

January 17, 2003

Summary of New and Existing Port Facility Security Legislation

James W. Conrad, Jr.
American Chemistry Council

On November 25, 2002, President Bush signed the Maritime Transportation Security Act of 2002, Pub. L. No. 107-295 (MTSA). The new law creates a comprehensive port security program overseen by the Secretary of the Department of Homeland Security (but likely to be delegated within the DHS primarily to the Coast Guard). Because the legislation addresses facility vulnerability assessments, security planning and implementation of security measures, ACC member facilities subject to it will have to take many of the same steps that are required by the Responsible Care Security Code, or that would have been mandated under chemical security legislation considered (but not adopted) by the 107th Congress. The precise requirements of the law, particularly which facilities it covers, will be determined by a Coast Guard rule set to emerge in June 2003.

This memo first discusses those aspects of U.S. law affecting port facility security as they existed prior to enactment of the MTSA. It also notes recent security amendments added to the international Safety of Life at Sea (SOLAS) Convention, which the Coast Guard is implementing in parallel with the MTSA. It then summarizes the MTSA's provisions affecting facilities, focusing on the sequence of implementation and questions that need to be answered.

I. Backdrop: Related Law

A. The Magnuson Act

1. Legal authority

The Coast Guard has had authority since 1917 to take actions, pursuant to rules issued by the President, to safeguard vessels, harbors, ports and "waterfront facilities" against "destruction, loss, or injury from sabotage or other subversive acts, accidents or other causes of similar nature" ¹ Under this law, known as the "Magnuson Act," the President has issued regulations regarding the security of vessels, harbors and waterfront facilities,² and the Coast Guard has established security zones at specified ports and around certain vessels.³ These regulations authorize a Coast Guard Captain of the Port (COTP) to issue an order "whenever it appears to him that such action is

¹ 50 U.S.C. § 191(b). The statute also authorizes the Coast Guard to take actions regarding *vessels* as necessary "to secure the observance of rights and obligations of the United States." *Id.* § 191(a). For decades, however, the Coast Guard and its rules have read these two subsections together, so that the Coast Guard also asserts the power to take actions with respect to *waterfront facilities* as needed to secure treaty rights and obligations. *See* 33 C.F.R. § 6.04-5.

² 33 C.F.R. Part 6.

³ *Id.* § 165.30. For example, the Houston Ship Channel is covered by *id.* § 165.T08-050.

necessary in order to . . . prevent damage or injury to any . . . waterfront facility” located in that port.⁴

2. Applicability

The coverage of the Magnuson Act depends on two issues: what is a “waterfront facility,” and how far “upstream” does this authority extend?

As to the first issue, the Magnuson Act does not define “waterfront facility,” but the Coast Guard’s rules do:

Waterfront facility, as used in this part, means all piers, wharves, docks, or similar structures to which vessels may be secured and naval yards, stations, and installations, including ranges; areas of land, water, or land and water under and in immediate proximity to them; buildings on them or contiguous to them and equipment and materials on or in them.⁵

This authority would thus apply to at least some part of any ACC member facility that has a pier or similar structure to which a vessel could be secured. The important question is *how much* of the facility would be included in the “areas of land . . . in immediate proximity . . . or contiguous to [such structures].” Coast Guard practice in most cases under the Magnuson Act has been to limit coverage only areas directly connected to the pier or dock (sometimes referred to as “marine transfer areas”). For example, at a bulk liquid natural gas facility, Coast Guard jurisdiction would end at the last valve before the tank that receives the LNG coming off a ship.⁶ Unlike many EPA definitions of “facility,”⁷ therefore, the Coast Guard has only occasionally used its jurisdiction over docks and piers to regulate the entire piece of contiguous property under common ownership.

As for the “upstream” issue, the Magnuson Act definition seems to be limited to bodies of water that are navigable in fact by “vessels,” rather than the more expansive notion of “navigable waters,” used in many other statutes, that does not require a body of water to be physically navigable.⁸ Coast Guard practice under the Act apparently has followed the narrower, navigable-in-fact approach.

⁴ *Id.* § 6.04-5.

