EXPLANATORY NOTES

GENERAL

1. Introduction

The purpose of this Regulation is to implement the bases and sub-bases of delegation in the Merchant Shipping Protection Act (WtBK) and the Merchant Shipping Protection Decree (Bbk). In accordance with Instruction 2.24 of the Drafting Instructions, this Regulation fleshes out the provisions of the Act and the Decree, including rules of an administrative and technical nature.

The content of the Regulation is therefore important to maritime security organisations, ship managers, masters and maritime security personnel, but also to the government bodies charged with implementation, such as the Coast Guard and the Human Environment and Transport Inspectorate (ILT). The Regulation contains a number of annexes with model forms. These model forms not only streamline the work processes of the Coast Guard and the ILT, but will be particularly useful in the implementation practice of shipowners, masters and maritime security organisations. Because of the international nature of the Dutch merchant shipping industry, the model forms are also provided in English.

Similarly, it is noted that various forms are already available in existing practice, for example for incident reports. The aim of creating model forms is to maximise alignment with existing practices.

It should be noted that the purpose of the Regulation is not to codify existing practices in piracy incidents. Existing practices and procedures for piracy incidents are unchanged. Nor does the Regulation deal with applications for military protection, as this is an existing work process that is not affected by the WtBK and its underlying regulations. The reason for the Act and regulations, including this Regulation, is to introduce the possibility of Dutch-flagged merchant ships being protected by armed private security guards. Supplementary to the Act and the Decree, this Regulation provides what is necessary for that purpose. For a further explanation of the Act and the Decree, please refer to the relevant explanatory notes.

2. Legislative framework

As indicated above, the WtBK and the Bbk contain a range of grounds for regulating the subjects in this Regulation.

Based directly on the Act, rules have been set by ministerial regulations concerning the reasonable protective measures to be applied by the ship manager and the master (Section 6 of the Act), reporting by the master and the team leader to the ILT (Section 12 of the Act), the fee for a permit (Section 13(5) of the Act) and the amounts of the administrative fines that may be imposed pursuant to the Act for breaches of the Act and regulations (Section 17 of the Act).

The other topics covered in the Regulation are indirectly based on the Act, via the Bbk.

A number of specific subjects may be regulated by ministerial decree. These are further rules with regard to:

- The data and documents that the master and team leader must prepare prior to the boarding of the security team (Article 2.4(5) Bbk);
- Reasonably guaranteeing the continuity of the maritime security company (Article 5.4(3) Bbk); and
- The secure storage, management and transport of firearms and ammunition (Article 5.10(3) Bbk).

3. Granting permission

The Coast Guard Centre will handle requests from ship managers for permission to use armed private security, and applications for security from the Ministry of Defence in the form of a Vessel

Protection Detachment (VPD). In the case of an application for private security, an assessment will also be performed to determine whether the transport should be eligible for VPD security. This will include an examination of whether it is indeed a merchant ship that is entitled under Dutch law to fly the flag of the Netherlands, whether it is indeed a transport through the designated high-risk area, whether a risk analysis is attached, and whether the reasonable protective measures to be taken by the ship manager and the master will be complied with. If the application does not provide sufficient clarity on these matters, the Coast Guard will request additional information. As a last resort, the Coast Guard may refuse permission to use armed private security if no risk analysis has been performed or if there is a valid expectation that not all reasonable protective measures will be taken.

There will then be an examination of whether, given the size of the ship, a VPD could be offered, and whether a VPD can be mobilised in time. If the answer to those questions is negative, permission may be granted for armed private security to be provided by a maritime security company that holds a Dutch permit. If the answer to the latter questions is in the affirmative, and military protection is possible in principle, an assessment will be carried out as to whether, in that case, a disproportionate detour (of more than 100 nautical miles) would have to be made, or whether disproportionate additional costs would be associated with the deployment of a VPD. If not, military protection will be offered. If this is the case, the transport will be eligible for armed private security provided by a maritime security company that holds a Dutch permit. Article 2 contains a reference to the application form to be used when requesting permission.

Annex 1 contains a model form for requests for permission. Interested parties (usually the applicant) may lodge an objection with the Coast Guard regarding the decision to grant (or refuse) permission.

A legal condition of eligibility for private security is that the ship manager and the master must also take protective measures, as set out in Article 3, to prevent the ship from being attacked by pirates. After all, having armed private security on board is not an alternative to taking security measures; it is merely a supplementary course of action that may be dictated by the risk analysis. For a more detailed explanation, please refer to the explanatory notes for the individual articles.

