SØFARTSSTYRELSEN

Cyber and Information Security Strategy for the Maritime Sector

2019 - 2022

Danish Maritime Cybersecurity Unit

Contents

1 Introduction

In the context of the 2018-2023 Defence Agreement, the Danish Government will reinforce Denmark's defences against cyber threats considerably and has on that basis prepared the national cyber and information security strategy. With this strategy, the Government will launch a number of initiatives aimed at improving cyber and information security activities in the critical sectors of society. The maritime sector has been designated as one of the sectors of particular importance to cyber and information security in Denmark. Consequently, it must be ensured that a clear plan is in place for the cyber and information security activities within the sector, and that is the purpose of this strategy.

Cyber and information security in the maritime sector includes the safety of navigation in Danish waters and the safety and security of Danish-flagged ships and their crews. Cyber security for ships includes services such as traffic monitoring, warnings and navigation information (AIS, NAVTEX), systems used by ships and ship operation software, including software for propulsion and navigation.

The Danish Maritime Authority's strategic aim with the sub-strategy for cyber and information security is *that security on board Danish ships and in Danish waters should not be compromised as a result of cyberattacks.* The cyber and information security challenges of the maritime sector will form an integral element of the maritime security activities of the Danish Maritime Authority and will be addressed alongside other challenges and tasks related to maintaining security on board Danish ships and the safety related to navigation in Danish waters.

The sub-strategy will complement the implementation of the EU Directive on Security of Network and Information Systems (the NIS Directive) by implementing specific initiatives. Based on the sector's vulnerabilities and the threat scenario in the maritime domain, these initiatives will contribute to greater resilience to cyberattacks and thus to improved cyber security in the maritime sector. Given the global nature of the maritime sector, it may also be necessary to establish contact to reliable international partners for sharing experience and knowledge in the field of cyber and information security.

2 Scope of application

In the Danish Cyber and Information Security Strategy, the Government has emphasised that the responsibility for cyber and information security activities in Denmark is based on the principle of sectoral responsibility: The authority responsible for a given function on a day-to-day basis is also the responsible authority when a cyber and information security incident occurs. Accordingly, the responsibility for cyber and information security in the maritime sectors lies with the Danish Maritime Authority and covers safety of navigation in Danish waters and security on board Danish ships, including systems used by ships and ship operation software, including software for propulsion and navigation, see the Danish Act on Safety at Sea. Cyber and information security in the maritime sector also covers services such as traffic monitoring, warnings and navigation information as well as other systems related to safe and secure navigation.

In this strategy the concept of information security encompasses the overall measures to secure information with regard to confidentiality, integrity (alteration of data) and accessibility. This includes organisation of security measures, influencing behaviour, data processing procedures, supply chain management and technical security measures.

For the purpose of this strategy, cyber security encompasses protection against breaches of security resulting from attacks on data or systems via a connection to an external network or system. Cyber security thus focuses on vulnerabilities inherent to the interconnection of systems, including connections to the Internet.

3 Threats, risks and vulnerabilities in the maritime sector

In order to strengthen cyber and information security in the sector, it is necessary to describe the current threat scenario it is facing. Furthermore, it is necessary to identify and describe the sector's vulnerabilities to the threats.

Below is a description of the specific threat assessment for the maritime sector based on the current threat assessments[1] made by the Centre for Cyber Security (CFCS). The threat assessments outline the threats primarily facing the maritime sector and where to consider taking preventive measures. This is done by ranking the individual threats according to the sector's vulnerability to them. The next section presents the conclusions of the risk and vulnerability analysis prepared for the Danish Maritime Authority by an external consulting firm in November 2018. The analysis provides an overview of the risks and vulnerabilities facing the maritime sector as a result of the current threat scenario and as a result of the increasing usage of automated ship systems as well as Internet and information services.

3.1 CFCS threat assessment

In its threat assessment, the CFCS concludes that

- the general cyber threat against the maritime sector is directed against commercial businesses and does not currently pose a direct threat to maritime operations;

- the threat from destructive cyberattacks against the maritime sector is low. However, maritime lines of communication, including vessels and ports, may be targets for destructive cyberattacks during times of conflict;

- the threat from cyber espionage against the maritime sector is very high, and it is assessed that states systematically use cyber espionage as a means to achieve industrial and business advantages and promote political and economic interests;

- the threat from cyber criminals against the maritime sector is very high. In particular, there is a considerable threat from cyber criminals aiming to blackmail public authorities, businesses and individuals (ransomware). Networks of cyber criminals exist that are organised and work towards long-term objectives, and cyber crimes are probably also committed by government-backed hackers;

- the threat of cyber activism against the maritime sector is low. The shipping industry does not enjoy a high degree of attention from cyber activists, and as such is not a high-profile target;

- the threat of cyber terrorism against the maritime sector is low. Terrorist groups have only shown a limited interest in the maritime sector. Also, terrorist groups lack the capabilities and resources to launch spectacular cyberattacks against the maritime sector.

