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

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;

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)).

ENCLOSURE (3) TO NVIC 10 – 04

SENSITIVE SECURITY INFORMATION (SSI) HANDLING PROCEDURES

1. HANDLING SSI.

a. A covered person must take reasonable steps to safeguard SSI in their possession or control from unauthorized disclosure.

(1.) When SSI material is not secured in a locked container, Commanding Officers or appropriate security officers shall make reasonable efforts to prevent unsupervised, unrestricted access to SSI by individuals not cleared to view SSI.

(2.) During office hours, SSI is to be placed in an out-of-sight location if authorized personnel do not maintain access control to the location (e.g., unrestricted access to work area where visitors may be received). During non-working hours where internal building security with access control measures are provided, SSI may be filed out of sight with other unclassified material. Where such internal security is not provided, the material should be stored in a locked container such as a desk, file cabinet or in a locked room.

b. Disclose or otherwise provide access to SSI only to "covered persons" who have a "need to know", unless otherwise authorized in writing by the Coast Guard. Mark SSI with the appropriate marking and distribution limitation as specified below.

c. Dispose of SSI as described herein.

d. Ensure records or information containing SSI data is only posted on the Intranet or Internet within a secure socket layer with minimum access and control consisting of a password and username.

e. Industry should review existing records and files that contain information about facility vulnerabilities and for other SSI data and apply the appropriate SSI markings.

f. Unmarked SSI. If a Covered Person receives a record containing SSI that is not marked with the appropriate marking and distribution limitation statement, the Covered Person should:

(1.) Mark the record with the appropriate marking and distribution limitation statement as described herein; and

(2.) Inform the sender of the record that the record must be marked with the appropriate marking and distribution limitation statement as described herein.

g. Tab (A) of this enclosure is provided to assist with quick identification of records that contain SSI; however, its use voluntary.

h. Duty to report unauthorized disclosure. When a Covered Person becomes aware that SSI has been released to unauthorized persons, the Covered Person must promptly inform the local Coast Guard COTP/Federal Maritime Security Coordinator (FMSC).

2. Marking SSI – Documents/Publications.

a. SSI Marking and the Distribution Limitation Statement: The cover page or first page of the document shall prominently display the SSI marking and the distribution limitation statement. Each subsequent page of the document that contains SSI should also display the SSI marking and distribution limitation statement. The SSI marking should be conspicuously placed on the top of the page and the distribution limitation statement on the bottom.

b. SSI Marking: The SSI marking consisting of the words "SENSITIVE SECURITY INFORMATION" must be applied to all documents that contain SSI. This marking should be written or stamped in plain style bold type.

c. The Distribution Limitation Statement: The distribution limitation statement consisting of the words below must be applied to all documents that contain SSI.

"WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER THE PROVISIONS OF 49 CFR 1520. NO PART OF THIS RECORD MAY BE DISCLOSED TO PERSONS WITHOUT A 'NEED TO KNOW" AS DEFINED IN 49 CFR PART 1520, EXCEPT WITH THE WRITTEN PERMISSION OF THE ADMINISTRATOR OF THE TRANSPORTATION SECURITY ADMINISTRATION. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTY OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE IS GOVERNED BY 5 U.S.C. 552 AND 49 CFR PART 1520."

Note: Additionally, covered persons must take all reasonable care to prevent the disclosure of any confidential business information. Graphs, photographs, charts, maps, or other visual media that depict SSI information shall be marked with the SSI marking and the distribution limitation statement to the maximum extent possible.

3. Electronic Media.

a. CD/DVDs: The disk itself must be marked above the title section with the protective marking on the non-optical side of the CDROM or DVD. The distribution limitation statement shall be placed on the inside of the protective sleeve. In all cases, both the SSI marking and Limited Distribution Statement will be shown wherever physically possible on each document contained within the medium.

b. Discs/Portable memory storage devices: SSI contained on electronic and magnetic media must have protective markings and the distribution limitation statement applied at the beginning and end of the electronic and magnetic text. The protective marking and distribution limitation statement must be displayed in such a manner that both are fully visible on the screen or monitor when the text is viewed. The protective marking and distribution limitation statement must also be applied to each side of the disk and the disk sleeve/jacket.

c. Motion Picture Films and Video Recordings:

(1.) SSI Marking and Distribution Limitation Statement. The SSI marking and distribution limitation statement must be applied at the beginning and end of each reel and affixed in such a matter that it is fully visible on the screen or monitor.

