THE MARITIME TRANSPORTATION SECURITY ACT OF 2002 AND THE INTERNATIONAL SHIP AND PORT FACILITY SECURITY CODE

By

Kenneth Gale Hawkes, Esq.
Miami, Florida

Introduction

On November 25, 2002, President George Bush signed into law the Maritime Transportation Security Act of 2002.[1] This Act has become known as the MTSA. Less than three weeks later, on December 13, 2002, the International Maritime Organization (IMO) adopted the 2002 Amendments to the Safety of Life at Sea Convention, 1974 (SOLAS). Contained in those amendments are new international maritime security requirements known as the International Ship and Port Facility Security Code (ISPS Code). The purpose for both the MTSA and the ISPS Code is to improve the security of ships and ports—the former with regards to the United States and the latter with regards to the international maritime industry as a whole—and both establish mandatory security requirements with which the maritime industry has never before had to contend. As a result, maritime trade and commerce stand to be affected more

[1] 46 U.S.C. 70101, *et seq.*

significantly than anything that has occurred in the history of the industry. Bills of lading, charter parties, vessel purchase contracts, insurance coverage, intermodal transportation liability issues, and everything else related to the movement of cargo, both afloat and ashore, must now be reviewed in light of the new security requirements. In addition, many nations besides the United States have enacted their own maritime security legislation based upon differing interpretations of the ISPS Code. The European Union has not only legally challenged certain portions of the amendments as being violative of the EU Constitution,[2] but also made it known that it intends to pass legislation contrary to some interpretations of the ISPS Code. The combined effect will be an exponential rise in the cost of shipping goods and an increase in cargo transportation litigation. This paper shall address some of the considerations of the interplay here in the United States between the ISPS Code and the MTSA.

The ISPS Code and MTSA Connection

The 2002 Amendments to the SOLAS Convention were ratified by the members of IMO on January 1, 2004 when one-third of the states failed to object. Consequently, there are an estimated 43,000 ships and 20,000 port facilities around the world that must comply with the ISPS Code by July 1, 2004, and the substantial cost of doing so is just now being realized by many nations. The cost of properly securing a port or port facility can easily be several million dollars. The price of complying with the ISPS Code can cost a shipowner tens of thousands of dollars per vessel. Thus, what might have seemed like a good idea a year ago, may well now be recognized as creating a financially

[2] E.g., Regulation 11-1 relating to alternative bilateral security agreements.

burdensome requirement that most countries and many shipowners simply cannot meet. Non-compliance with the Code will result in a particular ship or port facility being denied the ability to trade internationally. For port facilities, that will mean that no ship will call to either load or discharge international cargo. For ships, no shippers will contract to ship their cargo on that vessel.

The public law of nations was long ago incorporated into the common law of the United States. *The Paquete Habana*, 175 U.S. 677, 700 (1900). To the extent possible, courts must construe U.S. law so as to avoid violating principles of public international law. *Murray v. The Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64, 102 (1804). Public international law, however, is controlling only "where there is no treaty and no controlling executive or legislative act or judicial decision." 175 U.S. at 700.[3] Interestingly enough, Congress obliquely referred to the ISPS Code in the MTSA:

> The International Maritime Organization and other similar international organizations are currently developing a new maritime security system that contains the essential elements for enhancing global maritime security. Therefore, it is in the best interests of the United States to implement new international instruments that establish such a system.[4]

The ISPS Code and the SOLAS Amendments are specifically incorporated by reference in both the temporary interim rules (published in the Federal Register on Tuesday, July 1, 2003[5]) and the final rules (published in the Federal Register on Wednesday, October 22, 2003[6]) by the U.S. Coast Guard:

---

[3] See *Garcia-Mir v. Meese*, 788 F.2d 1446 (11th Cir. 1986), cert. denied sub. nom. *Ferrer-Mazorra v. Meese*, 479 U.S. 899.
[4] Finding 15.
[5] 68 F.R. 39240-39368
[6] 68 F.R. 60448-60570

> [W]here appropriate, the Coast Guard intends to implement the MTSA *through the requirements* in the SOLAS amendments and the ISPS Code, parts A and B, for all vessels and facilities that are currently required to meet SOLAS….[7] [Emphasis supplied.]

Clearly, the MTSA is domestic legislation. It is applicable to all U.S.-flag vessels within certain parameters, foreign-flag vessels over 100 gross tons calling at U.S. ports, and U.S. ports and port facilities "that the Secretary believes may be involved in a transportation security incident."[8] It does not require the existence of the ISPS Code to be effective and, in fact, it differs from the ISPS Code and the SOLAS Amendments in numerous ways, some of which shall be discussed, *infra*. It is the *implementation* of the MTSA by the U.S. Coast Guard *through* the ISPS Code that will cause considerable confusion and litigation. This is because the ISPS Code is extremely vague, which allows for all sorts of individual interpretations and legal challenges. Furthermore, because of its fundamental conceptual flaw that allows each of the 167 member states to interpret it as each state sees fit, the ISPS Code has created not a uniform system of maritime security, as intended, but rather, a non-uniform system fraught with clear uncertainties and legal loopholes. Thus, the refusal of a ship's entry by the United States, or her detainment within a U.S. port, based upon a perceived non-compliance with the ISPS Code founded upon a misinterpreted section of the Code, will certainly generate a lawsuit against the U.S.[9] It may also generate lawsuits by cargo interests against the vessel, the flag state that approved her security plan, and perhaps other entities. In

