key Activities**
- Knowledge of environmental conditions

**Enablers**
- Are personnel trained to consider the potential impacts of failing to take action towards a suspicious activity?
- Are personnel trained to consider the implications of re-tasking previously deployed law enforcement resources?
- Are personnel trained to present these options and implications to the decision maker when identifying priorities?

**Capability Indicators**
- Are personnel trained to consider available resources and priority areas and activities to identify an effective response?
- Are personnel able to rapidly communicate this tasking to the law enforcement personnel involved in the response?

**Funds**
- Are there funds available to support resources to be continuously underway?

**Trained personnel**
- Are personnel trained in the operation of resources?
- Are personnel and resources readily deployable if they are not already underway?

**Knowledge of environmental conditions**
- Do personnel know the environmental conditions that may restrict navigation (rain, wind, draft, etc.)?
- Do personnel have ready access to information relating to environmental conditions while on board?
8. Apprehension Protocol

These protocols provide guidance to law enforcement operators when taking a vessel and operator into custody. A vessel can be further investigated, and the operator can be questioned and detained, until a decision is made regarding the ability to conduct judicial proceedings. The ability to apprehend a suspected adverse actor depends on law enforcement authorities instructing a suspected vessel to stop, and pursuing a suspected vessel that ignores instruction (contingent upon the right to pursue in certain waters). Once a suspected vessel is stopped and inspected, if there is evidence to suggest criminal activity, vessel operators must be detained and the vessel brought to port for further investigation.
9. Protocols and Resources to Defeat an Imminent Threat

In some cases, when there is an immediate threat to life, lethal force may be required to keep the threat from being carried out. The option to defeat an adversary is a last resort; it puts law enforcement officers at a greater risk of life and could endanger other people aboard the vessel. However, it is an ability law enforcement officers need to be prepared for, as in some cases there are no other options to protect against some criminal acts. These protocols and resources ensure necessary preparation. Similar to apprehension, the ability to defeat requires law enforcement authorities to instruct a suspected vessel to stop, and to pursue a suspected vessel that ignores instruction (contingent upon the right to pursue in certain waters). In the event that the suspected vessel does not stop, and it poses a threat to life, authorities may take action to foul a vessel, forcing it to stop. When this occurs the suspected vessel must be recovered and brought to port for further action.

<table>
<thead>
<tr>
<th>Key Activities</th>
<th>Enablers</th>
<th>Capability Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Bring vessel to port</td>
<td>Escort</td>
<td>Can maritime law enforcement personnel escort a vessel to port?</td>
</tr>
<tr>
<td></td>
<td>Ability to tow</td>
<td>Can a maritime law enforcement vessel tow the captured vessel to port if necessary?</td>
</tr>
<tr>
<td></td>
<td>Standard operating procedure</td>
<td>Does procedure dictate when a vessel may be required to go to port?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Is there a standardized procedure to be followed when escorting a vessel to port?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does procedure govern what port a vessel should be brought to?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Is there a procedure in place for towing a vessel to port?</td>
</tr>
<tr>
<td></td>
<td>Laws and agreements</td>
<td>Are there agreements in place dictating where a vessel should be brought if needed based on the vessel’s flag?</td>
</tr>
<tr>
<td></td>
<td>Trained personnel</td>
<td>Are personnel trained to take action to escort a vessel to port?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Are personnel trained to tow another vessel into port?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Are personnel trained to explain to crew members where the vessel is going and why?</td>
</tr>
</tbody>
</table>
## Key Activities

1. **Instruct vessel to stop**
   - At-range loudhailer
     - Are all systems equipped with a loudhailer to provide auditory instructions?
     - Can these instructions be provided at a safe distance until the status of the other vessel can be determined?
   - Lights
     - Are all systems equipped with lights that provide a visual cue to another vessel underway to stop?
     - Can these lights be observed during daytime operations?
   - Standard operating procedure
     - Is there a standardized procedure in place regarding when auditory instructions should be communicated to a vessel?
     - Does procedure dictate what information must be communicated?
     - Does procedure require that instructions be provided a certain number of times?
     - Does procedure require that instructions be provided in certain languages depending on location?