3.2 Risk and vulnerability analysis of the maritime sector

The purpose of the analysis is to uncover the principal vulnerabilities faced by the maritime sector as a result of increasing usage of automated ship systems as well as Internet and information services. The analysis has identified maritime services operators, including their services, functions and systems, which are particularly critical to the maritime sector. Moreover, the analysis has identified a number of areas where a special targeted effort is required to ensure cyber and information security. The risk and vulnerability analysis was prepared in close dialogue with maritime sector players, including Danish Shipping and other public authorities.

3.2.1 General observations

The increasing IT usage in ships has led to considerable dependency on IT usage for core activities in the maritime sector. The analysis shows that the respondents are working with cyber security at different levels. Some players,

[1] "Cybertruslen mod Danmark" – May 2018, and "The Cyber threat against the maritime sector" – March 2017

including the public authorities, generally apply the ISO 27001 standard in relation to cyber security. The private-sector players take a broader approach to cyber security, seeking inspiration from recognised standards such as ISO 27001, but also from specific technologies and other security-related branches, such as physical security.

3.2.2 Identified risks

According to the analysis, the maritime sector in general considers three cyber and information security risks as particularly significant:

- Lack of timely response to technical vulnerabilities: Respondents mentioned a technology gap between the information technology (IT - e.g. administrative systems) and operational technology (OT- e.g. propulsion systems) applied in ships versus land-based IT and OT technology. Land-based systems are generally better updated than the corresponding ship-based systems. In case of insufficient focus on potential risks and threats and due to a failure to update the ship-based systems, there is a risk that the IT and OT usage in ships is more susceptible to cyberattacks.

- No process in place for upgrades: Respondents mentioned that some of the procedures applied for upgrading OT equipment do not match the guidelines applied for IT technologies. This entails a risk of failed upgrades, for instance of SCADA systems, which are applied for monitoring and control of industrial processes.

- Securing critical systems: Respondents mentioned that systems, including databases and registers based on older technology, may be particularly vulnerable to targeted attacks aimed at compromising and/or deleting critical data. The potential consequences are loss of data, lack of data integrity, loss of reputation and, not least, a potential financial loss. For example, the Danish Maritime Authority's registers of shipping represent a risk for the Danish Government in terms of ship mortgages. If such a register is destroyed or compromised, it may involve a risk of financial loss.

3.2.3 Recommendations

The analysis describes a number of strengths concerning the players' capabilities to manage and deliver cyber security. The responses showed that analogue capabilities and options are good, defined as the options for acting without the use of IT systems. The analogue capabilities and options can be applied to maintain operations and services in the event of a breakdown of IT and OT systems. Many respondents have worked intensively on cyber security and are therefore also very attentive to their own weaknesses and strengths.

The analysis recommends as follows:

- Use of technologies in the maritime sector which are resilient to cyber threats – e.g. encryption of navigation and communication infrastructure.

- Use of recognised IT security standards. Through compliance with or inspiration from standards such as ISO 27001 in relation to cyber and information security, the players can – through their selection or omission of controls in the Statement of Applicability (SoA) – implement security and control measures that are adapted to their specific risk profile. Standards are understood and perceived in the same way among international players, which makes security efforts and the understanding of IT usage across the sector transparent.

- Raised awareness of IT security among maritime sector employees. According to observations, IT awareness and training are not high-priority issues on board ships. The maritime sector already has training and routines in place for other security aspects – e.g. fire instructions. This mindset should be applied to IT usage as well.

- Communication, management and guidance on IT security should come from top management. A ship or a department should never act in isolation with respect to IT security.

- Efforts to strengthen supply chain management. Vessels are increasingly digitised, and the newest vessels are updated and maintained directly by the suppliers of the systems. However, owing to the complexity of such systems, their maintenance is increasingly outsourced. It is recommended to make specific requirements with respect to suppliers' security level and review of suppliers' quality performance.

