ANNEX I

PORT SECURITY ASSESSMENT

The port security assessment is the basis for the port security plan and its implementation. The port security assessment will cover at least:

— identification and evaluation of important assets and infrastructure which it is important to protect;

— identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures;

— identification, selection and prioritisation of counter-measures and procedural changes and their level of effectiveness in reducing vulnerability; and

— identification of weaknesses, including human factors in the infrastructure, policies and procedures.

For this purpose the assessment will at least:

— identify all areas which are relevant to port security, thus also defining the port boundaries. This includes port facilities which are already covered by Regulation (EC) No 725/2004 and whose risk assessment will serve as a basis;

— identify security issues deriving from the interface between port facility and other port security measures;

— identify which port personnel will be subject to background checks and/or security vetting because of their involvement in high-risk areas;

— subdivide, if useful, the port according to the likelihood of security incidents. Areas will be judged not only upon their direct profile as a potential target, but also upon their potential role of passage when neighbouring areas are targeted;

— identify risk variations, e.g. those based on seasonality;

— identify the specific characteristics of each sub-area, such as location, accesses, power supply, communication system, ownership and users and other elements considered security-relevant;

— identify potential threat scenarios for the port. The entire port or specific parts of its infrastructure, cargo, baggage, people or transport equipment within the port can be a direct target of an identified threat;

— identify the specific consequences of a threat scenario. Consequences can impact on one or more sub-areas. Both direct and indirect consequences will be identified. Special attention will be given to the risk of human casualties;

— identify the possibility of cluster effects of security incidents;

— identify the vulnerabilities of each sub-area;

— identify all organisational aspects relevant to overall port security, including the division of all security-related authorities, existing rules and procedures;

— identify vulnerabilities of the overarching port security related to organisational, legislative and procedural aspects;

— identify measures, procedures and actions aimed at reducing critical vulnerabilities. Specific attention will be paid to the need for, and the means of, access control or restrictions to the entire port or to specific parts of a port, including identification of passengers, port employees or other workers, visitors and ship crews, area or activity monitoring requirements, cargo and luggage control. Measures, procedures and actions will be consistent with the perceived risk, which may vary between port areas;

— identify how measures, procedures and actions will be reinforced in the event of an increase of security level;

— identify specific requirements for dealing with established security concerns, such as 'suspect' cargo, luggage, bunker, provisions or persons, unknown parcels, known dangers (e.g. bomb). These requirements will analyse desirability conditions for either clearing the risk where it is encountered or after moving it to a secure area;

— identify measures, procedures and actions aimed at limiting and mitigating consequences;

— identify task divisions allowing for the appropriate and correct implementation of the measures, procedures and actions identified;

— pay specific attention, where appropriate, to the relationship with other security plans (e.g. port facility security plans) and other existing security measures. Attention will also be paid to the relationship with other response plans (e.g. oil spill response plan, port contingency plan, medical intervention plan, nuclear disaster plan, etc.);

— identify communication requirements for implementation of the measures and procedures;

— pay specific attention to measures to protect security-sensitive information from disclosure;

— identify the need-to-know requirements of all those directly involved as well as, where appropriate, the general public.

ANNEX II

PORT SECURITY PLAN

The port security plan sets out the port's security arrangements. It will be based on the findings of the port security assessment. It will clearly set out detailed measures. It will contain a control mechanism allowing, where necessary, for appropriate corrective measures to be taken.

The port security plan will be based on the following general aspects:

— defining all areas relevant to port security. Depending on the port security assessment, measures, procedures and actions may vary from sub-area to sub-area. Indeed, some sub-areas may require stronger preventive measures than others. Special attention will be paid to the interfaces between sub-areas, as identified in the port security assessment;

— ensuring coordination between security measures for areas with different security characteristics;

— providing, where necessary, for varying measures both with regard to different parts of the port, changing security levels, and specific intelligence;

— identifying an organisational structure supporting the enhancement of port security.