2. **Pursue vessel that ignores instruction**
   - Laws and agreements
     - Is the coastal nation party to regional, bilateral, or multilateral agreements that allow pursuit to continue into the sovereign waters of another nation?
     - Are there agreements in place that authorize another state to take action on behalf of the coastal state?
   - Continued, overt presence
     - Can a coastal nation’s law enforcement resources provide a continued, overt presence through the use of manned surface vessels, manned aircraft, or UAVs until the adversary vessel is captured or enters another nation’s sovereign waters?
   - Cooperative relationships
     - Does the maritime law enforcement agency regularly interact with regional organizations, other national and international law enforcement agencies, and maritime operators?
     - Do these relationships allow for continued pursuit into another nation’s waters?
     - Do these relationships allow access to additional resources to pursue, or apprehend, a suspected vessel that ignores instruction?
     - Are there conditions related to when another nation’s resources may be used in pursuit?
   - Communication systems
     - Do communications systems exist for deployed maritime law enforcement personnel to notify others within the same agency of a vessel that requires pursuit?
     - Do communications systems exist for a coastal state to communicate with another to provide information regarding a pursuit entering its waters and the outcome of an action taken?
     - Are there multiple systems that can be used to provide the same information, creating redundancy and improving the ability of communications to continue despite events that may affect the operations of some systems?
     - Are law enforcement personnel trained on these systems?
     - Are law enforcement personnel required to maintain a certain level of proficiency on these systems?
   - Shipriders
     - Are shipriders deployed aboard partner country assets to extend the reach of the maritime law enforcement agency?
     - Are deployed shipriders authorized to pursue vessels that ignore instruction?
   - Standard operating procedure
     - Is there a standardized procedure in place regulating when fouling actions may be taken?
     - Are there requirements on communicating the fact that fouling actions will be taken if the vessel does not comply?
     - Does protocol govern which law enforcement personnel have the authority to determine when fouling actions are conducted?
     - Are there restrictions on what fouling actions may be applied depending on the situation?
   - Laws and agreements
     - Are there agreements in place that prevent the use of fouling or lethal force?
     - Do agreements restrict these actions for use against vessels conducting certain types of activities?
   - Fouling technology
     - Are deployed resources have access to fouling technology?
   - Trained personnel
     - Are law enforcement personnel trained to identify situations that require fouling?
     - Are law enforcement officials able to rapidly evaluate which fouling approach is the most conducive to the current situation?
     - Are maritime law enforcement personnel trained to use available fouling technology?
     - Are these law enforcement officers required to maintain a minimum proficiency on these technologies?
   - Salvage divers and equipment
     - Does the state have access to salvage divers and equipment should a vessel be scuttled or sunk during fouling?

3. **Foul**
   - Escort
     - Can maritime law enforcement personnel escort a vessel to port?
   - Ability to tow
     - Can a maritime law enforcement vessel tow the captured vessel to port if necessary?
   - Standard operating procedure
     - Does procedure dictate when a vessel may be required to go to port?
     - Is there a standardized procedure to be followed when escorting a vessel to port?
     - Does procedure govern what port a vessel should be brought to?
     - Is there a procedure in place for towing a vessel to port?
   - Laws and agreements
     - Are there agreements in place dictating where a vessel should be brought if needed based on the vessel’s flag?
   - Trained personnel
     - Are personnel trained to take action to escort a vessel to port?
     - Are personnel trained to tow another vessel into port?
     - Are personnel trained to explain to crew members where the vessel is going and why?
10. Investigation Protocols and Resources

When inspections or actions of a suspicious vessel suggest that the vessel may have been involved in illegal activities, investigation is required. Investigation identifies, collects, and preserves evidence to facilitate the prosecution of criminals. Investigations rely on preliminary inspections of vessel compartments, detection of drugs, and the identification of vessel operators using biometric data. When evidence is identified on board a suspected vessel, the crime scene must be secured, allowing the evidence to be preserved and collected to facilitate further investigations and the evaluation of evidence.
IV. Framework

Key Activities

2. Detect drugs

- Collection device
  - Are personnel equipped with appropriate equipment to collect trace amounts of drugs for testing?

