Input paper: [[1]](#footnote-1)VTS47-3.1.10

Input paper for the following Committee(s): Purpose of paper:

**□**ARM **□**ENG **□**PAP **X** Input

**□**ENAV **X**VTS **□** Information

Agenda item 3

Technical Domain / Task Number 2.1.2

Author(s) / Submitter(s) China MSA: Jin Shengli, Xue Feng, Wang Wei, Liu Wei,

Yi Congbo.

Proposal on the Recommendation on Cyber-Security related to VTS

# summary

Considering the task of Produce a Recommendation on Cyber-Security related to VTS (VTS Task Plan 2018-2022--2.1.2) will be launched at the VTS 47 meeting, analysis on the characteristics and contents of VTS Cyber-Security are provided in this proposal, based on the practice and experience of China Maritime Safety Administration.

**1.1 Purpose of the document**

The purpose of this document is to provide input for the consideration of the VTS Committee in developing the Recommendation on Cyber-Security related to VTS (Task 2.1.2).

## Related documents

VTS46-7.1 VTS Task Plan 2018-2022

VTS46-7.2 VTS Task Register 2018-2022 20181004

# background

According to the Task Register, the expected outcome of this task is an IALA Recommendation providing guides for VTS authorities to better implement VTS Cyber-Security protection.

# discussion

## Characteristics of Cyber-Security related to VTS

1. VTS system involves the application of multi-source data such as radar, AIS, CCTV, VHF, etc. At the same time, except for the competent authorities, VTS system may link with other relevant organizations and allied services, including pilotage, port, search and rescue department, etc. As a result, VTS system has more network boundaries and data exchange interfaces, and consequently the Cyber-Security risk is much higher than other common information systems.
2. As an important data source of VTS system, radar is equipped with special industrial communication protocol, which can be used to remotely control and parameters setting. Therefore the VTS system faces the risk of data leakage and network intrusion.
3. VTS contributes to safety of life at sea, safety and efficiency of navigation and protection of the marine environment, which base on the uninterrupted operation of VTS system. Once the system is damaged, the delivery of vessel traffic services will be suspended, which causes adverse effects on the functions of VTS and, consequently, the safety of participating ships.
4. The VTS system stores a large number of ship files, voyage data, and traffic data, some of which are confidential information. In the event of information leakage, some unpredictable consequences may be caused.

## Contents to be considered in developing Recommendation on Cyber-Security related to VTS

In combination with China's VTS Cyber-Security practices, the following matters are advised to take into consideration when establishing a Recommendation on Cyber-Security related to VTS.

### Definition of Cyber-Security scope related to VTS

Generally speaking, the scope of Cyber-Security related to VTS mainly includes VTS centre, VTS sub-centre, radar stations, VHF base stations and other sensors (such as CCTV, meteorological and hydrological sensors, etc.).Servers, data storage devices, operation consoles, remote browsing terminals, AIS data source, remote maintenance interface, which process and display data, should also be included.

### VTS Cyber-Security technical protection measures

1. Physical and environmental security. It mainly includes the physical environment security of the radar station and the VHF base station room. Security systems such as monitoring, access control, and alarm should also be considered.
2. Cyber and communication security. Cyber architecture, Cyber boundary protection (firewall), access control and intrusion prevention should be considered.
3. Equipment security. Consideration should be given to identity, strong password settings, remote access control, malicious code protection, etc.
4. Application (software) and data security. Login identification, access control, software fault tolerance, resource control, software fault tolerance, important data backup and recovery should be considered.

### VTS Cyber-Security management protection measures

1. Cyber-Security management regulation

A set of operating procedures needs to be established and published in a formal and effective manner, with version control and periodic review and revision.

1. Cyber-Security related organizations and personnel

The department in charge of information security should be set up and empowered. The roles of system administrator, network administrator, security administrator and other posts should be established, combined with the clarification of corresponding responsibilities

1. Education and training on Cyber-Security awareness

Education and skills training on Cyber-Security awareness should be carried out for relevant personnel, including relevant responsibilities and disciplinary measures.

1. Security scheme design

The security plan should be designed according to the level of security protection, and the basic security measures should be defined, and implemented after verification by relevant experts.

1. Product procurement and use

The choice of service providers for various types of hard ware and software should be considered in accordance with relevant regulations.

1. Environmental management

The security management system should be established for VTS equipment room, radar stations and other places.

1. Storage media management

According to the protection requirements of different equipment, the use requirements, registration regulations and storage regulations of corresponding media (flash memory, CD, etc.) should be established.

1. Equipment maintenance management

The regulations on maintaining supporting facilities, software and hardware should be established to effectively manage the work procedure, including clarifying the responsibilities of maintenance personnel, the approval of third-party services, and the supervision and control of the maintenance process.

1. Vulnerability and risk Management

Measures should be taken to identify security vulnerabilities and hidden dangers so as to evaluate and repair them.

1. Network and system security management

Establish a network and system security management system, including account management, configuration management, log management, upgrade and patch management, password cycle update, etc.

1. Backup and recovery management

The backup procedure, frequency, media, period and recovery procedures of the backup data should be specified.

1. Cyber-Security incident response plan

The emergency plan should be designed to clarify the reporting, responding and recording process of different Cyber-Security incidents.

# ACTION REQUESTED OF THE COMMITTEE

The Committee is requested to consider the comments provided above and communicate with other Committees in progressing Task 2.1.2 --Develop Recommendation on Cyber-Security

1. Input document number, to be assigned by the Committee Secretary [↑](#footnote-ref-1)