Sensitive Security Information Regulations under 49 U.S.C. 114 (s) and 49 CFR 1520.7 (k) (Transportation Security Agency Regulations).

"The information in this document is for use as an aid to interpretation. Should anything in this document be in conflict with Navigation Vessel Inspection Circular (NVIC) 9-02, Change 1, or CG policy, then NVIC 9-02 and the CG policy determinations control."

Q. The Maritime Transportation Security Act (MTSA) regulations refer to Sensitive Security Information (SSI). What is Sensitive Security Information?

Ans. On November 25, 2002, the President signed into law the MTSA. These regulations, found at 33 CFR Subchapter H—Maritime Security, established a new framework for maritime security. Primary elements of this framework are National, area, port, facility, and vessel security plans.

The Transportation Security Agency (TSA), an organizational element of the Department of Homeland Security (DHS) has issued regulations under 49 U.S.C. 114 (s) and 49 CFR 1520.7 (k) that allows TSA to designate as SSI, any information obtained or developed in carrying out security requirements that would be detrimental to the security of transportation if that information was disclosed.

Q. What specific types of information have been designated as Sensitive Security Information under the MTSA regulations?

Ans. The U.S. Coast Guard, as designated lead federal maritime agency for administration of the MTSA regulations requested the TSA to designate certain information developed in accordance with implementation of the MTSA, as SSI. Accordingly, in the interest of maritime transportation security, the TSA has designated the following information and records as SSI:

(1) Any vessel, maritime facility, or port area security plan required or directed under federal law.
(2) Maritime Security Directives issued by the U.S. Coast Guard under 33 CFR Part 101.405.
(3) Navigation Vessel Inspection Circulars (NVIC(s)) issued by the U.S. Coast Guard related to maritime security.

See 49 CFR Part 1520 and NVIC 9-02 (rev 1).

Q. Can you be more specific as to other types of information that may be designated as Security Sensitive Information (SSI)?

Ans. In accordance with 49 U.S.C. 114 (s), SSI is information obtained or developed in the conduct of transportation security activities, including research and

development, the disclosure of which the Transportation Security Agency (TSA) has determined would:

(1) Constitute an unwarranted invasion of privacy including, but not limited to information contained in any personnel, medical, or similar file.
(2) Reveal trade secrets or privileged or confidential information obtained from any person.
(3) Be detrimental to the security of maritime transportation.

Q. As a vessel or maritime facility owner and/or operator, where do I find more specific U.S. Coast Guard guidance about my responsibilities for proper handling of Sensitive Security Information (SSI)?

Ans. Navigation Vessel Inspection Circular NVIC 9-02 (rev 1) provides detailed guidance on responsibilities associated with handling SSI. After reviewing the NVIC guidance and other listed references, if you are still uncertain as to how to handle SSI or you have other legal questions relative to the handling or release of information, contact your area/district legal office, G-MPS-2, or G-LRA for specific guidance. In addition, certain information may be subject to Freedom of Information Act requirements.

Q. Who is authorized to handle Sensitive Security Information (SSI)?

Ans. A "covered person" with a "need to know" may handle SSI materials.

Q. Who is considered a "covered person" for purposes of the Sensitive Security Information regulations?

Ans. Included under the definition of a "covered person" for purposes of the Sensitive Security Information (SSI) regulations, are the following:

(1) Each owner, charterer, or operator of a vessel, including U.S. and foreign vessel(s) that are required to have a security plan under Federal or International law.
(2) Each owner or operator of a maritime facility that is required by the MTSA to have a security plan.
(3) Each person participating in a national or area security committee established in accordance with 46 U.S.C. 70112, or a port security committee.
(4) Each maritime industry trade association that represents covered persons and that has entered into a non-disclosure agreement with the Department of Homeland Security (DHS).
(5) DHS and DHS Agency employees.
(6) Each person conducting research and development activities that relate to maritime transportation security and are approved, accepted, funded, recommended, or directed by the DHS.
(7) Each person who has access to SSI, as specified in 49 CFR 1520.11.

(8) Each person employed by, contracted to, or acting for a covered person, including a grantee of the DHS, or a person formerly in such position.
(9) Each person for which a vulnerability assessment (VA) has been directed, created, held, funded, or approved by the DHS, or that has prepared a VA that will be provided to the DHS in support of a Federal security program.
(10) Each person receiving SSI under 49 CFR 1520.15(d) or (e).

Q. Who in accordance with the Sensitive Security Information (SSI) regulations has a "need to know" SSI?

Ans. (a) In general. A person has a "need to know" SSI when the person is carrying out maritime transportation security activities approved, accepted, funded, recommended, or directed by the DHS and:
(1) Requires access to specific SSI;
(2) Is in training;
(3) Requires information necessary to supervise or otherwise manage individuals;
(4) Needs the information to provide technical or legal advice to a covered person regarding MTSA requirements, federal law, or in connection with any judicial or administrative proceeding regarding those requirements.

(b) Federal employees, contractors, and grantees.
(1) A Federal employee has a need to know if the information is necessary for performance of official duties.
(2) A contractor, acting in the performance of a contract or with a grant from the DHS if the information is necessary to performance.

Q. Can legal restrictions be placed on an individual's access to Sensitive Security Information (SSI)?

Ans. Yes. The TSA or U.S. Coast Guard may restrict an individual's access to SSI contingent upon satisfactory completion of a security background verification or invoke other procedures and requirements for safeguarding SSI materials.

In addition, for some specific SSI, the DHS may make a finding that only specific persons or classes of persons have a "need to know".

Q. What are the provisions for proper handling of Security Sensitive Information (SSI)?

Ans. Individuals in custody of SSI should take reasonable steps to safeguard the information as follows:
(1) If the SSI is in their possession, prevent unauthorized disclosure.

(2) When the individual is not in physical possession of the SSI, it must be stored in a secure container such as a locked desk or file cabinet or in a locked room secure from unauthorized access.
(3) A covered person must destroy SSI completely to preclude recognition or reconstruction of the information when the SSI is no longer needed.
(4) If a covered person becomes aware that SSI may have been compromised by release to unauthorized persons, he/she must promptly inform the local COTP/FMSC. See Navigation Vessel Inspection Circular 9-02 (rev 1).

Q. Will members of an Area Maritime Security Committee (AMSC) be required to undergo a Background Investigation (BI) as a prerequisite to having access to Sensitive Security Information disseminated by the Federal Maritime Security Coordinator (FMSC)?

Ans. No, however under certain circumstances the FMSC, may designate individual AMSC members individually or as members of a subcommittee to conduct work that requires access to "classified" materials above the SSI designated level of information.

If an AMSC member is designated to have access to "classified" information above the SSI designated level, that member would be required to undergo a BI appropriate for the level of classified information access required. Though the BI checks are voluntary, the procedure requires completion of a personal information disclosure waiver before the BI is requested. See Navigation Vessel Inspection Circular 9-02 (rev 1).