⁵ *Id.* § 6.01-4.

⁶ U.S. Coast Guard, *Marine Safety Manual*, vol. II, sec. B, ch. 7, at B7-6 (May 21, 2000).

⁷ *See, e.g.*, 40 C.F.R. § 122.2 (“‘facility’ . . . means any NPDES ‘point source’ or any other facility or activity (including land and appurtenances thereto) that is subject to regulation under the NPDES program.”).

⁸ For example, the Clean Water Act says “[t]he term ‘navigable waters’ means the waters of the United States . . .” 33 U.S.C. § 1362(7). This term has been read to include irrigation canals that are hydraulically connected with streams or lakes. *See Headwaters Inc. v. Talent Irrigation District*, 243 F.3d 526 (9th Cir. 2001). Recently, the Supreme Court held that “isolated ponds” are not included. *Solid Waste Agency of Northern Cook County v. U.S. Army Corps of Engineers*, 531 U.S. 159 (2001).

B. The Ports and Waterways Safety Act

Since 1986, the Secretary of the department where the Coast Guard is housed has also had the power, under the Ports and Waterways Safety Act (PWSA), to require “commercial structures” within or adjacent to the “marine environment” (essentially, everything except small, isolated wetlands) to establish security zones and to develop contingency plans and procedures to prevent and respond to acts of terrorism.⁹ The scope of this law – on its face, anyway -- is thus much broader than the Magnuson Act: it does not refer to piers or wharves, and indeed does not refer to vessels. Coast Guard inspection guidance, however, suggests that the Coast Guard has generally not implemented its regulatory powers under the PWSA any more broadly than under the Magnuson Act.¹⁰

C. The SOLAS Convention

In December 2002, the International Maritime Organization (IMO), which includes the United States, adopted new security amendments to the Convention for the Safety of Life at Sea (SOLAS), including a new International Ship and Port Facility Security (ISPS) Code. The SOLAS amendments enter into force on July 1, 2004. The Coast Guard just published a Federal Register notice containing the amendments and the ISPS Code and explaining the Coast Guard’s intent to implement them and the MTSA in an integrated fashion.¹¹ The SOLAS amendments address “port facilities,” which are locations determined by the relevant nation “where the ship/port interface takes place.” Hence SOLAS and the ISPS Code would apply to generally the same sorts of facilities covered by the Magnuson Act and the NVIC, and potentially other facilities within ports.

⁹ See 33 U.S.C. § 1226 (authority of dep’t), § 1222(1) (defining “marine environment” as “navigable waters,” discussed in footnote 8 above). The Supreme Court has repeatedly held that the PWSA and related enactments that address maritime security preempt state requirements. In some cases, this preemption is limited to circumstances where the state requirements conflict with the federal ones; in other cases it extends to any state requirements addressing an issue dealt with by federal rules. See *United States v. Locke*, 529 U.S. 89 (2000) (referred to as the “Intertanko” case). The MTSA can reasonably be expected to have at least conflict preemption power, since it is, in practical effect, an extension of the powers already given to the Coast Guard by the PWSA. It is also quite possible that MTSA rules or directives that relate to the hazardousness of particular materials would preempt conflicting state or local requirements by operation of Section 1711(b) of the Homeland Security Act of 2002 (Pub. L. No. 107-296). While that provision is technically an amendment to the Hazardous Materials Transportation Act, the preemptive effect of the resulting language is not limited to the HMTA, but instead applies to any state, local or tribal requirement that conflicts with “a hazardous materials transportation security regulation or directive issued by the Secretary of Homeland Security.” See 49 U.S.C. § 5125(a), as amended. The Coast Guard typically defines the applicability of its facility safety and security requirements by the type of cargo handled at the facility, suggesting that HMTA/HSA preemption would apply.

¹⁰ *Marine Safety Manual*, *supra* note 6, at B7-4. In some cases, e.g., nuclear power plants adjacent to the ocean, the Coast Guard has used its Magnuson Act and PWSA authorities to circumscribe an entire parcel of property. See, e.g., 33 C.F.R. § 165.115.