(2.) Motion Picture Reels. Motion picture reels that are kept in film cans or other containers must have SSI marking and distribution limitation statements, which must be applied to each side of each reel and to all sides or each can or other storage container.

(3.) Videotape Recordings. Videotape recordings that contain SSI must include on the recordings conspicuous visual protective markings and distribution limitation statements at both the beginning and the end, if practicable. Protective markings and the distribution limitation statement must also be applied on the front and back and on each side of the video case and storage containers.

(4.) Computer Monitors. When viewing SSI material on the computer care must be taken to avoid leaving the material unattended for any length of time to prevent unauthorized viewing.

4. Disclosure of SSI.

a. In general. Except as provided in paragraphs (d) through (h) of this section, and notwithstanding the Freedom of Information Act (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and other laws, records containing SSI are not available for public inspection or copying, nor does the Coast Guard release such records to persons without a "need to know." SSI designated information is not permitted to be distributed outside of the organization (industry or agency) to which it is initially provided and/or identified by the Coast Guard. Exceptions to this are handled on a case-by-case basis and require written approval by Commandant (G-MP) or the FMSC prior to disclosure. SSI should be withheld in response to FOIA and PA requests. Additional guidance is found at 49 CFR § 1520.15.

b. Generally, the Coast Guard will not disclose SSI without having a non-disclosure agreement on record for the covered individual. (*See* enclosure (5) Tab A). One example of an exception to this policy is when the Coast Guard is disclosing SSI to the owner/operator about his/her own vessel/facility. It is assumed that the owner/operator's security interest in this information will be sufficient to prevent unauthorized disclosure.

c. To assist owners and operators with tracking conditional access to SSI, sample non-disclosure agreements suitable for internal company and industry use are provided as enclosure (5) Tab B. Use of the sample non-disclosure agreement is voluntary and owners/operators may utilize alternative means of tracking conditional access to SSI.

d. Non-Disclosure under the Freedom of Information Act and the Privacy Act. If a record contains both SSI and information that is not SSI, the Coast Guard, on a proper Freedom of Information Act or Privacy Act request, may disclose the

record with the SSI redacted, provided the record is not otherwise exempt from disclosure under the Freedom of Information Act or Privacy Act. The redacted SSI material will be withheld pursuant to exemption (b)(3) of the FOIA (5 USC 552(b)(3)) and 49 USC 114(s).

e. Disclosures to committees of Congress and the General Accounting Office. The Coast Guard may disclose SSI to a committee of Congress authorized to have the information or to the Comptroller General, or to any authorized representative of the Comptroller General without a non-disclosure agreement.

f. Disclosure in enforcement proceedings.

(1.) In general. The Coast Guard may provide SSI to a person in the context of an administrative enforcement proceeding when, in the sole discretion of the DHS or the Commandant of the Coast Guard, as appropriate, access to the SSI is necessary for the person to prepare a response to allegations contained in a legal enforcement action document issued by the Coast Guard.

(2.) Obligation to protect information. When an individual receives SSI pursuant to paragraph (f)(1) of this section, that individual becomes a Covered Person and is subject to the obligations of a Covered Person.

g. No release under FOIA. When the Coast Guard discloses SSI, the disclosure is for the sole purpose of conveying SSI to covered person(s) with a need to know. Such disclosure is not a public release of SSI information under the Freedom of Information Act.

h. Disclosure in the interest of safety or security. The Commandant of the Coast Guard may disclose SSI where necessary in the interest of public safety or in furtherance of transportation security. See 49 CFR §1520(c).

5. Consequences of Unauthorized Disclosure of SSI.

a. Violation of 49 CFR Part 1520 pertaining to the protection of sensitive security information, is grounds for a civil penalty under 46 USC 7017 and other enforcement or corrective action by DHS and appropriate personnel actions for Federal employees.

b. Examples of consequences include, but are not limited to: Suspension and Revocation of Merchant Mariner licenses or credentials, or termination of an individual's access to SSI as a Covered Person.