4. Granting permits

The regulation lays down detailed rules regarding applying for a permit to provide and perform maritime security work and various specific permit conditions. Pursuant to Article 4.2 of the Merchant Shipping Protection Decree, permit applications must be submitted to the Human Environment and Transport Inspectorate (ILT). The Merchant Shipping Protection Decree provides the basis for setting further rules (permit conditions) regarding the reliability of the maritime security company, the continuity of the company, the company's operations and internal monitoring. Pursuant to Section 13(4) of the Act, the Regulation also sets the prices (fees) for processing permit applications. The various requirements are discussed in more detail in the explanatory notes for Article 9 ff. Annex 7 to this Regulation contains a model form for permit applications. That form will be made available on the Coast Guard website.

5. Supervision and enforcement

Section 16 of the Act provides that the Minister may issue a separate decree designating the officials charged with supervising compliance with the rules set out in or pursuant to the Act. To that end, the Minister has designated officials from the Human Environment and Transport Inspectorate (ILT). The supervisory officials have the usual powers pursuant to the General Administrative Law Act. Section 17 of the Act provides that administrative fines may be imposed in the context of supervision and enforcement. The Regulation contains more details regarding the framework around the power to impose administrative fines. In practice, such fines will be imposed by supervisory officials from the ILT. The ILT will use a catalogue of fines setting out the exact amount of the administrative fine applicable to each breach.

For the sake of completeness, it is noted that the Act also provides for criminal enforcement of a number of provisions. This pertains in particular to the authorised use of force by maritime security personnel. The master will submit reports on the use of force (legitimate or otherwise) to the Public Prosecution Service. Article 6(3) of the Regulation contains a reference to the model

form for reporting the use of weapons. The Public Prosecution Service will investigate, in collaboration with the police, whether the use of weapons occurred in a lawful manner. If the private maritime security guards do not act in accordance with the provisions of the Merchant Shipping Protection Act, they may breach the Weapons and Ammunition Act, which is a criminal offence.

6. Data protection impact assessment

As indicated in Paragraph 5 of the Explanatory Memorandum to the Merchant Shipping Protection Decree, the implementation of the Act will result in personal data being processed by permit applicants, permit holders (maritime security companies) and the various government organisations charged with implementation of laws and regulations. The data protection impact assessment carried out when the Act was being drafted led to the inclusion of additional legal grounds for the processing (and protection) of personal data. This assessment was also taken into account during drafting of the Merchant Shipping Protection Decree.

In response to comments from the Dutch Data Protection Authority and the Advisory Division of the Council of State the relevant provisions, or their explanatory notes, were made more precise. For a more detailed explanation, please refer to the further report[1] and the relevant explanatory notes for the Act[2] and the draft decree[3].

After receiving the response from the Advisory Division of the Council of State, Article 24 of the Regulation was amended to provide further safeguards around the processing of personal data, in addition to retention periods. The article states that the supervisory officials of the Human Environment and Transport Inspectorate must indicate in their privacy statement how they will provide certain safeguards in connection with the processing of personal data. The privacy statement must be posted on the Inspectorate website.

7. Regulatory burden and financial consequences of the WtBK and associated regulations (private parties)

During the drafting of the Merchant Shipping Protection Decree and the Merchant Shipping Protection (Amendment) Act, the impact of the Act and the Decree on the regulatory burden was analysed, along with the financial consequences.[4] The Merchant Shipping Protection Regulation elaborates on or clarifies the provisions of the Act and the Decree. The Regulation is based on the Act and the Decree; as such, it does not contain any new elements that could lead to an additional regulatory burden. However, the original assumptions have been examined to determine whether they are in line with current insights and are still tenable. The current insights have not given rise to any adjustment of the original assumptions.

8. Workload impact and financial consequences of the WtBK and associated regulations (government)

The above statements with regard to the regulatory burden and financial consequences for private parties also broadly apply to the workload impact and financial consequences for the government organisations involved.

