|  |  |
| --- | --- |
| From: VTS30 | VTS30/output/15 |
| To: IALA Council | 18 September 2009 |

Liaison Note

Support of VTS to security in the maritime domain

# Introduction

Following inter-sessional meetings, the VTS Committee

# Aim of the document

The aim of the document is to brief the Council on the developments

# Action requested

The Council is invited to approve the developed vision, definitions clarification and views contained in Annex A.

1. SUPPORT OF VTS TO SECURITY IN THE MARITIME DOMAIN

# INTRODUCTION

One of the tasks of WG4, on request of the IALA VTS Committee and the eNAV Committee, is to develop a view on the possible support of VTS towards ship and shore security 9TASK 11 OF THE Working Programme 2006-2010 of the VTS Committee.

# CONSIDERATION OF THE TASK

The VTS Committee studied the task as mentioned above and concluded that, due to the identified role and position of VTS within the VTM functional framework (document VTS30-output- XX)

* the role and especially the information position of VTS within the VTM framework
* possible changes to current VTS measures and services (primary services)
* the possible contribution of VTS towards current and future services, and
* the development of e-Navigation

should be taken into account.

The possible stakeholders related to Security in the maritime domain will have to be identified. Also present legislation, guidelines and manuals are to be studied in order to identify the limitations of possible support of VTS to Security as well as to identify needed modifications and inconsistencies with these legislation, guidelines and manuals.

# Maritime Security

Though much has been written about Maritime Security in all relevant documents, there is no existing definition. SOLAS Chapter XI only provides a definition on Security Incident:

“**Security incident** means any suspicious act or circumstance threatening the security of a ship, including a mobile offshore drilling unit and a high-speed craft, or of a port facility or of any ship/port interface or any ship-to-ship activity.”

Protection against terrorist action in the maritime domain requires, among many things, a complete image of vessel traffic in areas of concern with information on the intentions and cargoes of those vessels as well as vigilant monitoring of this vessel traffic. This information could also be of use to support actions against smuggling of goods and illegal immigrants. VTS monitors a traffic image of almost all vessel traffic in the VTS area and possibly in adjacent waters. VTS has trained operators monitoring this traffic real-time. Whilst it is recognized that security issues are a national matter, VTS Centres can, at present, only contribute to certain security issues. Mainly because VTS Centres are not able to see all traffic, particularly small craft, and VTS-operators are not specifically trained to recognise potential security threats nor are they qualified and equipped to deal with them.[[1]](#footnote-1)

In order to define the role and position of VTS within VTM with respect to Maritime Security, it was necessary to develop a new (working) definition:

“Maritime Security – efforts by various stakeholders which are involved in the prevention and mitigation of harm to people, vessels, waterways, ports and infrastructure from intentional acts”

# Criteria for VTS to contribute to Maritime Security

Recognizing that institutional circumstances may differ worldwide and between countries, the following criteria for VTS to contribute to Maritime Security should be taken into account:

* Depending on the authorities and responsibilities of the VTS Authority, a VTS may provide information to support maritime security services in addition to its primary VTS services;
* VTS provision of or support to maritime security services shall not compromise the provision of the primary VTS services (INS, NAS, TOS) in support of navigation safety, efficiency and protection of the marine environment.
* Through its role in monitoring vessel positions, intentions and other critical information, VTS has a substantial amount of information that is valuable for ship and port security. Through its position, VTS may obtain information to aid or assist security agencies in counter-terrorist activities.
* Sharing of information should occur when a VTS authority enters into specific agreement with appropriate security authorities on a case-by-case basis[[2]](#footnote-2).
* In the case VTS only supports maritime security services, the relationship between the VTS Authority and the appropriate security authorities, and their positions in the decision making processes, should be unambiguously defined in advance.

# CONTRIBUTION TO THE AIMS OF VTM

The contributions and benefits of the support of VTS to Security were analysed in respect to the aims of VTM.

## Security

* Through routine VTS operations and interaction with maritime traffic, VTS operators familiar with the normal operations and circumstances in the VTS area may be in a position to detect and report events out of the ordinary.
* VTS may assist security assessments through:
* VTS in-depth knowledge of port and waterway infrastructure and its criticality and vulnerable locations;
* VTS real-time knowledge of vessel activity, including scheduled movements, vessel locations and intentions;
* VTS in-depth knowledge of regular port operations, including vessel routes, activities and port stakeholders;
* When a vessel is denied access to a port or restricted area for security reasons the VTS may deter-mine a safe anchorage, holding area or designated route. The VTS may communicate this information to the vessel and to the appropriate security authority, and monitor the vessel’s status while anchored or in the holding area, or its progress and compliance to the designated route.

## Safety

* Prevention of intentional harm to vessels, waterways and infrastructure will contribute to the safety of personnel, vessels and cargo.

## Efficiency

* Support from VTS can make compliance with security requirements more efficient by sharing VTS data with multiple stakeholders and one-time reporting of the same information by vessels (e.g., notice of arrival to coastguard, customs, immigration, etc.).

## Protection of environment

* Prevention of intentional harm to vessels, waterways and infrastructure will reduce risks to the marine environment.

# IDENTIFICATION OF POSSIBLE STAKEHOLDERS IN THE RELATIONSHIP BETWEEN VTS/MARITIME SECURITY

|  |  |  |
| --- | --- | --- |
| **Law enforcement organizations** | **Security Organizations** | **Other stakeholders** |
| Police – port, local, national | Port State Control | National administration (Coastal state) |
| Customs | Port authorities | Ministries |
| Border control | Ship Security Oficer (SSO)  Port Security Officer (PSO) | Ships in the area |
| Immigration | Military | Shipping companies |
| Fishery inspection |  | Pilot organizations |

Note : This list may not be comprehensive.

# SPECIFIC REMARKS

* Stakeholders involved in or responsible for ship and/or port security may also collect information that will be valuable for VTS services (INS, NAS, TOS). For example:
* existence of safety or security zones around facilities or vessels,
* the security status of vessels and port facilities,
* any security-related restrictions on vessel operations (e.g., naval vessel escort),
* coordination of vessel security checks.
* VTS may collect vessel security information from vessels as they enter the VTS area, e.g., vessel security level, last port(s) of call. This information will be of interest to security stakeholders.

# IDENTIFIED ACTIONS

It is recognised that VTS within VTM will benefit maritime security by the availability and support of relevant information, but that Security should not be considered as one of the primary tasks of VTS.

In order to achieve this benefit the following actions should be considered:

* The relationship between the VTS Authority and the appropriate security authorities and their positions in the decision making process should be determined unambiguously and defined in advance in arrangements between these stakeholders within VTM;
* Identification of security stakeholder information needs;
* Determine the use of information provided by the VTS;
* Data sharing agreements between the VTS Authority and the various stakeholders;
* Limitations on information sharing, including confidentiality, privacy are to be identified and guidelines on data security should be developed.

The identified actions should be incorporated in the ongoing task 11 of the VTS Committee in the working programme 2010-2014.

1. VTS Manual, section 0410 [↑](#footnote-ref-1)
2. VTS Manual section 0410 [↑](#footnote-ref-2)