6. Disposing of SSI.

a. DHS. Subject to the requirements of the Federal Records Act (5 U.S.C. 105), including the duty to preserve records containing documentation of a Federal agency's policies, decisions, and essential transactions, DHS destroys SSI when no longer needed to carry out the agency's function. Non-DHS entities will similarly destroy SSI that they maintain when it is no longer required. Approved methods include burning, pulping, shredding, melting, chemical decomposition,

and mutilation. The destruction method should ensure that the SSI cannot be reconstituted or recognized.

b. Other Covered Persons.

(1.) In general. A Covered Person must destroy SSI completely to preclude recognition or reconstruction of the information when the covered person no longer needs the SSI to carry out transportation security measures. Approved methods include burning, pulping, shredding, melting, chemical decomposition, and mutilation.

(2.) Exception. Paragraph (b)(1) of this section does not require a state or local government agency to destroy information that the agency is required to preserve under state or local law.

7. Communicating SSI Material.

a. SSI material is to be disseminated via methods that prevent accidental disclosure. Packaging of SSI material should at a minimum include use of opaque envelopes, wrappings, or cartons.

b. The below methods may be utilized:

(1.) Hard copy dissemination may be accomplished via:

(i.) U.S. Mail or commercial courier service or similar business. Addressing the mail with an attention line containing the name and office of the recipient that is a known covered person helps to ensure that the SSI material is received and opened only by authorized personnel;

(ii.) Inter-office mail; or

(iii.) Hand-carrying within/between buildings.

(2.) Electronic transmission of SSI may be accomplished via:

(i.) Facsimile. The sender must confirm that the facsimile number of the recipient is current and valid and the facsimile machine is in a controlled area where unauthorized persons cannot intercept the SSI facsimile, or the sender must ensure that an authorized recipient is available at the receiving location to promptly retrieve the information. The information to be transmitted must have a cover sheet that clearly identifies the sender's name and telephone number and contains a warning that, if the message is received by other than the intended recipient, the individual receiving the message must immediately notify the sender for disposition instructions.

(ii.) Electronic Mail. SSI may be transmitted as an attachment or within the text of an email if it is being sent within the CG Intranet to a CG email address and the individual is determined to be a "covered person" with a "need to know". If the email is being sent outside of the CG Intranet to any other address, for example ".gov", ".mil", ".com", or ".net", it must be provided within a password protected document. Files that are password protected are considered to meet this requirement. The password may not be contained in the email and must be provided separately to the intended recipient.

(iii.) Telephone. The caller must ensure that the person receiving the SSI is an authorized recipient. Wherever possible, the use of telephones with an unprotected, wireless component should be avoided to reduce the risk of interception and monitoring; however this should not preclude the initiation of immediate action to respond and/or investigate a reported security situation or condition. It is understood that use of unprotected, wireless devices may be required to facilitate this process and are authorized in the facilitation of the response/investigation.

(iv.) Wireless Devices. The risk of monitoring and interception of SSI is greater when using wireless devices. Therefore, cellular phones, pagers, cordless telephones or personal digital assistants (PDA's) should not be used to transmit SSI unless the transmission is encrypted or there is an emergency.

(v.) Internet. Internet posting of SSI is allowed if the posting is within a secure socket layer (SSL) with minimum access controls, consisting of a user name, and password. The Primary Content Approval Official (PCAO), or Webmaster, is responsible to ensure that no documents/databases containing SSI information are released to unauthorized parties. In addition, FMSCs may also require SSI warning banners upon logon; electronically signed non-disclosure agreements at each logon; limited user permissions (based on need-to-know); or limitations on storage of SSI information.

Note: When marking paragraphs that contain both SSI and classified information, the abbreviation (U/SSI) is recommended, e.g.:

1. (S) Pier XX is routinely used for military outloads of munitions for OIF.

2. (U/SSI) Pier XX is guarded only X hours per day by contractors.

3. (S) Waterside patrols will visit Pier XX Y-times per day and conduct shoreside patrols every morning and evening.