However, the Coast Guard was asked for an impact analysis and the ILT was asked to perform an additional assessment of enforceability, feasibility and financial consequences. Based on the Coast Guard's impact analysis, an additional €31,000 was allocated to the Coast Guard for costs related to preparation for the work, including the recruitment of a planning coordinator. Although the Director of the Coast Guard indicates that the funding for a 0.5 FTE (Scale 10) position is tight, for the time being it is assumed that it will be sufficient for the handling of the anticipated hundred or so applications for permission. Incidentally, a trial was conducted in September with a number of

[1] Parliamentary Papers II, 35 811, No. 4.

[2] Parliamentary Papers II, 35 811, No. 3, pp. 9–10.

[3] Explanatory notes on the draft Merchant Shipping Protection Decree, pp. 19–20.

[4] For a detailed explanation, see Paragraph 6 of the Explanatory Memorandum to the draft Merchant Shipping Protection Decree.

fictitious applications for permission from ship managers, allowing the Coast Guard to test its intended work process.

The original EFF test performed by the ILT was based on outdated principles in the Act regarding the role and responsibilities of the ISO certification institutions. Accordingly, the ILT was asked to perform an additional EFF test. This test provided further insight into the funding required for supervision and enforcement. The test was also important for determining the administrative fees that will be charged for permit applications. The basic principle is that the fees should cover the costs incurred by the ILT in granting a permit. For a further explanation, please refer to the explanatory notes for Article 8.

With regard to criminal enforcement of the Act and associated regulations, the Public Prosecution Service (and, by extension, the police) first want to gain practical experience with the Act, before working out what the staffing, organisational and financial consequences will be. For now, it is expected that current capacity will be sufficient for investigating reports on the use of weapons by private maritime security guards. As such, the provisions of the Regulation, and specifically the model forms to be used, have no consequences for the workload of the Public Prosecution Service or the police.

9. Notification procedure

TBA

10. Online consultation

The draft regulation is open to responses from online consultation from TBA to TBA.

INDIVIDUAL ARTICLES

Article 1

Article 1 defines a number of terms used in the Regulation. These terms supplement the terms used in the Act and the Decree.

Article 2

Article 2 provides that a separate form must be used to request permission for armed private security on board ships. This standard form, included in Annex 1, facilitates both the submission of applications by ship managers and the processing of the applications by the Coast Guard.

Article 3

Section 6(1) of the Act provides that the master and the ship manager must apply all reasonable security measures prior to and during a transport on which maritime security personnel are deployed. The Act states that these reasonable protective measures will be set out in a ministerial regulation. This article provides more details about these reasonable protective measures. The use of armed private security guards is not a substitute for taking measures; security guards are merely supplementary to such measures. When an application for permission is made the Coast Guard checks whether the required measures will be met, based on the submitted form. If the application does not provide sufficient clarity, the Coast Guard will request additional information. As a last resort, the Coast Guard may refuse permission to use private maritime security if it believes that all reasonable protective measures will not be taken (Art. 2.2(5) Bbk).

The measures are derived from the most recent version of the internationally applied Best Management Practices (BMP5). The prescribed reasonable measures that must be taken do not replace the recommendations of the BMP5; instead, they ensure that a minimum level of protection measures is taken. As such, the measures are not new within the sector. In principle, the measures listed are all reasonable protective measures that apply regardless of the type and size of the ship. Nevertheless, there are ships on which not all of these basic measures can be taken. The application for permission may provide justification for why certain measures cannot be applied.

Article 3(1), and 3(2) and (3), distinguish between the measures to be taken by the ship manager and the master respectively.

The ship manager is responsible for creating the preconditions for practical protective measures to be put in place under the authority of the master. The ship manager must also list the guarantees to be taken in the security management system (SMS) of the ship manager.

In practice, the measures taken by the master will be translated into the ship security plan (SSP).

Naturally, the ship manager and the master are free to take additional measures if they so desire.

Article 3(1)(e) and 3(2)(f)

Materials that enable windows and portholes to be strengthened include bars and cover plates. These may offer protection against projectiles, but can also prevent intrusion by third parties.