- Cooperation on cyber security in systems, services, technologies and data applied across the critical sectors of society. Joint efforts across the sectors make good sense, but require coordination and targeted regulation to provide for a minimum security level.

4 Increased effort to strengthen cyber and information security in the maritime sector

Based on the threat assessment and the vulnerability analysis, the following measures, specified in sections 4.1.1-4.18, will be launched to strengthen cyber and information security in the sector.

4.1.1 The Danish Maritime Cybersecurity Unit

To perform the task of implementing the cyber and information security strategy for the maritime sector, the Danish Maritime Authority has established the Danish Maritime Cybersecurity Unit, which is tasked with delivering the initiatives set out in the strategy. On the basis of current threat assessments and in-depth knowledge of the maritime sector (players, services and infrastructure), the Unit will provide advice and will serve as a communication hub with respect to cyber and information security for the entire maritime sector and as an internal expert function at the Danish Maritime Authority regarding cyber and information security.

Its primary responsibilities in this connection will be to communicate, procure, create and validate IT security-related information between maritime sector players. Other responsibilities will include coordination tasks and organisation of professional workshops and conferences related to specific IT security issues in the maritime sector. An action plan will be prepared for the specific efforts, which will be implemented in close cooperation with the sector, for example in relation to skills enhancement, enforcement, regulation, supply chain management and information initiatives.

4.1.2 Implementation of EU and international law

The EU Directive on Security of Network and Information Systems (the NIS Directive) entered into force on 9 May 2018 and aims to increase security of services dependent on network and information technology. Being among the sectors mentioned in the Directive, the maritime sector must comply with the requirements provided in the Directive, including those regarding identification of operators of essential services and notification of security incidents. It follows from the NIS Directive that operators of essential maritime services in the maritime sector must notify the Danish Maritime Authority (the Danish Maritime Cybersecurity Unit) and the CFCS of incidents having had a significant impact on the continuity of the maritime services they provide.

Accordingly, at the beginning of 2019 the Danish Maritime Authority will issue an Order on security of network and information systems of importance to the security and navigation of ships, which implements the NIS Directive in Denmark in this field. The Order will lay down requirements for shipowners and ships as well as certain providers of maritime services. This means that Danish shipowners and ships using network and information systems will be required to incorporate cyber security in their risk management measures with a view to the safe and secure navigation of the ships. Furthermore, they must notify the Danish Maritime Authority and the CFCS of any incidents covered by the Order and having an impact on the security and navigation of the ships.

Large cargo ships and passenger ships are subject to the International Safety Management (ISM) Code and thus already required to address cyber security. Other ships may also have vulnerable systems, such as electronic nautical charts and communication systems, and thus also need to meet appropriate security standards. The Order therefore authorises the Danish Maritime Authority to lay down detailed requirements for such ships.

Based on the above risk and vulnerability analysis, the Danish Maritime Authority will determine which other vessel types should be subject to cyber and information security requirements. Also, ships sailing in Danish waters use various digital maritime services, which provide the ships with data or monitor their activity. This includes Vessel Traffic Service (VTS), which monitors vessel traffic in the Great Belt and Oresund, navigation information (navigation warnings) to vessels in Danish waters and information exchange systems such as AIS (Automatic Identification System). When the Order comes into force, the Danish Maritime Authority will prepare a list of operators of maritime services that are covered by the Order. This list will also be forwarded to the European Commission. At least every two years, the Danish Maritime Authority will review and update the list.

Supervision of vessels and shipowners will form part of the periodic surveys already conducted by the Danish Maritime Authority today, and going forward, the supervision will include maritime services.

4.1.2.1 International efforts by the Danish Maritime Authority:

It is important for Danish shipping and the Danish Maritime Authority that maritime sector regulation generally takes place at the international level, given the global nature of the maritime domain. Therefore, it is a fundamental Danish priority that Danish maritime regulation is in alignment with international rules and regulations, and that common global cyber security rules apply to all shipowners and vessels. This will contribute to delivering a common high, global level of cyber and information security, as this is the only way to ensure that ships sailing through Danish waters or calling at Danish ports meet reasonable cyber and information security standards. Moreover, it would be detrimental to Danish shipowners and shipping in general if Denmark or the EU were to introduce stricter or merely different requirements compared with the rest of the world, as this could distort competition.

The Danish Maritime Authority will therefore work towards making the cyber and information security framework in the maritime sector global and negotiated at the level of the UN International Maritime Organization (IMO), and towards the establishment of relevant cooperative relationships at both international and EU level so that Danish shipowners may apply the same global standards to prevent cyberattacks.

