

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;

Status: EU Directives are being published on this site to aid cross referencing from UK legislation. After IP completion day (31 December 2020 11pm) no further amendments will be applied to this version.

- 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.