Article 3(2)(a)

Article 3(2)(a) concerns the availability of a safe room or safe muster point for seafarers and any passengers on board. Based on the risk assessment and planning procedure followed by the ship manager, a safe room and/or safe muster point must be designated on the ship. A safe muster point is a designated zone on a ship offering maximum physical protection to the crew. It is designated during the planning procedure. If the threat assessment identifies risks that may result in damage to the hull at or below the waterline, a muster point above the waterline will be designated. On many ships, the central stairwell is a safe place because it is protected by the crew quarters and is located above the waterline. A safe room is a place where everyone present may seek protection if pirates threaten to enter the ship. Safe rooms are designed and built to prevent violent access. The preference is for a so-called "citadel", where, if the need arises, people can safely hide while continuing to communicate with the outside world, for example via VHF or INMARSAT, and can also retain control of the ship. Control of the ship's propulsion and steering systems may provide effective protection during an attack. A simple VHF connection to an antenna through the funnel to the outside or a ship phone that can receive INMARSAT calls via the ship's switchboard may be sufficient to make an emergency call where necessary. No possibility of communication with the shore or nearby ships means that no rescue action can be initiated, for example by military vessels. The use of a safe room is in addition to, not instead of, all other measures to protect the ship. Use of the safe room must be practised and the ship safety plan must specify the conditions and supporting logistics for its use.

Article 3(2)(c)

The use of water and/or foam sprayers, which are already required to be present, is effective for preventing or delaying attempts to board the ship unlawfully. The use of water may make it difficult for an attacking boat to stay alongside and makes it considerably more difficult to climb on board. It is important to attach water hoses and sprayers near potential boarding points and preferably make them able to be controlled remotely, since manual activation could put the operator at risk. The reach of the water can be increased by using fire hoses in the high-pressure position and installing splash plates a short distance from the front of the nozzle. Water cannons allow water to be sprayed in a vertical arc and may be used to protect a larger part of the hull. Water spray rails with spray heads produce a water curtain over larger surface areas. In terms of foam sprayers, it is noted that these may be used to protect against piracy in addition to the ship's standard fire-fighting equipment. Foam has a disorienting effect and makes the deck slippery. Training, observation and drills are required to ensure that the equipment can be used effectively at the ship's vulnerable points.

Article 3(2)(g)

It goes without saying that attackers should be prevented from boarding the ship in the first place. In exceptional situations where pirates do manage to get on board, it is important that no equipment or materials on deck fall into the hands of unauthorised persons, since they could be stolen or used to penetrate further into the ship. In accordance with the BMP5 measures, such items should be stored below decks before entering a high-risk area.

Article 3(2)(h)

The ship registration area of the Maritime Security Centre – Horn of Africa (MSCHOA) is intended to keep military forces combating piracy informed about merchant ships passing through the Indian Ocean and the Gulf of Aden. The United Kingdom Maritime Trade Operations (UKMTO) voluntary reporting area is indicated on nautical charts with security information such as Map Q6099 from the United Kingdom Hydrographic Office (UKHO). Ships entering the voluntary reporting area are advised to register with United Kingdom Maritime Trade Operations (UKMTO). Registration enables direct contact between the reporting ship and United Kingdom Maritime Trade Operations (UKMTO). In practice, the UKMTO is always informed. This practice was assumed when the UKMTO was mentioned in this provision.

Article 3(3)(a)

Effective lookout posts are the most efficient way to protect the ship. Lookout posts can spot suspicious approaching vessels and attacks at an early stage, so that defensive means can be deployed. The objective is to consider which places on the ship are best suited to serve as a lookout post. It does not mean, of course, that structural adjustments must be made in order to set up lookout posts.

Incidentally, it was decided not to mandate the installation of a CCTV system. Not all ships are already fitted with such a system, and where cameras are present, they are usually aimed at vital onboard equipment; in most cases, their purpose is not to provide a view of the activities of intruders on board ships. There was consideration of whether ship managers should be required to install overview cameras, with a central server where footage from the ship and the security guards could be consolidated and synchronised. However, such provisions are not yet included in the usual Best Management Practices. Ship managers are of course free to install such systems of their own accord. For the time being, the obligation for maritime security guards to generate video recordings in the event of incidents by means of helmet cameras is sufficient.

Article 3(4)

There may be special circumstances in which it is not possible to take one or more of the measures described in Article 3(1) to (3). This may be due, for example, to the specific size of the ship or to exceptional circumstances on board. In such cases, the ship manager will give reasons on the permission application form why the measure(s) concerned cannot be taken on the intended transport. If applicable, the ship manager may also indicate to what extent alternative protective measures will be taken.