4.1.3 User-friendly recommendations to maritime sector players

The digitisation and automation of systems and processes in the maritime sector support not only the objectives of secure and efficient cargo handling, increased safety of navigation, minimisation of fuel consumption and improved customer experience in the form of flexible and user-friendly customer platforms, but also the objectives of compliance with international rules on aspects such as ship surveys, emergency response planning, environmental considerations, personal safety and carriage of dangerous goods. As mentioned in the risk and vulnerability analysis, however, increased dependence on digital solutions engenders a series of vulnerabilities, which may result in incidents that could cause breakdowns of ship management and logistics systems, bodily injury and property damage and have a negative impact on passability or communication to customers.

Specifically, the following initiatives will be launched:

The Danish Maritime Authority will formulate concrete and user-friendly recommendations to contribute to providing a sharper focus on cyber and information security in the sector. They include the following overall recommendations:

- cyber and information security requires the attention and priority of management;

- the foundations for cyber and information security work derive from a continuous focus on risk and vulnerability assessment;

- annual emergency response drills should be conducted in the individual organisations; and

- maritime operators of essential services should always have business continuity plans in place for all critical systems and business processes.

- Moreover, by applying concrete recommendations, the Danish Maritime Cybersecurity Unit must support and advise all players in the maritime sector to qualify their continued efforts to strengthen cyber and information security in the individual organisations.

The initiatives will be realised and implemented through close cooperation with, among others, Danish Shipping and through direct meetings with industry players, including shipowners and maritime equipment manufacturers.

4.1.4 IT security culture and awareness

The maritime sector has always focused intensely on safety and security issues and has therefore come a long way in its efforts to offer general safety at sea. Focus on aspects such as employee safety, transport and cargo security and not least navigational safety and maritime security has been instrumental in building the strong security culture we see in the maritime sector today. This security culture now needs to be developed to also include the cyber and information security domain, which involves people, technologies and processes in relation to cyber and information security breaches.

Management's commitment to taking the lead responsibility for cyber and information security is a visible indicator, externally as well as internally, of an organisation's maturity in the domain. Clear backing from management encourages and supports a positive security culture, which again supports an effective security and awareness programme to improve security at all levels and in all areas of the organisation. However, a strong cyber and information security culture is not created through regulations and procedures alone, but to a very high degree by people in their daily work, including the behaviour demanded and displayed. That is why a security culture is underpinned by security communications, and safety and security management is a key prerequisite for achieving a high level of awareness among the maritime sector players.

Specifically, the following initiatives will be launched:

The Danish Maritime Authority will increase the general awareness level in the maritime sector through targeted awareness campaigns rooted in industry-specific knowledge and skills. In close cooperation with the sector players, awareness campaigns will be conducted annually across the sector. That could for instance be information campaigns on GDPR compliance, but could also be more direct and focused campaigns on protection against phishing mails or instructions in how to achieve maximum mobile security.

4.1.5 Focus on standardised processes in relation to cyber and information security management

It is today mandatory for all Danish central government authorities to apply the ISO 27001 standard, which is a recognised and widely used international security standard that describes best practice for an information security management system. The ISO 27001 standard could usefully be supplemented with the cyber-security framework tool provided by the National Institute of Standards and Technology (NIST). While the ISO 27001 standard is typically used in Europe, NIST's framework tool is often used in a more global context. Although the two standards naturally overlap quite a bit, they feature different strengths. The ISO 27001 standard focuses primarily on management and processes,

whereas NIST has a stronger focus on technical security measures. In this fashion, the two standards are mutually complementary.

By using recognised IT security standards, the maritime sector can achieve effective IT security management that suits its specific needs and ensure that this effectiveness is maintained through a standardised process for ongoing improvement. This means that IT security is regularly updated to enable the maritime sector to tackle the challenges of a digital world that is in a state of constant change and under constant attack.

Specifically, the following initiatives will be launched:

- Work on cyber and information security management in the maritime sector needs to be strengthened by directing the focus on standardised processes in relation to cyber and information security management, including the use of recognised IT security standards that set standards for the establishment, implementation, maintenance and ongoing improvement of an IT security management system.

- It is necessary to facilitate a risk-managed process to ensure and maintain the confidentiality, integrity and accessibility of information so as to achieve the best possible protection of information from unauthorised disclosure or access.