- Drug detection device
  - Are personnel equipped with devices used to identify a drug?

- At-sea access to a database of drug composition
  - Do personnel have access to a database to identify the composition of a drug or how individual components may be used to make certain types of drugs?

- Standard operating procedure
  - Is there a standardized procedure governing when a search for drugs may be conducted?
  - Does protocol exist defining how this search must be conducted?
  - Are procedures for identifying and collecting trace amounts of drugs outlined?

- Trained personnel
  - Are personnel trained to identify smells that may be associated with drugs or attempts to conceal the presence of drugs?
  - Can personnel identify paraphernalia associated with drugs or used to make drugs?
  - Are personnel trained in the handling and testing of drugs, equipment, etc.?

- Shipriders
  - Are shipriders deployed aboard partner country assets to extend the reach of the maritime law enforcement agency?
  - Are deployed shipriders trained and authorized to identify and test for drugs as necessary?

3. Identify vessel operators using biometric data

- Biometrics collection device
  - Are on-scene personnel equipped with devices and procedures to collect biometric data from vessel operators?

- At-sea access to biometrics database
  - Do on-scene personnel have real-time access to biometrics databases to identify the vessel operators?

- Standard operating procedure
  - Do procedures exist regulating when vessel operators may be required to provide biometric data in addition to documentation to ensure proper identification?
  - Are there regulations regarding how this biometric information may be provided?
  - Are there procedures in place to ensure the rights and safety of vessel operators?

- Trained personnel
  - Are personnel trained in the collection of biometric data?
  - Are personnel trained in accessing available biometrics databases?
  - Are personnel trained to ensure their own safety should the need arise?

- Shipriders
  - Are shipriders deployed aboard partner country assets to extend the reach of the maritime law enforcement agency?
  - Are deployed shipriders trained and authorized to use biometric data to identify vessel operators?

4. Secure crime scene

- On-scene, trained personnel
  - Are personnel trained to understand what constitutes a crime scene and in methods to identify a crime scene?
  - Are personnel on-scene appropriately trained to secure the crime scene?
  - Are personnel trained to secure the scene?

- Standard operating procedure
  - Is there a standardized procedure associated with securing a crime scene aboard a vessel at sea?

- Laws and agreements
  - Are there national laws regarding how a crime scene must be secured?

5. Identify, preserve, and collect evidence

- On-scene, trained personnel
  - Are personnel trained to identify different types of evidence that may relate to various maritime crimes?
  - Are personnel trained in methods of collecting and/or preserving the evidence identified?
  - Are personnel on-scene appropriately trained to identify, preserve, and collect evidence?

- Evidence storage
  - Do on-scene personnel have access to appropriate evidence storage equipment?

- Standard operating procedure
  - Does procedure dictate how the presence of evidence should be documented prior to collection?
  - Is there a standardized procedure in place pertaining to the collection and storage of evidence?
  - Is procedure aligned with the type of evidence being collected?

- Electro-optic cameras
  - Are electro-optic cameras used to allow for possible use during investigations?
  - Are personnel trained to analyze and evaluate camera feeds for the identification of evidence?
  - Can software be used with camera feeds to improve the identification of evidence?

- Infrared cameras
  - Are infrared cameras used to allow for possible use during investigations?
  - Are personnel trained to analyze and evaluate camera feeds for the identification of evidence?

- Unmanned aerial vehicles
  - Are UAVs equipped with real-time camera feeds? Can these camera feeds be stored to allow for possible use during investigations and judicial proceedings?
  - Can these camera feeds be collected at a distance to reduce the potential of the vehicle being identified and the criminal activity halted?
11. Lessons Learned Program

A lessons-learned program allows for a post-event analysis of the actions conducted by all stakeholders, highlighting well-executed actions and identifying areas for improvement. The ability to identify lessons depends on the ability to identify the need to take action in order to adjust threat management operations. Conducting debriefs following events may help to highlight areas for improvement. To ensure that all operators take action in accordance with accepted standards, identified lessons and smart practices need to be appropriately distributed; cooperative relationships assist in this distribution.