Article 4

This article lays down further rules with regard to the weapons locker on board the ship. The weapons locker is the locked storage place on board the ship where weapons and ammunition are stored in their transport case(s). For the sake of clarity, the weapons locker is distinguished from transport cases.
The weapons locker is accessible only by the master or an official with instructions from the master. It goes without saying that a weapons case or transport case containing weapons and ammunition should be opened only by the leader of the security team (and not by the master). However, the master must record on the embarkation form the number, make and type of weapons. In addition, the weapons present are recorded on a daily basis. This daily weapons count is performed by the team leader. The master must always sign the record.

Two hours before the ship reaches the high-risk area, control of the master's weapons locker keys is transferred to the team leader. According to standard practice in the maritime security sector, the transport cases are then brought to the bridge. Any weapons not being used during the passage through the high-risk area are stored in a transport case on the bridge. Transport cases are not locked during the passage and are supervised by the armed member of the security team on duty on the bridge. The security guard on duty on the bridge carries his or her own weapon at all times. This is in line with usual practice and instructions in the maritime security industry.
No more than two hours after leaving the high-risk area, the weapon transport cases are returned to the weapons locker.

The permit holder must draw up a set of instructions concerning the operation and maintenance of firearms. The team leader will supervise the implementation of these instructions pursuant to Article 4(10).

Article 5

Video and audio recordings will be made from the time the imminent threat of piracy arises until the threat has been avoided or averted (Section 11(2) WtBK). Article 5 of the Regulation contains a number of requirements with regard to the cameras to be used. The article is based on Section 11(5) of the Act and Article 5.13(2) of the Decree.

Article 5(1) makes it clear beyond doubt that every individual member of the security team must wear a camera. The camera must be worn on the helmet. As security guards are expected to use semi-automatic firearms in special circumstances, using a helmet camera seems the most appropriate option. Using a bodycam makes it difficult to create usable footage if a semi-automatic firearm is to be fired at the same time.

Article 5(2) sets out the other functional and technical requirements for the cameras and microphone. Article 16(1) of the Regulation emphasises that the team leader must ensure the proper use and functioning of the camera and microphone.

Article 6

Article 6 is based on Section 12(1) and (3) of the Act and on Article 2.4(5) of the Decree and makes reference to Annexes 2 to 6 of the Regulation.

Article 6(1) provides that the master will receive the required information from the ship manager at least four hours before the embarkation of the security team, weapons, cameras and microphones. This time is intended to give the master sufficient opportunity to absorb the information and prepare for the embarkation of the security team.

Article 6(2) refers to the model embarkation form in Annexes 2 and 3 for recording information concerning, among other things, the security measures taken or to be taken on board, the size and composition of the security team, the weapons, and copies of relevant documents. If the security team boards the ship first and the weapons arrive later, the embarkation forms will be completed in two stages. In practice, a copy of the crew list may also be attached with the required information about the members of the security team.

After the transport, the completed embarkation form must be sent to the ILT as part of the final report. If other forms submitted by the master or team leader already contain the necessary information, they may of course be attached to the prescribed embarkation form, without the relevant parts of the embarkation form having to be filled in separately.

Article 6(3) contains a reference to the reporting forms to be submitted by the master and team leader, set out in Annexes 4 and 5.

To report the use of weapons, the master will use the model form in Annex 6.

Article 7

Article 7 is based on Section 13(6) of the Act. It provides that rules must be set in or pursuant to a general order in council regarding the application, duration, transfer and renewal of permits and the conditions that may be attached to a permit.

Article 7(1) provides that the model form in Annex 7 should be used to submit a permit application. This provides clarity to applicants about the information required and the documents involved in assessing a permit application.

Article 7(2) states that as part of the permit application procedure, the ILT checks that the supporting documents listed in Articles 9 to 15 are present. Article 7(2) enables the ILT, for

efficiency reasons, to perform an initial assessment of the most essential aspects, then request or inspect additional documents once that stage has been completed.

Article 7(3) makes it clear beyond doubt that the Inspectorate may perform an audit at the company's premises before a decision is made about a permit application.

Article 7(4) states that the ILT may formulate specific conditions with which the permit holder must comply. These may include conditions relating to smooth interactions and good communication with public authorities, such as the Coast Guard or the ILT.

Article 8

Section 13(5) of the Merchant Shipping Protection Act provides that, in accordance with the rules to be issued by the Minister, the applicant must pay a fee for the processing of an application for a permit to offer and provide maritime security services. Article 8 of the Regulation sets the amount of the fees.

