U.S. Department of Transportation
United States Coast Guard

Commandant
United States Coast Guard

2100 Second St. S.W.
Washington, DC 20593
Staff Symbol: G-MPS-2
Phone: (202) 267-1448

COMDTPUB 16700.4
NVIC 10 04

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 10 04 AUG 20 2004

Subj: GUIDELINES FOR HANDLING OF SENSITIVE SECURITY INFORMATION (SSI)

Ref: (a) 46 USC 701
(b) 49 USC 114
(c) 49 CFR Part 1520
(d) Security Classification and Designation Policy for Port Security Assessments, Critical Infrastructure Listings, and Port Security Assessment Tools, Enclosure (2), COMDTINST 5510.5 (series) (NOTAL)

1. PURPOSE.

   a. The purpose of this Circular is to provide guidance to field commanders and the maritime industry on the access, safeguarding, and disclosure of information, designated as Sensitive Security Information (SSI), as defined in 49 CFR Part 1520 (as amended). SSI is information that the Transportation Security Administration (TSA) has determined must be protected from improper disclosure in order to ensure transportation security. TSA has amended its SSI regulations to cover the security measures required by the Maritime Transportation Security Act (MTSA) of 2002 and exempts information related to maritime security from public disclosure under the Freedom of Information Act (FOIA). (*See* 69 Federal Register 28066, May 18, 2004 on the Worldwide Web at http://www.gpoaccess.gov/index.html).

   b. This circular does not apply to the access, maintenance, safeguarding, or disclosure of national security information, as defined by Executive Orders 12968 and 12958 (as amended). The examples of SSI in this guidance are not all-inclusive and may, in some instances, also contain classified information. The Classified Information Management Program, COMDTINST 5510.23 (series) should be referenced.

2. ACTION. Commanding Officers of Marine Safety Offices, Sector Commanders, Captains of the Port (COTP), Commanding Officer Marine Safety Center, and maritime

DISTRIBUTION -SDL No. 141

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A																										
B		2	10		1			1						132	1			1								30
C												1														
D	1	1		1							1															
E															1											
F																										
G																										
H																										

NON-STANDARD DISTRIBUTION

stakeholders should utilize the guidelines in this circular when examining security programs required by 33 CFR, Subchapter H and whenever reviewing other records and information subject to 49 CFR Part 1520. The term Federal Maritime Security Coordinator (FMSC) is used to designate the COTP when implementing the provisions of 33 CFR Subchapter H. The Coast Guard will distribute this circular by electronic means only. It is available on the Worldwide Web at http://www.uscg.mil/hq/g-m/nvic/index.htm.

3. DIRECTIVES AFFECTED. None.

4. BACKGROUND.

a. SSI is a specific category of information that requires protection against disclosure. 49 U.S.C. 114(s) limits the disclosure of information obtained or developed in carrying out certain security or research and development activities to the extent that TSA and the Coast Guard have determined that disclosure of the information would:

(1). be an unwarranted invasion of personal privacy;

(2). reveal a trade secret, privileged, confidential commercial or financial information;

(3). be a detriment to the safety and security of the Marine Transportation System (MTS).

b. The information that falls within the scope of the statute is prescribed by TSA regulations in 49 CFR Part 1520. The purpose of the provision is to prevent unauthorized disclosure of information while being mindful of the legitimate interest and right to know transportation security information among certain segments of the public. Limiting access to this information is necessary to guard against disclosure to those who pose a threat to transportation security and lessen their ability to develop techniques to subvert security measures.

c. Although subject to certain legal disclosure limitations, SSI is not classified national security information subject to the handling requirements for classified information. SSI handling procedures are laid out in enclosure (2).

