

Marine Transportation Security Clearance Program

Access to Security Information

1. What is Security Information?

Security Information is any information that is operationally or security sensitive in nature that if released or compromised could have a detrimental effect on the economic, personnel or physical attributes of a facility. As one example, if the information provides details about such things, as security plans, responses to security incidents, operational functions or features of the facility, or security components, this would be considered security information.

2. What is Access to Security Information?

There are many other examples of information/documentation that are more basic in nature that could be considered a potential security risk if compromised.

If a person has a physical copy of a document related to container or cargo movement that contains more than one element of information, such as a container number and location, location on the facility and the location on the ship, as well as the time of movement and to what location, etc., then this would be considered access to security information. The physical possession or knowledge of this type of information should be assessed from the perspective of what could the person possessing this information do with it or what effect would it have with respect to the safety or security of the facility if it were compromised. In other words, if a person wanted to inflict economic damage or cause loss of life or injury, would the possession or release of this information be sufficient to make it possible?

Access to security information also relates to the creation, alteration, control or maintenance of cargo documentation or crew/passenger lists. A person with this kind of access may or may not be on the facility or port but may have advance access to what would be considered security information. This information if mishandled, compromised or distributed, could have a security impact on the operation of a facility, port or a ship and the persons contained within.

3. What Makes a Document/Information a Security Issue?

Any information that if in the hands of any person can be used to disrupt the operations of a marine facility, facilitate the development of a threat profile, or an actual attack, is considered a security issue.

4. What makes it necessary for certain information to be secure?

The key points one has to consider, as to whether information is operationally or security sensitive and should be subject to security safeguards, is to assess whether the misuse, or distribution of such information could create an impact on the operations of a marine facility or its personnel. Examples of why certain information should be secure would be, if a person possessing security information or parts thereof misuses, or gives this information to someone who could use it:

- to cause a preventative measure to be circumvented, caused to be ineffective, or fail, etc.,
- to potentially delay the response to a security incident, i.e., by misdirection or by providing false or incomplete information, etc.,
- to negatively affect the recovery from a security incident through misdirection, false information, creating obstacles either physical or perceived, etc.

5. Examples of Security Information

The following are a few examples to provide guidance in determining what is deemed as security information. A more comprehensive list is contained in the Designated Position Tool, notes 4 and 11. This in no way is an exhaustive list and each document and variations thereof will have to be reviewed on a case-by-case basis in whole or in part.

Description of Document	No Security Implications	Security Implications	Portions may be Secure	To be determined on a case-by-case
Buck Slip		✗		
Baplie File		✗		
Bay Plan			✗	
Security personnel shift schedules		✗		
Security personnel patrol schedules		✗		
Ship Scheduling Plans			✗	
Stowe Plans		✗		