The basic principle for the legislature was that fees should be set on a cost recovery basis, i.e. they are intended to cover the costs incurred by the ILT in processing a permit application. The fee is therefore payable even if a permit application is ultimately rejected. Similarly, the fee is payable in cases where a permit application has been rejected and a new application is later submitted. Naturally, an objection may be made to the refusal to issue a permit.

The amount of the fee is based on the costs incurred by the ILT in the permit-issuing process and the number of permit applications expected each year. To that end, the ILT has performed calculations as part of its enforceability, feasibility and fraud resistance test. The proposed fee is based on the assumption that around six permit applications will be processed by the ILT in the first three years.

Article 9

Article 9 is based on Section 13(6) of the Act as well as Article 5.4(1) and (2) of the Merchant Shipping Protection Decree. It contains further details on the required continuity of the company. The continuity of the maritime security company is deemed to be reasonably guaranteed if the company has a number of relevant documents. These include an extract from the Trade Register, adequate liability insurance, an up-to-date auditor's statement showing that the company is not bankrupt, no suspension of payments has been granted and no seizure order has been executed with respect to a substantial share of the assets, and an overview of key suppliers. This overview provides insight into the company's dependence on specific suppliers and its vulnerability in the event of the temporary or permanent loss of a supplier.

Article 9(2) imposes further requirements with regard to liability insurance.

Article 10

Article 10 provides further details on the requirement concerning the reliability of the company. This article is based on Section 13(6) of the Act, as well as on Article 5.5 of the Decree. Reliability is deemed to be assured if, in view of the plans and history of the company and of the people who set its policies, there is a reasonable expectation that the company will comply with the rules laid down in or pursuant to the Act, the people who set or help to set the policies hold a Certificate of Good Conduct (VOG) or an extract from court records issued within three months of the submission of the permit application and are not subject to a guardianship order, the company and the people who set its policies are not affiliated with any national government, the company supports the principles of the International Code of Conduct Association, and the company acts in accordance with the generally accepted standards for a good security organisation. The International Code of Conduct Association (ICoCA) was established in 2013 to ensure that private providers of security services respect human rights and humanitarian law. It serves as the governance and supervisory mechanism of the International Code of Conduct for Private Security Service Providers.

Article 10(2) provides that if the registered office, administrative headquarters or principal place of business of the maritime security company is not in the Netherlands, any permit or recognition from the competent authorities of the country where the company has its registered office, administrative headquarters or principal place of business will be taken into account when assessing the reliability of the company and of the persons who set or help to set its policies.
For the sake of completeness, it is noted that in addition to the requirements in Article 10, the establishment requirement is imposed in connection with the company's required reliability. However, this requirement is not included in Article 10, as it is already provided for in Article 5.3(2) of the Decree. In short, it means that if the principal place of business or registered office of the maritime security company is not in the EU or EEA, the maritime security activities must be organised from a branch office in the Netherlands that is registered in the Dutch Trade Register. This applies even if the company already has a branch office in another country within the EU or EEA.

Article 11 (Art. 5.6 Bbk)

Article 5.6 of the Decree sets requirements for the operations of the maritime security company. The operations must be set up in such a way as to ensure that the armed maritime security activities are organised in a responsible, reliable and verifiable manner, and to allow for monitoring of compliance with the rules and regulations laid down in or pursuant to the Act and their enforcement. Article 11 provides further details of the requirements imposed on the operational setup. This includes personnel records, such as records of the private maritime security guards to be deployed, with evidence of their reliability and professional competence, the training they have received, their medical fitness and their command of the English language. In addition, the maritime security company must have relevant policy documents, work instructions and overviews in order to qualify for a permit under the WtBK.

Article 12

Article 5.7 of the Decree sets requirements for the internal monitoring of the maritime security company. Article 5.7(2) states that the internal monitoring system must include safeguards for the separation of the functions of management and internal monitoring and for the functional independence of the internal compliance officers. These requirements are fleshed out in more detail in Article 12 of the Regulation. The internal monitoring system requires evidence of a quality policy, a policy on the process of continuous improvement, management reviews, an auditing system, a policy on incident reporting and the handling of incidents, and document checks. This evidence may consist of relevant policy documents or management reports, for example.