4.1.6 Ensuring a consistent and robust cyber and information security emergency response in the maritime sector

"It is not a question of whether an organisation will be affected by an IT security incident, but a question of when. Perhaps the organisation has already been affected without knowing it." No matter how well an organisation protects itself, an IT security incident is bound to occur sooner or later. It could for instance be an unintended breakdown of an administration system, an infringement of the Danish Act on Processing of Personal Data or an external cyberattack completely paralysing Denmark's production facilities. When an IT security incident occurs – in whatever form it materialises – it is important to be able to roll out full-scale systems to gain an overview and to have established and tested appropriate emergency response procedures that are capable of handling the IT security incident to which the organisation is exposed.

IT emergency management or Business Continuity Management offers tools for ensuring the continued operation of an organisation whose production facilities are affected by an IT security incident, including its business-critical processes, systems and products. This is also referred to as Respond & Recover and is designed to ensure that the organisation's IT support can be sufficiently restored within a desired period, depending on when the performance of tasks and responsibilities is threatened to an extent where the consequences are unacceptable.

Specifically, the following initiative will be launched:

A consistent and robust cyber and information security emergency response in the maritime sector is obtained through the Danish Maritime Authority's practice of providing general advice to the sector about IT emergency management, including the importance of emergency response planning to ensure that the plans for instance include serious IT security incidents that completely paralyse all forms of IT systems and to ensure that all employees involved know their functions and are able to perform them.

4.1.7 Exchange point between maritime sector players and the CFCS

The Danish Maritime Authority will serve as an exchange point between the maritime sector players and the CFCS. Its primary responsibilities in this connection will be to communicate, procure, create and validate IT security-related information between the parties. Other responsibilities will include coordination tasks and organising professional workshops and conferences related to specific IT security issues in the maritime sector.

Given the global nature of the maritime sector, it may be necessary to establish contact to reliable international partners for sharing experience and knowledge in the field of IT security. The United States is one of the countries that have indicated an interest in acquiring knowledge of the Danish Government's cyber and information security strategy, and it would therefore be appropriate to stimulate global coordination with key players in the domain.

Specifically, the following initiatives will be launched:

The Danish Maritime Authority aims:

- to be able, in close cooperation with the CFCS, to analyse and provide information about the threat scenarios facing the maritime sector, making it possible to respond quickly and effectively to cyber threats;

- to contribute to preparing threat assessments in cooperation with the threat assessment unit of the CFCS;

- to be responsible for maintaining regular contact (gateway) to the relevant players in the maritime sector and contribute to ensuring that knowledge provides direct support to cyber security work in the security organisations of the authorities and businesses operating within the sector; and

- to contribute to intensifying the global focus and cooperation on maritime cyber security.

4.1.8 Inpatriation of maritime employees to the CFCS

A maritime employee will be inpatriated to work at the CFCS. The purpose is to ensure and promote that the CFCS has the necessary knowledge about the maritime domain and possesses the skills and competencies on which the Danish Maritime Authority and the maritime sector can capitalise in its work to ensure a high level of cyber and information security.

4.2 Maritime Cyber and Information Security Forum

To facilitate exchange of experience and knowledge sharing across the maritime sector, the Maritime Cyber and Information Security Forum will be established.

The forum will consist of IT security representatives from Danish authorities who are involved directly in maritime activities. The Danish Maritime Authority will undertake the duties of coordinator and secretary in the Maritime Cyber and Information Security Forum, and members are expected to be able to share experience with each other in relation to specific IT security measures. The forum may serve as a platform for discussing how various security incidents have been handled by the parties involved, enabling all members of the forum to benefit from the experience they have gained in the given situations.

The primary objectives of the forum are:

- to be responsible for coordinating the handling of cyber and information security across the maritime sector; and

- through knowledge sharing, to identify and map out areas where joint initiatives can be launched to strengthen cyber and information security in the maritime sector.

The Maritime Cyber and Information Security Forum is going to implement a range of initiatives over the life of the strategy. These initiatives are described in more detail in sections 4.2.1.-4.2.3.

4.2.1 Increased awareness level through cooperation and knowledge sharing in the maritime sector

Knowledge sharing in the maritime sector is centred on efforts to cooperate across disciplines and utilise the cyber and information security knowledge that is already available with the individual authorities within the maritime sector. This must be achieved by ensuring that players who need knowledge have access to knowledge.