5. DISCUSSION.

a. This circular provides guidance to field commanders and the maritime industry on how to control access to, maintain, and safeguard SSI information while implementing and enforcing the provisions of CFR Title 33, Subchapter H, pertaining to the establishment and implementation of Facility Security Plans (FSPs), Vessel Security Plans (VSPs), Alternative Security Plans (ASPs), Area Maritime Security (AMS) Plans, Security Incident Response Plans, and the National Maritime Transportation Security Plan. It applies to SSI information encountered in the implementation and enforcement of security programs including the International Port Security Program, High Interest Vessel Program, and the Positive Control Boarding Program. Additional SSI guidance may be

found in reference (d). Based on the promulgation of the new TSA SSI regulation, a new SSI COMDINST will be forthcoming.

b. Plans and programs that contain SSI necessitate the protection of the information. Guidance for handling security plans and programs, dissemination, and protection of SSI is provided in enclosures (1) through (3) of this circular. Enclosure (4) provides pertinent definitions relating to key terms. Enclosure (5) are sample non-disclosure statements.

c. While the guidance contained in this document may assist the maritime industry, public, the Coast Guard, other Federal and state regulators in applying statutory and regulatory requirements, the guidance is not a substitute for applicable legal requirements, nor is it a regulation in itself; thus, it is not intended to, nor does it, impose legal requirements.

6. IMPLEMENTATION. Coast Guard field commanders and maritime stakeholders shall use the guidance in this circular to assist them in the implementation and enforcement of the various maritime security regulations and programs.

7. ENFORCEMENT.

a. The goal of enforcement of SSI requirements is to ensure safeguarding of SSI. Educating Federal, State, local, and industry partners about the importance of compliance with the requirements is a necessary condition of any successful enforcement regime. Deterrence also plays an important part. Therefore, the Coast Guard should consider the entire scale of enforcement tools available when issuing enforcement measures, such as documenting an initial minor violation in a letter of warning, with subsequent violations documented in NOVs, or civil penalties. Action may include issuance of an order requiring retrieval of SSI. *See* 49 CFR §1520.17

b. An unauthorized disclosure of maritime sensitive security information and a failure to report an unauthorized disclosure to the cognizant COTP pursuant to 49 CFR §1520.9 by a covered person may jeopardize the security of the marine transportation system and result in a civil penalty up to $25,000 per violation. *See* 46 USC 70117.

8. FORMS/REPORTS. None.

T. H. GILMOUR
Assistant Commandant for Marine Safety,
Security and Environmental Protection

Enclosures: (1) Examples of Sensitive Security Information (SSI)
(2) Access to Sensitive Security Information (SSI)
(3) Handling Sensitive Security Information (SSI)
(4) Definitions
(5) Non-disclosure Statement(s)

ENCLOSURE (1) TO NVIC 10 – 04

EXAMPLES OF SENSITIVE SECURITY INFORMATION (SSI)

(The italicized text reflects 49 CFR § 1520.5 and the examples listed are not exhaustive.)

1. **Security Programs and Contingency Plans** 49 CFR § 1520.5(b)(1) -
Any security program or security contingency plan issued, establish, required, received, or approved by the Coast Guard, including –
(i) Not applicable;
(ii) Any vessel, maritime facility, area security plan required or directed under Federal law;
(iii) Any national or area maritime security plan prepared under 46 USC 70103; and
(iv) Any security incident response plan prepared under 46 USC 70104.

Note: This section covers all security plans required, (including draft forms) by the MSTA regulations. Plans include but are not limited to:
- MTSA Vessel and Facility Security Plans
- Area Maritime Security Plans
- Security Incident Response plans contained in Vessel, Facility, and Area Maritime Security (AMS) Plans
- National Maritime Security Plan
- Alternative Security Programs
- Equivalent security measures
- Requests for waiver from 33 CFR Subchapter H
- State and local maritime security plans shared with the Coast Guard
- Facility and vessel security plans provided to the Coast Guard that are required by 33 CFR Subchapter H.

Security Programs include but are not limited to:
- International Port Security Program
- High Interest Vessel (HIV) program information
- Domestic Port Security Assessment Program

2. **Security Directives** 49 CFR § 152.5(b)(2) -
Any Security Directive or order –
(i) Issued by the Transportation Security Administration (TSA) under 49 CFR 1542.303, 1544.305 or other authority;
(ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR Part 6, or 33 USC 1221 et seq, related to maritime security; or
(iii)Any comments, instructions, and implementing guidance pertaining thereto.