¹¹ 67 Fed. Reg. 79742 (Dec. 30, 2002).

II. The Maritime Transportation Security Act of 2002

The Coast Guard must now integrate the authorities just discussed with a new one, the MTSA.¹² As discussed more fully below, the Coast Guard intends to issue an interim rule implementing the MTSA by June 2003 and must issue a final rule by November 2003. Some indication of what those rules will provide is given by a brand new Navigation and Vessel Inspection Circular (NVIC) under the Magnuson Act and the PWSA entitled “Recommended Security Guidelines for Facilities.”¹³

A. Scope

Rather than speak of “waterfront facilities,” the MTSA applies simply to “facilities,” which are defined as “any structure or facility of any kind located in, on, under or adjacent to any waters subject to the jurisdiction of the United States.”¹⁴ On its face, this definition is very broad. It makes no references to docks, piers or wharves. It also is not limited to facilities located in “ports.” Given the breadth of U.S. jurisdiction over surface waters, this definition would seem to apply to any chemical facility that is adjacent to any body of water that affects interstate commerce. This would likely include any body of water that connects hydrologically to water that is navigable (e.g., tributaries of tributaries of navigable rivers).¹⁵ The new NVIC supports this interpretation:

[The MTSA definition of facility] indicates the clear intent that Coast Guard maritime security regulations should be aligned with our broader authority under the Ports and Waterways Safety Act . . . related to any public or commercial structure located on or adjacent to the marine environment, rather than our traditional approach of focusing on installations and terminals that have accommodations for vessels.¹⁶

While the issue is less clear, the use of the phrase “facility” without limitation to “waterfront” or to structures like docks suggests that Congress also intends the definition to apply to the entire property that is adjacent to the water. The new NVIC discusses this issue in some detail, providing that the boundary of a facility that handles regulated cargos should encompass the entire area where the cargo “is stored, handled

¹² The MTSA does not amend either the Magnuson Act or the PWSA, except to insert language in two parts of the MTSA to clarify that “the safety and security of United States ports and waterways” is of national importance and a factor to be considered by the Secretary of DHS in implementing the law. MTSA § 443. This change seems intended not to make any substantive change, but only to conform the “motherhood” portions of the PWSA to the preexisting PWSA section (33 U.S.C. § 1226) that already addresses port and waterway security.

¹³ NVIC No. 11-02 (January 13, 2002) (www.uscg.mil/hq/g-m/nvic/11-02.pdf).

¹⁴ Section 102 of the MTSA adds a new Chapter 701, entitled “Port Security,” to the “Shipping” title of the U.S. Code (title 46). Subsequent references are to sections in that chapter. The definition of “facility,” for example, is § 70101(2).

¹⁵ See footnote 8 above.

¹⁶ NVIC No. 11-02, at 2.

or processed.”¹⁷ Notably, this includes facilities that do not receive vessels.¹⁸ For a chemical manufacturing plant, this could involve all process and product area; i.e., everything except office and parking space. The NVIC also states that a facility owner or operator may declare the entire facility to be a restricted area, so long as it maintains an appropriate level of security for the entire facility.¹⁹

As noted earlier, the SOLAS Convention applies only to facilities where a ship/shore interface occurs. In its Federal Register notice on the integration of the MTSA and SOLAS, however, the Coast Guard states that it considers facility security requirements to be appropriate not just for those covered by SOLAS, but for other facilities “that are on or adjacent to U.S. waters and pose a risk to them.”²⁰ The language of the MTSA certainly supports a broad scope that would include the entire boundaries of any facility that abuts a waterway subject to interstate commerce. In the current, unsettled security situation, such a more comprehensive scope is arguably more precautionary and conservative. It ensures that more, rather than fewer facilities will be subject to federal government oversight, and that hazardous materials at a facility will be included regardless of where on the site they are located.