The responsibilities of the Maritime Cyber and Information Security Forum are:

- through meetings and workshops, to ensure cooperation and knowledge sharing on cyber and information security across the maritime sector players;

- through knowledge sharing, to identify whether special challenges cutting across the boundaries of responsibilities have emerged and whether such challenges may/must be met by joint action in relation to cyber and information security; and

- to identify any interfaces with existing cyber and information security forums, at both the national and international level.

4.2.2 Joint emergency response and early warning plan for handling IT security incidents

Knowledge sharing on cyber and information security is also a matter of emergency response planning and early warning, including efforts to convey the relevant knowledge faster to everyone. For instance, when an authority recognises that it has become the victim of a phishing attack, this knowledge needs to be shared and disseminated as soon as possible, thereby allowing other authorities to use the knowledge right away. The responsibilities of the Maritime Cyber and Information Security Forum are:

- to establish a joint emergency response plan for handling IT security incidents and for giving early warning to other relevant authorities in the event of emergency response plan activation;

- in the longer term, to identify and address the needs and possibilities for developing a digital hub/communications platform where cyber and information security knowledge is made easily accessible to, and searchable by, the authorities and stakeholders of the maritime sector.

4.2.3 Planning and implementation of joint cyber and information security drills

Cyber and information security drills should be a central part of all authorities' cyber emergency planning. The purpose of these drills is to test and develop the employees, plans, procedures and technologies of the authorities as well as their cooperative relations. All maritime sector authorities should therefore, by default, plan and organise regular and varied drills to prepare for the handling of relevant and current cyber threats. The best way to accomplish this is to ensure that the authorities both organise their own internal drills and participate in cross-cutting drills with a focus on cooperation.

The responsibilities of the Maritime Cyber and Information Security Forum are:

- to draw up emergency response plans to respond to relevant and current cyber threats; and

- to coordinate joint cyber and information security drills. The forum will for instance conduct cross-cutting emergency response drills involving training in scenarios where several players from across the maritime sector are affected by simultaneous cyber and information security incidents.

5 Conclusion

The cyber and information security challenges of the maritime sector will form an integral element of the maritime security activities of the Danish Maritime Authority and will be addressed alongside other challenges and tasks related to maintaining security on board Danish ships and the safety related to navigation in Danish waters. The Danish Maritime Authority's strategic aim with the sub-strategy for cyber and information security is that:

security on board Danish ships and in Danish waters should not be compromised as a result of cyberattacks.

The Danish Maritime Authority's work to contribute to cyber and information security in the maritime sector will be included as an integral part of the general security work carried out by the Authority, including enforcement of existing requirements and regulations, in relation to the prevention and handling of incidents.

The sub-strategy complements the implementation of the NIS Directive by implementing specific initiatives. Based on the sector's vulnerabilities and current maturity, these initiatives will contribute to greater resilience to cyberattacks and, accordingly, to improved cyber security in the maritime sector.

Established in mid-2018, the Danish Maritime Cybersecurity Unit will, among other functions, serve as an exchange point between the maritime sector players and the CFCS. Its primary responsibilities in this connection will be to advise, communicate, procure, create and validate IT security-related information between maritime sector players. Other responsibilities will include training, coordination tasks and organisation of professional workshops and conferences related to specific IT security issues in the maritime sector.

5.1 Time frame

The time frame for the strategic objectives and initiatives pursued in relation to the strategy for the maritime sector's cyber and information security:

Short term (2019)

Section 4.1.1: Establishment of the Danish Maritime Cybersecurity Unit (June 2018)

Section 4.1.2: EU and international law

Section 4.1.7: Exchange point between maritime sector players and the CFCS

Section 4.1.8: Inpatriation of maritime employees to the CFCS

Section 4.2.1: Increased awareness level through cooperation and knowledge sharing in the maritime sector

Medium term (2020 – 2021)

Section 4.1.3: Specific objectives and user-friendly recommendations to maritime sector players

Section 4.1.4: IT security culture and awareness

Section 4.1.5: Focus on standardised processes in relation to cyber and information security management

Section 4.1.6: Ensuring a consistent and robust cyber and information security emergency response in the maritime sector

Section 4.2.2: Joint emergency response and early warning plan for handling IT security incidents

Section 4.2.3: Planning and implementation of joint cyber and information security drills

Long term (2022)

Identify and address the needs and possibilities for developing a digital hub/communications platform where cyber and information security knowledge is made easily accessible to, and searchable by, the authorities and stakeholders of the maritime sector.