This includes:
- MARSEC Directives issued by the Coast Guard
- Security Directives issued by TSA

3. **Information Circulars** 49 CFR § 1520.5(b)(3) -

Any notice issued by DHS regarding a threat to maritime transportation, including specific Navigation and Vessel Inspection Circulars issued by the Coast Guard related to maritime security that are designated SSI.

Note: In general, not all NVICs related to maritime security will be designated as SSI, only those that contain specific information that is directly related to threats to maritime transportation or critical security measures such as screening guidance.

- Enclosure (1) of NVIC 06-04, Voluntary Screening Guidance Procedures for Owners/Operators.

4. **Performance Specifications** 49 CFR § 1520.5(b)(4) -
Any performance specification and any description of a test object or test procedure for detecting any weapon, explosive, incendiary, or destructive device or substance; and any communications equipment used by the Federal government or any other person in carrying out or complying with any maritime transportation security requirements for Federal law.

This includes:
- Radiation detection devices
- Passenger/baggage/cargo equipment screening standards/specifications
- Secure communications equipment specifications
- Satellite communications
- Access control, intrusion detection systems

5. **Vulnerability Assessments** 49 CFR § 1520.5(b)(5) -
Any vulnerability assessment directed, created, held, funded, or approved by the Coast Guard, or that will be provided to the Coast Guard in support of a Federal security program.

This includes:
- Vessel/Facility Security Assessment/Self-Assessment Report(s)
- AMS Assessments
- CG-6025A
- Any assessment included in an AMS plan
- Assessments required by the National Maritime Security Plan
- Any other assessments regardless of the agency (DOD, USCG, TSA, ICE, State, local, etc,)

6. **Security Inspection or Investigative Information** 49 CFR § 1520.5(b)(6) -
Details of any security inspection or investigation of an alleged violation of maritime transportation security requirements of Federal law that could reveal security vulnerability. This includes the identity of the inspector or investigator who conducted the inspection or audit. Coast Guard generated security information related to inspections and investigation in general shall be designated as SSI but may

be protected in accordance with FOUO standards listed in the Classified Information Management Program, COMDTINST M5510.23 (series).

This includes:

- The name of the port, facility or vessel where a violation occurred.
- The Port/Facility/Vessel identifier in the case number.
- Any security related discrepancy discovered or developed during inspections and/or investigations. The security discrepancy needs to be kept separate from the safety deficiencies and marked accordingly.
- Any security related documentation entered in a CG 840 for vessel and facility inspections and audits.
- MTSA Facility Compliance Guide
- Domestic Vessel Security Plan Verification Guide for MTSA/ISPS Code
- Any security related documentation entered in a CG 835.
- Documentation issued by Facility Inspectors addressing facility security plan/equipment deficiencies.
- Security related MISLE entries concerning deficiencies and narratives thereof.

Note: Whenever possible, notices of security deficiencies should be issued to a person with security responsibilities. However, in all cases, when someone receives security discrepancies, that person becomes a covered person with a responsibility to protect that information. Ordinarily, the Coast Guard will not disclose SSI information without having a non-disclosure agreement on record for an individual. However, in the case of the vulnerability information disclosed on a CG 835, completion of a nondisclosure agreement is not required because it is assumed that the company's security interest in this information is sufficient to prevent unauthorized disclosure.

7. **Threat Information** 49 CFR § 1520.5(b)(7) -
Any unclassified information held by the Coast Guard concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information, including threats against cyber infrastructure.