SSI CUSTODY, DISSEMINATION, TRANSMISSION, AND STORAGE REQUIREMENTS – QUICK SHEET

Custody	Dissemination and Transmission	Storage
Green cover sheet, enclosure (3) Tab A--optional Non-DHS employees handling SSI material may sign a non-disclosure agreement, which should be filed at the company. Owners/Operators may use other means to track employees authorized access to SSI. Employees who have custody of material designed as SSI shall exercise due caution to ensure that the information is not accessible to individuals who have no need to know. At a minimum, individuals who cannot demonstrate a "need-to-know" must not be able to access areas containing SSI unescorted or unobserved, or have visual access to SSI.	SSI may be transmitted via commercial courier service or USPS mail. SSI may be transmitted via Coast Guard email within the CG Intranet. The Internet is not secure and therefore should not be used to transmit SSI except as provided in paragraph 7b(2)(ii) or (v) of this enclosure. SSI is to be safeguarded and adequately protected from unlawful or improper disclosure. Information that has been identified and is known by the recipient as SSI shall be safeguarded from disclosure to unauthorized individuals whether or not the material is physically marked. Safeguarding from disclosure includes precautions against oral disclosure, prevention of visual access to the information and precautions against release of the material to unauthorized personnel. SSI leaving the control of CG personnel must be properly packaged, sealed and addressed specifically to the recipient with a "need to know". Senders of SSI material are highly encouraged to notify intended recipients of pending delivery. SSI may be discussed on the telephone. Use of voice privacy equipment or secure telephones should be considered depending upon MARSEC level. Generally, SSI should not be transmitted or discussed along **non-secure** pagers, or wireless devices. However, emergency situations or some circumstances may require the use of these devices. SSI may be transmitted via unclassified fax machines. However, the sensitivity of the material will determine the need for more secure transmission (e.g., secure fax).	During non-duty hours, SSI shall be afforded, at a minimum, protection of storage in a locked desk or file cabinet, or storage in a facility or area using physical access control measures that afford adequate protection to prevent unsupervised, unrestricted access by individuals that are not Covered Persons with a need to know the SSI. SSI stored and processed by an IT facility shall have adequate physical, administrative, and technical safeguards.

ENCLOSURE (3) TO NVIC 10 – 04

TAB A

SSI

THIS IS A COVER SHEET

FOR SENSITIVE SECURITY INFORMATION

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR Part 1520, except with the written permission of the Administrator of the Transportation Security Administration. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR Part 1520.

(This cover sheet is unclassified.)

SSI

ENCLOSURE (4) TO NVIC 10 – 04

DEFINITIONS

DEFINITIONS

Administrator: the Under Secretary of Transportation for Security referred to in 49 U.S.C. 114(b), or his or her designee.

Coast Guard: the United States Coast Guard.

Confidential: classified information, the unauthorized disclosure of which reasonably could be expected to cause damage to national security that the original classification authority is able to identify or describe.

Covered person: any organization, entity, individual, or other person described in 49 CFR § 1520.7. In the case of an individual, covered person includes any individual applying for employment in a position that would be a covered person, or in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment. Covered person includes a person applying for certification or other form of approval that, if granted, would make the person a covered person described in 49 CFR § 1520.7.

DHS: the Department of Homeland Security and any directorate, bureau, or other component within the Department of Homeland Security, including the United States Coast Guard.

For Official Use Only (FOUO): Coast Guard originated information that has not been given a security classification pursuant to the criteria of an Executive Order that requires protection against uncontrolled releases.

Maritime facility: any facility as defined in 33 CFR Part 101.

Proprietary Data: includes data received from an organization with instruction to safeguard the material and restrict access to U.S. government personnel only.

Record: includes any means by which information is preserved, irrespective of format, including a book, paper, drawing, map, recording, tape, film, photograph, machine-readable material, and any information stored in an electronic format. The term record also includes any draft, proposed, or recommended change to any record.

Secret: classified information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

Sensitive Security Information: information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would 1) constitute an unwarranted invasion of privacy, 2) reveal trade

secrets or privileged or confidential information obtained from any person, or 3) be detrimental to the security of transportation.