B. Facility Assessments and Plans

The MTSA imposes numerous obligations on the Coast Guard and facilities to improve facility security:

1. Vulnerability assessments

The Coast Guard has to do a two-level, national assessment:

Initial assessment -- First, it must conduct an initial assessment to identify which facilities on or adjacent to waters subject to U.S. jurisdiction “pose a high risk” of being involved in a “transportation security incident” – i.e., “a security incident resulting in a significant loss of life, environmental damages, transportation system disruption or economic disruption in a particular area.”²¹ Again, this requirement is not limited to facilities located in “ports,” but sweeps more broadly.²² Equally important, the definition of “transportation security incident” makes clear that the incident need not arise from, or have adverse consequences for, transportation. It merely needs to be a security incident at a facility subject to the legislation.

¹⁷ *Id.*, Enclosure 1 at 3.

¹⁸ *Id.*

¹⁹ *Id.*, Enclosure 1 at 5.

²⁰ 67 Fed. Reg. 79745.

²¹ §§ 70102(a), 70101(6). This section of the law refers to “United States” facilities. From the context of the law, this reference seems clearly to mean “subject to U.S. jurisdiction,” as opposed to “owned or operated by the U.S. government.”

²² Elsewhere, the law refers to “port vulnerability assessments” (e.g., § 70103(d)(1)), but this appears to be a carryover from the original House and Senate bills, both of which used this phrase. The section of the MTSA addressing vulnerability assessments never uses the word “port.”

Detailed assessments -- Based on the initial assessment, the Coast Guard must conduct a detailed vulnerability assessment of facilities that “may be” involved in a transportation security incident (presumably these are the “high risk” facilities identified in the initial assessment, but the law does not explicitly say so). The detailed assessments must address:

- Critical assets and infrastructures;
- Threats to the same; and
- Weaknesses in physical security, passenger and cargo security, structural integrity, protection systems, procedural policies, communication systems, transportation infrastructure, utilities, contingency response, and other areas as determined by the Coast Guard.²³

The detailed assessment must be provided to the facility owner or operator.²⁴

The law does not set a deadline for completion of the assessments, though it says they must be updated every five years.²⁵ As discussed below, however, the facilities that have to do security plans are the ones subject to the *detailed* assessments. Thus, it would seem that the Coast Guard ought to have completed the detailed assessment before facilities have to submit plans. If so, these assessments will have to proceed on a very fast track.

While the assessment section of the MTSA does not expressly authorize the Coast Guard to require facilities to conduct vulnerability assessments, the Coast Guard probably has that power under other provisions of law,²⁶ and the MTSA does permit it to accept assessments conducted by facilities that meet the requirements for Coast Guard assessments.²⁷ Indeed, the Federal Register notice and the NVIC indicate that the Coast Guard intends for facilities to conduct assessments.²⁸

2. National and area security plans

National plan -- The Coast Guard is also required to develop an umbrella National Maritime Transportation Security Plan that largely addresses federal preparedness and coordination to deter and minimize damage from transportation security incidents.²⁹ The plan must identify areas of the United States that will be (i) overseen by Coast Guard officials acting as Federal Maritime Security Coordinators for those areas and (ii) covered by Area Maritime Transportation Security Plans.³⁰ (These areas will be the same as those currently covered by port security plans, and the federal coordinators will

²³ § 70102(b)(1).

²⁴ § 70102(b)(2).

²⁵ § 70102(b)(3).

²⁶ The MTSA authorizes the Coast Guard to order a facility to take “any necessary interim security measures” until its facility security plan is approved.” See part II.C.1 of this memo. Conceivably, this power could include ordering a facility to conduct a vulnerability assessment. Also, the Coast Guard likely has that power under the Magnuson Act and the PWSA.

²⁷ § 70102(b)(4).

²⁸ 67 Fed. Reg. 79749; NVIC No. 11-02, Enclosure 1, at 7-9.

²⁹ § 70103(a).

³⁰ § 70103(a)(2).

be the relevant COTPs.³¹) Facility owners and operators can only learn of provisions of the national plan to the extent that the Coast Guard considers it necessary for security purposes.³² The law sets no deadline for issuance of the national plan. While the national plan must include “a risk-based system for evaluating the potential for violations of security zones,”³³ the law does not link the national plan to the vulnerability assessments discussed earlier, so the two may be able to proceed in parallel.