(i) "General Threat Information", that is information that is non-specific in nature that may be used for public awareness within the maritime industry. The distribution of this information will be specified by Commandant G-MP.
(ii) "Specific Threat Information", this is information targeting a specific vessel/facility/port or target of opportunity and must be SSI in order to protect the asset or decrease the security vulnerability of the asset/target.
(iii) Incoming Threat Information: Local FMSCs shall quickly determine the classification/designation (Classified, Sensitive, or non-Sensitive) of any threat made in their area of responsibility.
Note: Once an SSI determination is reached, the information should be protected appropriately. If the information is classified, refer to COMDTINST 5510.23 (series) for guidance. However, nothing in this section prohibits the timely

dissemination of threat information in order to protect public interests. See 49 CFR §1520(5)(c).

8. **Security Measures** 49 CFR § 1520.5(b)(8) -
Specific details of maritime security measures, both operational and technical, whether applied directly by the Coast Guard or another person, including -
(i) Security measures or protocols recommended by the Federal government;
(ii) Information concerning Coast Guard physical and operational security measures.

This includes:
- Minutes, discussions and deliberations of Area Maritime Security Committee that are concerned with SSI information; inspections, investigations, visits, operational concepts and/or resources.
- Unclassified OPSEC measures in the Area Security Plan, including various actions taken by law enforcement stakeholders.
- Public Access Facilities security measures.
- Log books, watch schedules, exercises and drills, other operational summaries or synopsis which discuss security measures.
- Security measures that document activities of State and local resources operating under the AMS plan.

9. **Security Screening Information** 49 CFR § 1520.5(b)(9) -
The following information regarding security screening under maritime transportation security requirements of Federal law:
(i) Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other authorized person.
(ii) Information and sources of information used by a passenger or property screening program or system, including an automated screening system.
(iii) Detailed information about the locations at which particular screening methods or equipment are used, only if determined by the Coast Guard to be SSI.
(iv) Any security screener test and scores of such tests.
(v) Performance or testing data from security equipment or screening systems.
(vi) Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.

This includes:
- Enclosure (1) of NVIC 06-04, Voluntary Screening Guidance for Owners and Operators of Vessels and Facilities Regulated under 33 CFR Subchapter H
- Redacted portions of NVIC 04-02, Security for Passenger Vessels and Passenger Terminals
- Guidance developed for screening of cargo
- Screening for entry into restricted port areas (AMS Plan)

- Details of any information contained within vessel and facility security plans that address their screening procedures

10. **Security Training Materials** 49 CFR § 1520.5(b)(10) -
Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Coast Guard or Industry or another person to carry out any maritime transportation security measures required or recommended by the Coast Guard.

Note:
(i) Not all training materials related to maritime security in general will be designated as SSI, only material that contain specific information that if released, would be detrimental to transportation security.
(ii) Commercial vendors should review the training materials and records of trained personnel for potential SSI issues. All Computer Based Training should be password protected. Not all commercially available material/courses related to maritime security in general will be designated as SSI, only those that contain specific information that, if released, is detrimental to transportation security.

This includes:
- Electronic formats – DVD, CD ROM, computer based training web based, floppy discs, and portable memory storage devices.
- Written/bound material.
- Video presentations (videotape and DVDs) - Must contain both the SSI marking and the limited distribution statement at the beginning and end of the presentation. The container holding the presentation must also be marked SSI and the inside sleeve of the protective covering must contain the limited distribution statement.
- Classroom discussion – Instructors must take reasonable precautions to prevent unauthorized disclosure (e.g., the classroom door should be closed; only people with a need to know are in the room; instructors should announce that the material being presented is SSI and give the limited distribution statement and remind the students not to disclose this information to others who do not have a need to know).
- Correspondence courses – Shall be treated as other written materials.
- Tabletop exercises.

11. **Identifying Information of Certain Transportation Security Personnel** 49 CFR § 1520.5(b)(11) -
Lists of the names or other identifying information that identify persons as:
(i) Having unescorted access to a secure area of a maritime facility, port area or vessel or;
(ii) Holding a position as a security screener employed by or under contract with the Federal government pursuant to maritime transportation security requirements of Federal law, where such lists are aggregated by port;

(iii) Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boardings, or engaged in operations to enforce maritime security requirements or conduct force protection.