---

12. Legislative Liaison

Laws and standards must be consistently developed and refined in order to ensure that harmful actions are identified as illegal activities against which law enforcement officers may take action. Law enforcement officers have an awareness of the criminal or disruptive acts occurring as a result of their proximity on the job; their knowledge should be leveraged in the development or redefinition of applicable laws and standards. Data associated with arrests should also be used to identify trends associated with illicit actors who are repeat offenders, to better inform the consequence standards associated with certain crimes. Similar to the identification of lessons learned, the development of laws and standards requires identifying the need for change; this can be done by threat management officials, or may be suggested through the involvement of stakeholders and the general public. When possible,
the public and stakeholders should be notified of proposed changes and allowed to comment on any interim rule developed before the rule becomes finalized. Actions must also be taken to use both international and national laws to criminalize these illicit activities and to ensure that the consequence standards are such that they discourage recidivism.

<table>
<thead>
<tr>
<th>Key Activities</th>
<th>Enablers</th>
<th>Capability Indicators</th>
</tr>
</thead>
</table>
| 1. Identify need for action | After-action report | • Is a report highlighting the successes and areas for improvement following a large-scale event compiled?  
• Does this report identify activities, rather than people or positions that could be improved? |
| | Knowledge of stakeholder perspectives | • Do stakeholders have a strong opinion that activities conducted by law enforcement officials require improvement?  
• Is the law enforcement agency aware of these opinions?  
• Are these opinions acknowledged and action taken to consider stakeholder perspectives? |
| | Input from law enforcement officers | • Are personnel trained to identify areas for improvement?  
• Is there a way for personnel to communicate this information with others within the law enforcement agency? |
| 2. Educate the public and stakeholders | Outreach mechanism | • Are stakeholders and the public notified of the potential for new maritime laws and regulations?  
• Do stakeholders and the public receive an explanation of why new laws and regulations are being considered? |
| | Trained personnel | • Are personnel trained in communicating with stakeholders and the public?  
• Can personnel communicate the importance of the new law or regulation while maintaining the prospect of freedom of navigation and access to the maritime domain?  
• Are personnel trained to explain the reasoning for the potential change? |
| | Standard operating procedure | • Does standard procedure govern the situations in which stakeholders and the public are educated regarding new laws and standards?  
• Is there a standard protocol dictating who is educated regarding these new laws and standards? |
| 3. Develop interim rule | Trained personnel | • Are personnel trained to incorporate multiple distinct perspectives in the development of an initial rule?  
• Are personnel trained to interact with stakeholders to elicit feedback on their perspectives? |
| | Knowledge of stakeholder perspectives | • Are stakeholder perspectives taken into account in the initial development of a rule?  
• Freedom of navigation?  
• Balance functionality with security? |
| 4. Submit interim rule for review and input | Outreach mechanism | • Are the purpose and rationale of the interim rule explained to stakeholders and the public?  
• Are stakeholders and the public provided with an explanation of the interim rule?  
• Is feedback from stakeholders and the public on the interim rule requested? |
| | Input mechanisms | • Do stakeholders and the public provide input regarding the interim rule? Changes they’d like to see? Other considerations?  
• Are there means in place to allow this input to be provided to relevant law enforcement personnel and decision makers? |
| | Standard operating procedure | • Does procedure govern whether and when stakeholders and the public are provided information regarding the interim rule?  
• Are there guidelines related to how long an interim rule must remain available for input?  
• Is there a standard procedure on how the rule, and input, must be provided? |
| 5. Develop final rule | Trained personnel | • Are personnel trained to incorporate multiple distinct perspectives when updating an interim rule?  
• Are personnel trained to interact with stakeholders to explain why input on the interim rule was or was not incorporated in the final rule? |
| | Outreach mechanism | • Are personnel made aware of the passing of a final rule?  
• Do law enforcement officials communicate when this finalized rule will become effective?  
• Are new rules posted in relevant, high-traffic areas (marinas, fishing shops, etc.)?  
• Are new rules discussed in an open forum through general body meetings? |
| | Standard operating procedure | • Is there a standardized procedure applied to the incorporation of stakeholder input?  
• Is there a set time between the closing of stakeholder input and the release of a finalized rule?  
• Is due publicity given to what stakeholder input has been reviewed but not included and why? |
| | Knowledge of stakeholder perspectives | • Is stakeholder input evaluated and incorporated as appropriate into the development of the final rule? |
13. Judicial System and Enforcement Entity