Article 13

Article 13 provides that when applying for a permit, the maritime security company must submit evidence of reliability, medical fitness, professional competence and training to the Inspectorate. The Inspectorate will keep a record of the maritime security guards deployed by the permit holder. Of course, this does not mean that no new security guards may be hired and deployed after the permit is issued. However, the Inspectorate must receive the evidence listed above with respect to the guards concerned before they can be deployed (Article 13(2) of the Regulation).

Article 14

This article concerns the reliability requirement for the maritime security guards. This reliability requirement is also one of the conditions for obtaining a permit to offer and provide maritime security services (Section 13(4) and (6) of the Act in conjunction with Article 5.9(1) and (3) of the Decree). To demonstrate the reliability of the maritime security guards to be deployed (both those employed by the company and those engaged via a temporary employment company), the permit application requires that the security guards hold a Certificate of Good Conduct (VOG) issued within the past twelve months.
In the case of security personnel who are residents of a country other than the Netherlands, an extract from court records (criminal records) issued within the past twelve months by the authorities of the country of residence must be submitted, along with a certified, authenticated translation. In maritime security practice, such documents are often already written in English.

The twelve-month period takes account of the fact that the people involved are often at sea for months at a time, and therefore do not always have the opportunity to request such documents from the relevant authorities within a short timeframe.

Article 15

Article 15 provides further details on the requirement concerning medical fitness. To be able to carry out maritime security activities, a medical certificate is required to show that the person concerned is physically and mentally capable of performing the required work at sea. Such a medical certificate is already a requirement for all seafarers. An example of a foreign equivalent is the British ENG1 certificate. The members of the security team must at all times hold a medical certificate declaring their fitness to perform maritime security activities. The certificate must be issued by an independent medical examiner. The examination requirements are broadly in line with the usual examination requirements for seafarers. Under the SOLAS Convention and the Maritime Labour Convention (2006), seafarers must hold a Medical Certificate for Services at Sea (ENG1). This maritime medical examination is mandatory for all persons working at sea or on inland waterways. The requirement therefore applies to people working as maritime security on board a Dutch ship. For permit-issuing purposes, the maritime security company must demonstrate that those who may be deployed as a member of a private maritime security team hold the required certificate.

Article 16

Article 15 is based on Article 5.9(3)(b) of the Decree and sets requirements for the professional competence and training of maritime security guards. For example, the guards must have acquired at least four years of operational service experience in a military or police organisation and have received an honourable discharge. This implies a reliability requirement. In addition, written evidence is required to show that the person concerned is competent and trained to carry out maritime security work and is competent and trained in dealing with semi-automatic firearms. This evidence or these certificates must have been issued in the past twelve months. In addition, the persons concerned must have a sufficient command of English. The requirements set in this article are in line with the usual requirements in the sector.

Article 17

This provision is based on Article 5.9(3)(c) and (d) of the Decree and describes a number of duties and actions that the team leader must perform before and after boarding the ship. This is in line with what is already customary in the maritime security sector.

Chapter 7 Administrative fine

Articles 18 to 22 are based on Section 17 of the Act and concern the amount of the administrative fines to be imposed for offences that are punishable by a fine. There are separate articles for each group of people at whom the standard is aimed. These articles create an additional framework for the possible fines for the different groups that are the focus of the standard. Based on this framework, the ILT will draw up a penalty catalogue setting specific penalty amounts for different breaches. This penalty catalogue will be published in the Government Gazette.

Article 18

Article 18 of the Regulation concerns the administrative fines that may be imposed on the maritime security company (the permit holder). Section 17(1) of the Act gives the Minister the power to impose an administrative fine on the permit holder, of an amount to be set in a ministerial regulation, for breaching rules laid down in or pursuant to the Act, or the conditions attached to the permit. In Article 18 of the Regulation, this is translated into the specific provisions of the Act and the Decree. The amount of the fines is tailored to the offenders. Account will be taken of the responsibilities of the parties involved, the nature of the breaches that occurred and the presumed financial capacity of the parties involved. Article 18(1) sets out a list of provisions; the breach of one of these provisions could result in a maximum fine of Category 4 (€21,750). Article 18(2) states that a breach by the permit holder of the obligation to provide information to

the team leader may be penalised with a Category 3 fine (€4,350). Under Article 18(3), a Category 3 fine may be imposed in the event of a breach of the conditions attached to the permit.

Article 19

Article 19(2)(a) and (c) provides that an administrative fine may be imposed on the ship manager. This could occur in the event of a breach of Section 6(1) or (3) of the Act. This section concerns all reasonable protective measures to be applied prior to and during the transport. These measures are specified in more detail in Article 3 of the Regulation. The section also concerns compliance with the ship manager's obligation to provide information to the master.