Area plans -- Once the area coordinators have been designated, they must develop Area Maritime Transportation Security Plans.³⁴ Area coordinators must also consult with Area Security Advisory Committees that the Secretary of DHS may establish.³⁵ Area plans must describe the infrastructure within the area, be coordinated with the national plan and with facility plans discussed below, and “be adequate to deter a transportation security incident to the maximum extent practicable.”³⁶ Within security zones established in an area, the Coast Guard must consider the use of public/private partnerships to enforce security.³⁷ The Secretary of DHS must approve area plans.³⁸

3. Temporary interim rule

“As soon as practicable” after enactment of the MTSA, the Coast Guard is to publish a temporary, interim final rule regarding implementation of the MTSA.³⁹ Among other things, that rule will establish requirements for facility-level security plans to be submitted to the Coast Guard. The Administrative Procedure Act (APA) will not apply to this rule, but the Coast Guard will have to propose and finalize a substitute rule under the APA by November 25, 2003 because the temporary rule will expire on that date.⁴⁰ According to the Federal Register notice, the Coast Guard intends to publish the interim rule by June 2003 and the final rule by November 2003.⁴¹

4. Facility security plans

Six months after the Coast Guard’s temporary interim rule has been issued, facilities that the Coast Guard believes “may be involved” in a transportation security incident must submit to the Secretary a plan “for deterring a transportation security incident to the maximum extent practicable.”⁴²

³¹ 67 Fed. Reg. 79744.

³² § 70103(a)(5).

³³ § 70103(a)(2)(H).

³⁴ § 70103(b)(1)(A).

³⁵ § 70103(b)(1)(B).

³⁶ § 70103(b)(2).

³⁷ § 70103(b)(4).

³⁸ § 70103(b)(3)(A).

³⁹ MTSA § 102(d)(1).

⁴⁰ MTSA § 102(d)(1), (2).

⁴¹ 67 Fed. Reg. 79744.

⁴² § 70103(c)(1).

Vulnerability assessments – As noted earlier, while the Coast Guard, rather than facilities, is required to conduct initial and detailed vulnerability assessments, the Coast Guard has already signaled its intent to require covered facilities to conduct the detailed assessments.⁴³ The facilities that must prepare security plans are same ones that must be covered in the detailed assessments.⁴⁴ Thus, it will be crucial for the Coast Guard to make it clear which facilities are covered by this obligation.

Provisions -- Facility plans must:

1. Be consistent with the national and area security plans (this would seem to require the latter to be completed first, but this is not clearly stated);
2. Identify qualified and accountable individuals to oversee security actions;
3. Include provisions for:
 - a. Physical, cargo and personnel security;
 - b. Access control to “secure areas”;⁴⁵
 - c. Procedural security policies;
 - d. Communications systems; and
 - e. Other security systems.
4. Identify, and ensure by contract or other means approved by the Coast Guard, the availability of security measures necessary to deter, to the maximum extent practicable, a transportation security incident or a substantial threat of the same; and
5. Describe training, periodic unannounced drills and other security actions.⁴⁶

These elements are generally consistent with the NVIC, except that the NVIC refers simply to “prevent[ing] and deter[ring] transportation security incidents.”⁴⁷ It remains to be seen whether the statute’s “deter, to the maximum extent practicable” language will result in different language being included in the MTSA regulations.

Under the NVIC, facility security plans are intended to contain increased measures keyed to the national system of threat levels (renamed Maritime Security (or MARSEC) levels).⁴⁸ The preventive security measures discussed in the NVIC are entirely related to reducing vulnerability via deterrence; there is no mention of eliminating or mitigating consequences (e.g., by not handling high consequence cargoes anymore). Plans must also include response and evacuation procedures.⁴⁹

⁴³ See footnote 28 *supra*.

⁴⁴ Both sections of the law speak of facilities that “may be involved” in a transportation security incident. See §§ 70102(b), 70103(c)(2)(A).

⁴⁵ The House Report states:

The number and scope of secure areas in a facility may vary depending upon the type of facility in question. For example, the entire facility at an oil terminal may be a secure area. In contrast, the Secretary may decide that only the areas at a container terminal where individuals have access to open containers or container manifests are secure areas.