Unclassified: information that is not classified on its own merits. That the information is marked unclassified does not mean it can be automatically released into the public domain. This information may be subject to other controls or distribution limitations.

TSA: the Transportation Security Administration.

ENCLOSURE (5) TO NVIC 10 – 04

TAB A

CONDITIONAL ACCESS TO SENSITIVE BUT UNCLASSIFIED INFORMATION NON-DISCLOSURE AGREEMENT

I, _____ hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain United States Government documents or material containing sensitive but unclassified information.

I understand and agree to the following terms and conditions:

1. By being granted conditional access to sensitive but unclassified information, the United States Government has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement.

2. As used in this Agreement, sensitive but unclassified information is any information which the loss of, misuse of, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Title 5, U.S.C., Section 552a, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

3. I am being granted conditional access contingent upon my execution of this Agreement for the sole purpose of *(identify)*_____.
This approval will permit me conditional access to certain information, e.g., *(circle type(s) of information as appropriate)* documents, memoranda, reports, testimony, deliberations, maps, drawings, schematics, plans, assessments, etc.) and/or to attend meetings where such information is discussed or otherwise made available to me. This Agreement will not allow me access to materials, which the Department of Homeland Security has predetermined, in its sole discretion, are inappropriate for disclosure pursuant to this Agreement. This may include sensitive but unclassified information provided to the Department of Homeland Security by other agencies of the United States Government.

4. I will never divulge any sensitive but unclassified information that is provided to me pursuant to this Agreement to anyone unless I have been advised in writing by the Department of Homeland Security that the individual is authorized to receive it. Should I desire to make use of any sensitive but unclassified information, I will do so in accordance with paragraph 6 of this Agreement. I will submit to the Department of Homeland Security for security review, prior to any submission for publication, any book, article, column or other written work for general publication that is based upon any knowledge I obtained during the course of my work on *(identify)* _____
in order for the Dept. of Homeland Security to ensure that no sensitive but unclassified information is disclosed.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of sensitive but unclassified information not consistent with the terms of this Agreement.

6. I hereby agree that when reviewing any official documents containing sensitive but unclassified information, such review will be conducted at a secure facility or under circumstances that will maintain the security protection of such material. I will not be permitted to and will not make any copies of documents or parts of documents to which conditional access is granted to me. Any notes taken during the course of such access will remain at the Department of Homeland Security, to be placed in secure storage unless it is determined by the Department of Homeland Security that the notes contain no sensitive but unclassified information. If I wish to have the notes released to me, Department of Homeland Security officials will review the notes for the purposes of deleting any sensitive but unclassified information to create a redacted copy of the notes. If I do not wish a review of any notes that I make, those notes will remain sealed in secure storage at the Department of Homeland Security.

7. If I violate the terms and conditions of this Agreement, I understand that the unauthorized disclosure of sensitive but unclassified information could compromise the security to the Department of Homeland Security.

8. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to sensitive but unclassified information. This may serve as a basis for denying me

conditional access to Department of Homeland Security information, both classified and sensitive but unclassified information in the future. If I violate the terms and conditions of this Agreement, the United States may institute a civil action for damages or any other appropriate relief. The willful disclosure of information to which I have agreed therein not to divulge may constitute a criminal offense.

9. Until I am provided a written release by the Dept. of Homeland Security from this Agreement or any portions of it, all conditions and obligations contained in this Agreement apply both during my period of conditional access, which shall terminate at the conclusion of my *(identify)*_____, and at all times thereafter.

10. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions shall remain in full force and effect.

11. I understand that the United States Government may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

12. By granting me conditional access to information in this context, the United States Government does not waive any statutory or common law evidentiary privileges or protections that it may assert in any administrative or court proceeding to protect any sensitive but unclassified information to which I have been given conditional access under the terms of this Agreement

13. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302 (b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that my compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

14. My execution of this Agreement shall not nullify or effect in any manner any other secrecy or nondisclosure Agreement which I have executed or may execute with the United States Government.