Pursuant to Article 19 of the Regulation, a Category 3 administrative fine may be imposed on the ship manager in the event of a breach of these provisions (€4,350). The amount of the fine for a breach of the ship manager's obligation to provide information corresponds to the amount of the fine that may be imposed on the permit holder for the same breach.

Article 20

Pursuant to Section 17(2)(a), (b), (d) and (e) of the Act, administrative fines may be imposed on the master. A fine could be imposed for a breach of the provisions regarding the reasonable protective measures to be taken before and during the transport, the master's "duty to ascertain" before the transport and the reporting obligation following completion of the transport. A fine may also be imposed on the master in the event of a failure to comply with the rules concerning the responsibility of the master for the safety of the ship and of the persons on board in connection with the maritime security work. Section 17(2)(d) of the Act allows an administrative fine to be imposed with respect to the master's obligation to postpone departure or entry into a high-risk area if, at the time of embarkation of the private maritime security personnel and their weapons, cameras and microphones, the rules laid down in or pursuant to the Act were not complied with. A Category 2 fine may be imposed for a breach of these provisions. The financial capacity of the person concerned will be taken into account.

Article 21

Pursuant to Section 17(2)(b) and (e) of the Act, administrative fines may be imposed on the team leader. Fines will be imposed where the team leader violates the "duty to ascertain" prior to the transport, or fails to comply with the reporting obligation after the end of a transport. Such breaches may be penalised with a Category 2 fine. The financial capacity of the person concerned will be taken into account.

Article 22

Article 22 enables supervisory officials to take special circumstances into account when determining the amount of a fine. An exhaustive list of these circumstances is given in Article 22(1). Article 22(1)(c) emphasises that previous breaches of laws and regulations other than the Merchant Shipping Protection Act will not be taken into account. However, not only the exact same breach, but all breaches of the Act and the Decree will be taken into account when considering fines under these provisions. The extent to which the offender cooperates in establishing the breach will also be taken into account. ISO-certifying institutions assume that maritime security companies will notify the government on their own initiative of irregularities identified in audits conducted by these institutions; this assumption also plays an important part in the consideration of a fine. Furthermore, the statutory system assumes that permit holders will notify the ILT on their own initiative if their ISO certificate is suspended or withdrawn.

Depending on the circumstances, the administrative fine imposed may be proportionately lower than the prescribed amount. This is stated in Article 22(2).

Article 23

Article 5.13(2)(c) of the Merchant Shipping Protection Decree provides that rules will be set by ministerial regulation regarding the retention periods and destruction of video and sound recordings. Article 23(1) concerns the retention period for footage created by maritime security

guards pursuant to the Act. Normally, following the use of force, the footage is sent to the Public Prosecution Service along with the prescribed report (Section 12(3) of the Act); the maritime security guards may then destroy the footage. In some cases, it may be necessary or desirable to keep the footage for a longer period of time.

The maximum retention period of 28 days is in line with the retention period for footage from police bodycams. However, files containing video and sound recordings may be kept for longer, if this is necessary for instituting, executing or substantiating a legal claim. This may include obtaining compensation for damage.

Incidentally, Article 5.8(1) of the Merchant Shipping Protection Decree states that the reports, including underlying information such as video footage, must also be sent by the maritime security guards to the maritime security company (the permit holder). The maritime security company is required to retain the footage for three years pursuant to Article 5.8(1)(i) of the Decree.

Due to their positions, the master and the team leader are entitled to view or listen to the full video and sound recordings. Under the GDPR, crew members, private maritime security personnel and third parties already have the right to view images in which they appear.

Article 24

Article 24 is based on Article 6.1(2) of the Merchant Shipping Protection Decree, which states that a ministerial regulation may provide for safeguards for the processing of the personal data referred to in Article 6.1(1), in addition to the safeguards referred to in Article 6.1(1) (retention periods). Article 24 provides that the Human Environment and Transport Inspectorate must indicate in its privacy statement how it will provide certain safeguards in connection with the processing of personal data. The privacy statement must be posted on the Inspectorate website.

Article 25

This article concerns the entry into force of the Regulation. The Regulation will take effect at the same time as the Act and the general order in council.

The Minister of Justice and Security