H.R. Rep. No. 405, 107th Cong., 2d Sess. 12 (2002).

⁴⁶ § 70103(c)(3).

⁴⁷ NVIC No. 11-02, Enclosure 1 at 9.

⁴⁸ NVIC No. 11-02 at 4.

⁴⁹ *Id.*, Enclosure 1 at 10.

Updating -- Plans must be updated and resubmitted every five years or whenever a facility change occurs that may substantially affect facility security.⁵⁰ The Coast Guard must promptly approve each plan or require amendments.⁵¹

Facility shut down -- One year after the interim regulations are issued, a facility may not operate unless its plan has been approved and it is operating consistently with it.⁵² The Coast Guard may grant a facility a 1-year extension from the time it submits its plan if the facility certifies that it has ensured, by contract or other means approved by the Coast Guard, the availability of security measures necessary to deter, to the maximum extent practicable, a transportation security incident or a substantial threat of the same.⁵³

Procedures for accepting alternatives, equivalencies and industry standards. The Federal Register notice and the NVIC make clear that the Coast Guard intends to allow facilities to comply with their assessment and planning obligations through alternative methods that would provide an equivalent level of security.⁵⁴ The Federal Register notice also says the Coast Guard is considering incorporating industry security standards by reference, and may adopt an alternative mechanism to Coast Guard review and approval.⁵⁵ These provisions indicate an opportunity for facilities implementing the Responsible Care Security Code or similar standards to demonstrate compliance through those mechanisms. Elsewhere, the notice suggests that a process of equivalency that does not include Coast Guard review may have to include third party audits.⁵⁶

C. Other Coast Guard/DHS Authorities and Obligations

1. Interim measures orders

The Coast Guard may order a facility to implement any necessary security measures until its facility security plan is approved.⁵⁷

⁵⁰ § 70103(c)(3)(F), (G).

⁵¹ § 70103(c)(4).

⁵² § 70103(c)(5).

⁵³ § 70103(c)(6). For whatever help it is, the Conference Report says:

The Conferees urge the Secretary to review and approve the vessel and facility security plans in a timely manner. Vessel and facility owners should not be required to cease their operations due to the failure of the Secretary to approve the vessel or facility transportation security plans in a reasonable time period.

H.R. Conf. Rep. No. 777, 107th Cong., 2d Sess. 80 (2002).

⁵⁴ 67 Fed. Reg. 79746; NVIC No. 11-02 at 3.

⁵⁵ 67 Fed. Reg. 79749; *see also* NVIC No. 11-02, Enclosure 1, at 7.

⁵⁶ 67 Fed. Reg. 79746.

⁵⁷ § 70103(c)(7).

2. Incident response plans

By April 1, 2003, the Coast Guard must establish security incident response plans for the facilities that are covered by the detailed vulnerability assessments and required to submit facility security plans. Facility plans may include this response plan.⁵⁸ The Conference Report makes clear the conferees' view that "antiterrorism response [is] the responsibility of local, state and Federal law enforcement agencies."⁵⁹

3. Biometric security cards/background checks

The Secretary of Homeland Security must issue rules requiring individuals to be prohibited from entering "secure areas" at facilities unless they (i) hold biometric transportation security cards issued by the Secretary and (ii) are authorized by the facility plan to enter the area or (iii) are accompanied by someone else who meets the first two requirements.⁶⁰ (This responsibility will likely be delegated to the Transportation Security Administration.) The law lists the classes of individuals that may be eligible to obtain these cards,⁶¹ as well as the grounds under which the Secretary may deny issuance of the cards.⁶² The Secretary must establish an administrative appeal process for persons denied cards.⁶³

The law also requires the Justice Department, upon request of the Secretary, to conduct background checks of persons seeking cards, looking at relevant criminal history, immigration status, relevant international databases and "any other national security-related information or database" identified by the DOJ.⁶⁴ Information gathered by the DOJ or the Secretary in this connection may not be made available to any member of the public, including the person's employer, who may only be informed of whether or not a card was issued.⁶⁵

4. Maritime safety and security teams

The Coast Guard is instructed to establish such teams as are needed to protect ports, vessels, facilities, etc. from terrorist attacks and to respond to them in accordance with the response plans discussed above.⁶⁶ Among their roles is assisting with facility vulnerability assessments.⁶⁷

⁵⁸ §§ 70104, M TSA § 102(c).