15. I make this Agreement in good faith, without mental reservation or purpose of evasion.

_____ _____

DATE NAME *(Last, First, Middle I.)*

This Agreement was accepted by the undersigned on behalf of the Department of Homeland Security as a prior condition of conditional access to sensitive but unclassified information.

_____ _____

DATE WITNESSED BY - Department of Homeland Security

This form is not subject to the requirements of P. L. 104-13, "Paperwork Reduction Act of 1995" 44 USC, Chapter 35.

ENCLOSURE (5) TO NVIC 10 – 04

TAB B

Non-Disclosure Agreement (employee/contractor)

Conditional Access to Sensitive Security Information

I, _____, as an officer or employee of _____ [***name of company***] (hereafter, the Company), hereby consent to the terms and conditions of this Non-Disclosure Agreement (hereafter, Agreement) in consideration of my being granted conditional access to certain United States Government documents or other material containing sensitive security information (hereafter, SSI).

I understand and agree to the following terms and conditions:

1. By being granted conditional access to SSI, special confidence and trust has been placed in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement and all applicable laws.

2. As used in this Agreement, SSI is that information defined in 49 CFR Part 1520 but also includes any information not specifically mentioned in Part 1520, but marked as "sensitive security information" or "SSI."

3. Based on the United States Coast Guard (hereafter, USCG) and/or the Company determination that I have a security-related need to know, I am being granted conditional access to SSI contingent upon my execution of this Agreement for the sole purpose of ***[insert purpose of disclosure;,/or*** **contracts, insert** ***"performing work under Contract No. _____ (hereafter, Contract)"].*** This approval will permit me to have conditional access to certain SSI, including but not limited to, ***[if possible, insert specific description*** **of SSI to** ***be disclosed, such as model algorithms, intelligence ratings, threat scenarios, and model output data,"]***, and/or to attend meetings in which such information is discussed or otherwise made available to me. This Agreement will not allow me to have access to materials that the USCG or the Company have determined, in its sole discretion, are inappropriate for disclosure pursuant to this Agreement. This may include sensitive but unclassified information provided to the USCG by other agencies of the United States Government, or any other SSI that I do not have a security-related need to know.

4. I will disclose SSI that is provided to me pursuant to this Agreement only to other officers or employees of the Company who have a security-related need to know and who have signed a non-disclosure agreement with the USCG. I will never divulge to anyone outside of the Company, or to anyone employed by the Company who does not have a security-related need to know, SSI that is provided to me.

5. If I become aware or have reason to believe that SSI may have been released to any unauthorized person, I will immediately notify the USCG.

6. I understand that the unauthorized disclosure of SSI could compromise the safety and security of transportation.

7. If I violate the terms or conditions of this Agreement, such violation may result in the cancellation of my conditional access to SSI. This may serve as a basis for denying me conditional access to other United States Government information, both classified and sensitive, in the future. If I violate the terms or conditions of this Agreement, the United States may institute a civil penalty against me pursuant to 49 U.S.C. 46301 and 49 CFR Part 1520 or take other enforcement or corrective action.

8. Unless and until I am provided a written release by the USCG from this Agreement or any portion of it, all conditions and obligations contained in this Agreement shall apply both during my period of conditional access, ***(which shall terminate at the conclusion of my work under this Contract)***, and at all times thereafter.

9. Each provision of this Agreement is severable. If any administrative or judicial tribunal should find any provision of this Agreement to be unenforceable, all other provisions shall remain in full force and effect.

10. I understand that the United States Government may seek any remedy available to it to enforce this Agreement, including but not limited to application for a court order prohibiting disclosure of information in breach of this Agreement, imposition of civil penalties, and any other enforcement or corrective action.

11. By granting me conditional access to information in this context, the United States Government does not waive any statutory or common law evidentiary privileges or protections that it may assert in any administrative or judicial proceeding to protect any SSI to which I have been given conditional access under the terms of this Agreement.

12. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), and other statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and supersede this Agreement to the extent of any conflict.

13. My execution of this Agreement shall not nullify or affect in any manner any other secrecy or nondisclosure Agreement which I have executed or may execute with the United States Government.

14. I make this Agreement in good faith, without mental reservation or purpose of evasion.

Signature _____ Date _____

Name _____ Title _____