Based on those general aspects, the port security plan will attribute tasks and specify work plans in the following fields:

— access requirements. For some areas, requirements will only enter into force when security levels exceed minimal thresholds. All requirements and thresholds will be comprehensively included in the port security plan;

— ID, luggage and cargo control requirements. Requirements may or may not apply to sub-areas; requirements may or may not apply in full to different sub-areas. Persons entering or within a sub-area may be liable to control. The port security plan will appropriately respond to the findings of the port security assessment, which is the

tool by which the security requirements of each sub-area and at each security level will be identified. When dedicated identification cards are developed for port security purposes, clear procedures will be established for the issue, the use-control and the return of such documents. Such procedures will take into account the specificities of certain groups of port users allowing for dedicated measures in order to limit the negative impact of access control requirements. Categories will at least include seafarers, authority officials, people regularly working in or visiting the port, residents living in the port and people occasionally working in or visiting the port;

— liaison with cargo control, baggage and passenger control authorities. Where necessary, the plan is to provide for the linking up of the information and clearance systems of these authorities, including possible pre-arrival clearance systems;

— procedures and measures for dealing with suspect cargo, luggage, bunker, provisions or persons, including identification of a secure area; as well as for other security concerns and breaches of port security;

— monitoring requirements for sub-areas or activities within sub-areas. Both the need for technical solutions and the solutions themselves will be derived from the port security assessment;

— signposting. Areas with access and/or control requirements will be properly signposted. Control and access requirements will appropriately take into account all relevant existing law and practices. Monitoring of activities will be appropriately indicated if national legislation so requires;

— communication and security clearance. All relevant security information will be properly communicated according to security clearance standards included in the plan. In view of the sensitivity of some information, communication will be based on a need-to-know basis, but it will include where necessary procedures for communications addressed to the general public. Security clearance standards will form part of the plan and are aimed at protecting security sensitive information against unauthorised disclosure;

— reporting of security incidents. With a view to ensuring a rapid response, the port security plan will set out clear reporting requirements to the port security officer of all security incidents and/or to the port security authority;

— integration with other preventive plans or activities. The plan will specifically deal with integration with other preventive and control activities in force in the port;

— integration with other response plans and/or inclusion of specific response measures, procedures and actions. The plan will detail interaction and coordination with other response and emergency plans. Where necessary conflicts and shortcomings will be resolved;

— training and exercise requirements;

— operational port security organisation and working procedures. The port security plan will detail the port security organisation, its task division and working procedures. It will also detail the coordination with port facility and ship security officers, where appropriate. It will delineate the tasks of the port security committee, if this exists;

— procedures for adapting and updating the port security plan.

ANNEX III

BASIC SECURITY TRAINING EXERCISE REQUIREMENTS

Various types of training exercises which may involve participation of port facility security officers, in conjunction with the relevant authorities of Member States, company security officers, or ship security officers, if available, will be carried out at least once each calendar year with no more than 18 months elapsing between the training exercises. Requests for the participation of company security officers or ships security officers in joint training exercises will be made bearing in mind the security and work implications for the ship. These training exercises will test communication, coordination, resource availability and response. These training exercises may be:

(1)   full scale or live;

(2)   tabletop simulation or seminar; or

(3)   combined with other exercises held such as emergency response or other port State authority exercises.

ANNEX IV

CONDITIONS TO BE FULFILLED BY A RECOGNISED SECURITY ORGANISATION

A recognised security organisation will be able to demonstrate:

(1)   expertise in relevant aspects of port security;

(2)   an appropriate knowledge of port operations, including knowledge of port design and construction;

(3)   an appropriate knowledge of other security relevant operations potentially affecting port security;

(4)   the capability to assess the likely port security risks;

(5)   the ability to maintain and improve the port security expertise of its personnel;

(6)   the ability to monitor the continuing trustworthiness of its personnel;

(7)   the ability to maintain appropriate measures to avoid unauthorised disclosure of, or access to, security-sensitive material;

(8)   knowledge of relevant national and international legislation and security requirements;

(9)   knowledge of current security threats and patterns;

(10)   the ability to recognise and detect weapons, dangerous substances and devices;

(11)   the ability to recognise, on a non-discriminatory basis, characteristics and behavioural patterns of persons who are likely to threaten port security;

(12)   knowledge of techniques used to circumvent security measures;

(13)   knowledge of security and surveillance equipment and systems and their operational limitations.

A recognised security organisation which has made a port security assessment or review of such an assessment for a port is not allowed to establish or review the port security plan for the same port.