

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 22202



**Transportation
Security
Administration**

FEB 20 2004

RADM Larry Hereth
c/o Commandant (G-MP)
United States Coast Guard
2100 2nd Street, SW, Room 2406
Washington, DC 20593-0001

Reference: (a) TSA letter to USCG (G-MP) dated December 12, 2003

Dear Admiral Hereth:

Reference (a) provided authority for Coast Guard to designate certain categories of information as Sensitive Security Information (SSI).

As requested in our staff's phone conversation of January 30, 2004, I have determined that categories of information and records detailed in enclosure (1) constitute Sensitive Security Information (SSI). In the interest of ensuring consistent guidelines on the use and handling of SSI, enclosure (2) is emphasized.

If you have any questions, please feel free to contact Paul Hankins at 571-227-1247.

Yours truly,

A handwritten signature in cursive script, appearing to read "Chet Lunner".

Chet Lunner
Assistant Administrator
Office of Maritime & Land Security

Enclosure: (1) Designation of Sensitive Security Information
(2) Interim Sensitive Security Information (SSI) Policies and Procedures for
Safeguarding and Control

Designation of Sensitive Security Information

Background

On November 25, 2002, the President signed into law the Maritime Transportation Security Act (MTSA), which established a new framework for maritime security, to be administered largely by the Secretary of the Department of Homeland Security (DHS), including through TSA, the Coast Guard, and the Bureau of Customs and Border Protection, along with the Maritime Administration of the Department of Transportation.

Primary elements of this framework are national, area, port, and facility and vessel security plans to be approved or required by DHS. Specifically, under the MTSA the Secretary of DHS must prepare a National Maritime Transportation Security Plan, which, in turn, will identify areas of the country for which DHS will adopt Area Maritime Security Plans. Section 70103 of MTSA also directs the Secretary of DHS to prescribe regulations requiring certain classes of vessels and maritime facilities to adopt plans for deterring a transportation security incident. 46 U.S.C. 70103(a).

The Coast Guard issued final rules on October 22, 2003, that require vessel and maritime facility operators to prepare security plans for Coast Guard approval. These types of documents are subject to the disclosure limitations of TSA's SSI regulation pursuant to the designation in reference (a).

Enforcement of these security plans is required by law. Instances of non-compliance with security requirements reveal vulnerabilities that can be exploited to the detriment of security and for that reason investigations and findings associated with these enforcement actions must be protected as SSI.

Pending amendment to TSA's SSI regulation to cover maritime security information, there is an immediate need to expand the existing legal protections governing SSI to maritime security, to the maximum extent possible under current regulation.

Under 49 U.S.C. 114(s) and 49 CFR 1520.7(k), TSA may designate as SSI any information obtained or developed in carrying out security that would be detrimental to the security of transportation if it were disclosed. The Coast Guard has requested that TSA designate the following information and records as SSI:

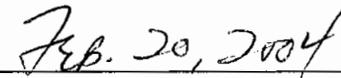
- (1) Details of any security inspection or investigation of an alleged violation of maritime transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit.

Designation

Accordingly, in the interest of transportation security, I have determined that the foregoing categories of information and records containing such information constitute Sensitive Security Information under 49 U.S.C. 114(s) and 49 CFR 1520.7(k).



Chet Lunner
Assistant Administrator
Office of Maritime and Land Security



Date