An effective judicial system and enforcement entity allows for the prosecution of adverse actors who have been detained and the enforcement of consequences for those found guilty of committing an offense. The coastal nation or the vessel’s flag state must effectively employ this capability in order to deter future illicit operators. To carry out judicial proceedings and enforce consequences for convicted adverse actors, there must first be laws in place criminalizing the activity, along with consequence standards associated with it. These laws and standards must be communicated to all those who use the maritime domain. Judicial proceedings also depend on the identification and preservation of evidence, the detainment of suspected criminals and vessels, and witness testimony of law enforcement officers.
<table>
<thead>
<tr>
<th>Key Activities</th>
<th>Enablers</th>
<th>Capability Indicators</th>
</tr>
</thead>
</table>
| 2. Contribute to development of consequence standards | Knowledge of stakeholder perspectives | - Do stakeholders have a strong opinion on curtailing the extent of activities conducted throughout their waters?  
- Is stakeholder input evaluated and incorporated as appropriate when considering the development of consequence standards? |
| | Cooperative relationships | - Does the maritime law enforcement agency regularly interact with regional organizations, other national and international law enforcement agencies, and maritime operators?  
- Do the members of these relationships strive to ensure consistency in the consequences for participation in maritime criminal activity?  
- Can agreements be reached within these relationships to jointly adjust the list of criminal maritime activities? |
| | Penitentiary system | - Does the coastal state have the penitentiary system to support an extension of consequence standards? |
| 3. Educate the public and stakeholders | Outreach mechanism | - Are stakeholders and the public notified when judicial proceedings are implemented?  
- Are stakeholders and the public aware of the charges faced and the potential consequences that could be applied?  
- Is the progress of the case consistently communicated to stakeholders and the public?  
- Are stakeholders and the public aware of the court’s final ruling and the consequences implemented?  
- Is this information communicated through media sources (TV, radio, social media)? Other sources?  
- Is the impact of laws and standards on the proceedings and consequence enforcement understood by stakeholders and the public? |
| | Trained personnel | - Are personnel trained in communicating with stakeholders and the public?  
- Can personnel communicate the importance of the new law or regulation while maintaining the prospect of freedom of navigation and access to the maritime domain? |
| | Standard operating procedures | - Is there a standard protocol for when information regarding judicial proceedings is shared with the public and stakeholders?  
- Does protocol dictate what information may be shared? |
| 4. Identify, preserve, and collect evidence | Stored evidence | - Are the purpose and rationale of the interim rule explained to stakeholders and the public?  
- Are stakeholders and the public provided with an explanation of the interim rule?  
- Is feedback from stakeholders and the public on the interim rule requested? |
| | Standard operating procedure | - Do stakeholders and the public provide input regarding the interim rule? Changes they’d like to see? Other considerations?  
- Are there means in place to allow this input to be provided to relevant law enforcement personnel and decision makers? |
| 5. Detain | Separation of those detained | - If there were multiple suspects, were they detained separately or consistently monitored to ensure limited communication between suspects? |
| | Standard operating procedure | - Were standard procedures followed in detaining suspects? |
| | Biometric identification of those on board | - Were operators on board identified using biometric data to ensure accurate identification? |
| 6. Bring vessel to port | Standard operating procedure | - Was procedure followed in bringing the vessel to port? |
| | Trained personnel | - Are personnel trained to provide witness testimony during judicial proceedings as necessary? |
| 7. Provide witness testimony | Cooperative relationships | - Does the maritime law enforcement agency regularly interact with regional organizations, other national and international law enforcement agencies, and maritime operators?  
- Is information regarding the status of relevant judicial proceedings shared across these relationships?  
- Does precedent exist facilitating a law enforcement officer from one country to provide witness testimony for proceedings carried out in another country?  
- Are there different methods of providing witness testimony that may be accepted in the case of foreign law enforcement personnel? |
| | Standard operating procedure | - Is there a standardized procedure dictating who may provide testimony?  
- Does procedure prescribe multiple methods of providing witness testimony when law enforcement officers from another country are unable to attend in person? |
FANTM was developed to provide individual coastal nations, regional organizations, and donor countries throughout Oceania with a consistent approach to evaluating and assessing maritime threat management capabilities. Our proposed use for each of these bodies is detailed below.