Note: This is interpreted to include all U.S. Coast Guard officials, State and local authorities and industry personnel acting under MTSA responsibilities. Any lists identifying security personnel, persons with special access to restricted areas, including frequent visitors (recurring visitors) to include long-term frequent vendors are also SSI.

These are internal records and the holder of these documents must follow the procedures for protecting SSI. The credentials themselves (e.g., ID badges) are not considered SSI material.

12. **Critical Maritime Infrastructure Asset Information** 49 CFR § 1520.5(b)(12) - *Any list identifying systems or assets, whether physical or virtual, so vital to the maritime transportation system that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is –*
    (i) Prepared by the Coast Guard; or
    (ii) Prepared by a State or local government agency and submitted by the agency to the Coast Guard.

    This includes:
    - Detain on board crew lists
    - Critical infrastructure lists
    - Procedures to re-establish/reopen the port
    - Critical components listed in VSPs/FSPs/ASPs

13. **System Security Information** 49 CFR § 1520.5(b)(13) - *Any information involving the security of operational or administrative data systems operated by the Federal government that have been identified by Coast Guard as critical to maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.*

    - Marine Information for Safety and Law Enforcement (MISLE) – MISLE maps over to the PSIX portal (e.g., Positive Control Boardings, all HIV and security boarding activity, security plans and security plan deficiencies, security investigations including civil penalty or ticket activities, Port Safety activities including COTP Orders which are specifically related to Security issues including denial of entry to U.S., expulsion from U.S. waters, Detain on Board orders). All the above items must be properly marked as SSI. All narratives must start with **SENSITIVE SECURITY INFORMATION.**
    - Ship Arrival Notification System (SANS)
    - National Response Center database relating to security breaches and suspicious activity reports
    - Homeland Security Information Network

- External security systems – information provided to the Coast Guard about industry, State and local government generated security systems should be deemed SSI and the appropriate controls should be put in place to prevent unauthorized disclosure

14. **Confidential Business Information** 49 CFR § 1520.5(b)(14) -
(i) Solicited or unsolicited proposals received by DHS, DOT, and Coast Guard and negotiations arising therefrom, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to maritime transportation security measures;
(ii) Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS, DOT, and Coast Guard in carrying out maritime transportation security responsibilities; and,
(iii) Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS, DOT, and Coast Guard in carrying out maritime security responsibilities, but only if the source of the information does not customarily disclose it to the public.

Note: The CG must prevent the disclosure of any confidential business information contained within any Vessel/Facility/Port security plans.

This includes:
- Results of vulnerability/risk assessments used in preparing a grant request (e.g., facility deficient in perimeter fencing & lighting submits grant request)
- Information contained in vessel and facility security plans
- Business sensitive proprietary information that is developed by the organization and recognized trade secrets and patents
- Commercial/Financial Information

15. **Research and Development** 49 CFR § 1520.5(b)(15) -
Information obtained or developed in the conduct of research related to maritime transportation security activities, where such research is approved, accepted, funded, recommended, or directed by the DHS or DOT, including research results.

Note: All data, information, research notes, reports, test results, etc which are used during vulnerability assessments and the development of security grant requests are considered SSI (at a minimum) and all protective measures shall be adhered to.

This includes:
- Criteria the industry and other quasi-governmental agencies use to assist in developing grant requests for DHS security grants.
- CG contracted research projects on other maritime infrastructure activities.
- Research of maritime security related issues conducted at the Coast Guard Research and Development Center in Groton, CT.

16. **Other Information** 49 CFR 1520.5(b)(16) -

Any information not otherwise described in this section that TSA determines is SSI under 49 USC 114(s) or that the Secretary of the Department of Homeland Security determines is SSI under USC 40119. Upon the request of another Federal Agency, TSA or the Secretary of the Department of Homeland Security may designate as SSI information not otherwise described in this section.

Note: The Coast Guard, in consultation with TSA, may determine other documents, policies, procedures or equipment to be designated as SSI.

This includes:

- Any letters/memos drafted by the Coast Guard addressing security plans and contingency plans.
- After action reports addressing lessons learned from security contingency drills/exercises.