⁵⁹ Conference Report, *supra* note 53, at 80.

⁶⁰ § 70105(a).

⁶¹ § 70105(b).

⁶² § 70105(c)(1), (2).

⁶³ § 70105(c)(3).

⁶⁴ § 70103(d).

⁶⁵ § 70103(e).

⁶⁶ § 70106(a).

⁶⁷ § 70106(c).

5. Maritime Security Advisory Committees

The Secretary of Homeland Security must appoint a national advisory committee that it may consult with on national maritime security matters, and may establish area security committees for one or more ports.⁶⁸ The area committees may review proposed area security plans.⁶⁹ The law does not require committee members to be drawn from particular constituencies, although they must have at least five years of practical experience in maritime security operations.⁷⁰ The Federal Advisory Committee Act applies to the national committee but does not apply to the area committees.⁷¹

D. Information Security

The MTSA provides that, notwithstanding any other law (e.g., FOIA), information developed under its security provisions is not required to be disclosed to the public. This includes vulnerability assessments and facility security plans, and “other information related to security plans, procedures or programs for . . . facilities authorized under [these provisions].”⁷² There are no penalties for disclosure of this information, and the law would appear to give the Coast Guard or other federal agencies the discretion to do so. Indeed, the Conference Report clarifies that the Coast Guard may give security plans and vulnerability assessments to the facilities that are the subjects of them.⁷³ The law also does not preempt state open records laws or create liability protection for such information. The Federal Register notice indicates that the Coast Guard intends to treat port, vessel and facility security information as “Security Sensitive Information” under Transportation Security Administration regulations.⁷⁴

E. Civil Penalties

Any person who violates the port security provisions of the MTSA or the Coast Guard rules implementing it is subject to a civil penalty of up to \$25,000 per violation.⁷⁵

F. Grants

The Maritime Administration of the Transportation Department is authorized to issue grants for enhanced facility security for the current and next five fiscal years. Grants must be “equitably allocated” among facility operators, port authorities, and state and local agencies required to provide security services under area security plans.⁷⁶ Eligible costs are the following, if required by the Coast Guard to correct vulnerabilities and ensure compliance with area and facility plans:

⁶⁸ § 70112(a).

⁶⁹ § 70112(a)(2)(A)(ii).

⁷⁰ § 70112(b).

⁷¹ § 70112(g).

⁷² § 70103(d).

⁷³ Conference Report, *supra* note 53, at 80.

⁷⁴ 67 Fed. Reg. 79746, referring to 49 C.F.R. part 1520.

⁷⁵ § 70117.

⁷⁶ § 70107(a).

- Personnel costs;
- Security equipment or facilities;
- Screening equipment; and
- Conducting vulnerability assessments.⁷⁷

The Conference Report states that costs incurred since 9/11 are eligible.⁷⁸ Grant recipients must supply at least 25% of costs for any project over \$25,000, unless the DOT concludes that a greater federal share is needed for the project to be undertaken.⁷⁹ The DOT must submit a funding proposal to Congress by May 25, 2003 for the grant program and other maritime security programs.⁸⁰ There is no limit to the authorization for this program.

DOT is also authorized to establish a grants program, with up to \$15 million/year for the same six years, for national labs, nonprofit organizations and academic institutions to support research and development of inspection, detection, tracking and monitoring technologies.⁸¹

⁷⁷ § 70107(b).

⁷⁸ Conference Report, *supra* note 53, at 81.

⁷⁹ § 70107(c).

⁸⁰ § 70107(g). Congress' consideration of this proposal is widely seen as another opportunity for a "user fee" funding mechanism to be repropounded in Congress.

⁸¹ § 70107(i).