Coastal Nation Use

Coastal nations, especially those facing growing trends of maritime threats, should assess their individual maritime threat management capabilities and take action to further develop these capabilities in accordance with priorities and resourcing and funding constraints. As a nation develops its national capabilities, the assessment should be periodically reviewed and updated. The results of these assessments should be shared with regional maritime organizations of which the nation is a part, as well as related donor countries.

Regional Organization Use

Regional organizations involved in maritime security and protection must continue to take an active role in assisting individual coastal nations’ efforts. Leveraging individual nations’ assessments, regional organizations can aggregate the capabilities in order to evaluate the region’s capabilities as a whole. This level of application can be used to evaluate how capability development in one country may impact the entire region’s ability to manage maritime threats. Regional assessments may also allow additional resource-sharing opportunities to be identified; this may help reduce the cost of implementation while still benefitting the region as a whole.

Donor Country Use

Due to the limited resources and scale of the Pacific Island countries, and their dependence on aid from donor countries to meet security needs, a donor country requires an understanding of the existing capabilities and gaps that can be filled. Donor countries may use the assessments provided by individual coastal nations or may conduct assessments of their own using FANTM. By conducting an assessment based on the same framework, both the donor country and coastal nation may have a more complete, agreed-upon view of the capabilities available, allowing for a concerted effort towards development.

Capability Development

While coastal nations hold the primary responsibility for the protection and security of their sovereign waters, their capabilities are further supported through regional organizations and donor country aid. However, these additional capabilities must be contributed in a way that is both useable and sustainable by coastal nations. To this end, we recommend that countries not only identify required
capabilities, but prioritize those needs in accordance with the threats they face, the resources they have, and the overall threat management strategies they have in place. Ultimately, a coastal state’s priorities will depend on the state’s goals, laws, and standards it has in place and the resources, infrastructure, and funding available to it.
VI. Conclusions

FANTM provides the Pacific Island countries with a holistic maritime threat management framework to help identify key capabilities for development and a means of assessing their existing capability gaps and needs. This framework can be applied by individual PICs, regional organizations, and donor countries throughout the WCPO to create a consistent approach to maritime threat management aimed at both protection from current threats and prevention of future threats. FANTM is a first step toward developing a standardized tool for assessing key capabilities targeted against a specific list of threats. It can be built upon to provide insights regarding the management of other maritime threats, such as terrorism and the proliferation of chemical, biological, radiological, nuclear, and explosive materials. It could also be expanded to include additional capabilities such as licensing processes, vessel registrations, and the Port State Measures Agreement.

Key capabilities identified through FANTM can be complemented by these landside capabilities, extending the layered approach to maritime security, furthering a nation’s ability to capture and deter illicit vessels that would exploit the coastal nation’s waters. Furthermore, applying the framework to island countries may help clarify the relative contributions each of the identified capabilities makes to overall maritime security, ultimately allowing coastal nations to apply metrics that can inform decisions on which capabilities to prioritize, given limited resources.