ENCLOSURE (2) TO NVIC 10 – 04

ACCESS TO SENSITIVE SECURITY INFORMATION (SSI)

1. Access to SSI designated material should be limited to those who meet the criteria of being a "covered person" with a "need to know" unless otherwise authorized in writing by either TSA or the Coast Guard.
2. Access to SSI does not require a security background check, but covered persons shall agree upon procedures that safeguard SSI in accordance with this NVIC.
3. "Covered Person" means any organization, entity, individual, or other person described below. (See 49 CFR § 1520.7).

- Every owner, charterer, or operator of a vessel, including foreign vessel owners, charterers, and operators required to have a vessel security plan, or equivalent under Federal or international law;
- Every owner or operator of a maritime facility subject to the Maritime Transportation Security Act, (Pub.L. 107-295), 46 U.S.C. 70101 et seq., 33 CFR Part 105, or 33 *U.S.C. 1221* et seq.;
- Every owner or operator of an Outer Continental Shelf facility subject to the Maritime Transportation Security Act, (Pub.L. 107-295), 46 U.S.C. 70101 et seq., 33 CFR Part 106, or *33 U.S.C. 1221 et seq.*;
- Each person participating in the National or Area Maritime Security Committee established under 46 U.S.C. 70112;
- Each industry trade association that represents Covered Persons and has entered into a non-disclosure agreement (Encl 5);
- Coast Guard officials and employees, including contract employees;
- Each person conducting research and development activities that relate to Maritime Transportation System (MTS) security and are approved, accepted, funded, recommended, or directed by the DHS or the Coast Guard;
- Each person who has access to SSI, as specified with a "need to know";
- Each person employed by, contracting with, or acting for a Covered Person, including a grantee of the Coast Guard, and including a person formerly in such position. An individual applying for employment in a position that would allow designation as a covered person, or one in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment may be considered a covered person;
- Each person for which a vulnerability assessment has been directed, created, held, funded, or approved by the U.S Coast Guard, or that has prepared a vulnerability assessment that will be provided to the Coast Guard in support of a Federal security program;
- Each person receiving SSI with a "need to know".

4. Persons with a "Need to Know". (See 49 CFR § 1520.11).

In general. A person has a "need to know" SSI in each of the following circumstances:

- When the person requires access to specific SSI to carry out MTS security activities approved, accepted, funded, recommended, or directed by the Coast Guard;
- When the person is in training to carry out MTS security activities approved, accepted, funded, recommended, or directed by the Coast Guard;
- When the information is necessary for a person to supervise or otherwise manage individuals carrying out MTS security activities approved, accepted, funded, recommended, or directed by the Coast Guard;
- When the person needs the information to provide technical or legal advice to a Covered Person regarding MTS security requirements of Federal law;
- When the person needs the information to represent a Covered Person in connection with any judicial or administrative proceeding, except in the case of an individual serving as litigation counsel who is not a direct employee of the Covered Person, the person has a "need to know" only if in the judgment and sole discretion of the Coast Guard, access to the SSI is necessary for adequate representation of the Covered Person in the proceeding.

Federal employees, contractors, and grantees.

- A Federal employee has a "need to know" SSI if access to the information is necessary for performance of the employee's official duties.
- A person acting in the performance of a contract with or grant from DHS or Coast Guard has a "need to know" SSI if access to the information is necessary to performance of the contract or grant.

  Note: The need to know may be further limited. The Coast Guard may make a finding that only specific persons or classes of persons have a "need to know specific SSI."

5. In general, an owner/operator can share SSI that is internal to the operation of the company with those employees and contractors they deem necessary, i.e., individuals with security responsibilities may be deemed to be covered persons with a need to know SSI that relates to conduct of their maritime transportation security activities. The owner/operator may utilize the applicable non-disclosure statement in enclosure (5) Tab B to assist with tracking individuals or entities that they have authorized to access SSI. (See paragraph 4.c. of enclosure (3)).