[7] 68 F.R. 39242
[8] 46 U.S.C. 70103(c)(2)(A)
[9] In the Canadian federal court case of Berhad v. Canada, 2003 FC 992, the Court refused to dismiss a suit against the Canadian government for negligent inspection by port state control inspectors that caused a ship to be unnecessarily detained, relying, in part, on Section 19(f) of the SOLAS Regulations that cautions signatory nations to avoid undue detention or delay of a ship.

addition, the MTSA contains a $25,000-per-violation civil penalty provision for violation of the Act, and every day the vessel remains in violation is a new violation.[10] So, if the U.S. Coast Guard intends to implement the Act through the requirements of the ISPS Code, and the ISPS Code is so vague and ambiguous as to leave serious doubt that the Coast Guard's interpretation regarding compliance is correct, and non-compliance with the Code is considered a violation of the MTSA for which fines in the hundreds of thousands of dollars may be levied, litigation of the Coast Guard's assessment of those fines is a certainty.

The ISPS Code

So, what are the requirements in the ISPS Code? The ISPS Code consists of two parts, Part A and Part B. Part A is mandatory, as is stated in the title ("Mandatory Requirements Regarding the Provisions of Chapter XI-2 of the International Convention for the Safety of Life at Sea, 1974, As Amended") and the initial Paragraph 1.1:

> This part of the international Code for the Security of Ships and Port Facilities contains *mandatory* provisions to which reference is made in chapter XI-2 of the International Convention for the Safety of Life at Sea, 1974 as amended. [Emphasis supplied.]

Part B, on the other hand, is not mandatory, but is instead offered as "guidance" to be used in implementing Part A, as is stated in Part B, Paragraph 3.1:

> The *guidance* given in this Part of the Code should be taken into account when implementing the requirements of chapter XI-2 and part A of this Code. [Emphasis supplied.]

A very real legal question exists as to what "taken into account" means, and this will become more apparent as the requirements of Part A are discussed. Many, including the

[10] 46 USC 70117

U.S. Coast Guard, contend that "taken into account" means mandatory compliance with Part B, arguing that one cannot comply with Part A unless he complies with Part B. However, if that were the case, there would have been no reason to divide the Code into two parts, a mandatory part and a guidance part. It is therefore reasonable to ague that only compliance with Part A is *required* by the Code.

The stated objectives of the ISPS Code are to:

- Establish an international framework to detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade;
- Establish respective roles and responsibilities at the national and international level for ensuring maritime security;
- Ensure the early and efficient collection and exchange of security-related information;
- Provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels; and
- Ensure confidence that adequate and proportionate maritime security measures are in place.

The key concept behind the Code is the creation of a uniform system of maritime security levels and a mechanism for ships and port facilities to respond to those levels. The mechanism envisioned is a properly implemented ship- or port-specific security plan. Thus, every ship or port facility must develop a security plan that establishes the security measures and procedures that will be utilized at each of three different security levels:

Level 1, Level 2 and Level 3. These have been referred to as "MARSEC levels." For ships, MARSEC levels are set by their flag administrations, and for ports, the MARSEC levels are set by the government of the country in which the port is located.[11] Thus, a ship may be operating at Security Level 1, as instructed by her flag administration, but enter a port facility operating at Security Level 2, as declared by the port control state. Under the Code, she must then increase her security measures to a MARSEC Level 2. On the other hand, a ship may be operating at Security Level 2 and enter a port operating at Security Level 1. In that case, the port facility does not have to increase its operational status to that of the ship's. The specific security measures required at each MARSEC level, however, are not specified in Part A of the Code, and thus a particular vessel may consider certain security measures applicable only at MARSEC Level 2 or 3 when a port control state considers them applicable at MARSEC Level 1. In that case, a ship operating at what she considers is MARSEC Level 2 will be operating only at what the port control state considers is MARSEC Level 1. For MARSEC Level 1, for instance, Part A merely states:

> 7.2 At security level 1, the following activities shall be carried out, through appropriate measures, on all ships, taking into account the guidance given in part B of this Code, in order to identify and take preventive measures against security incidents:
> .1 ensuring the performance of all ship security duties
> .2 controlling access to the ship
> .3 controlling the embarkation of persons and their effects
> .4 monitoring restricted areas to ensure that only authorized persons have access
> .5 monitoring of deck areas and areas surrounding the ship

[11] This government function is supposed to be based upon the international terrorist threat intelligence gathering and analysis capabilities of each Contracting Government, which can vary greatly from one nation to another.

.6 supervising the handling of cargo and ship's stores; and
.7 ensuring that security communication is readily available[12]

At Security Level 2, "additional protective measures" must be specified and implemented. At Security Level 3, "further specific protective measures" must be specified and implemented. None of these "additional" or "further specific" protective measures are described. In all instances, however, they must be "appropriate." What are "appropriate measures?" Part A is silent as to what these are, except to say that the guidance in Part B must be taken into account. Thus, so long as the security plan establishes security measures and procedures for each level, in cumulative fashion, and the shipowner can state that he "took into account" the guidance in Part B (not that he necessarily complied with such guidance), and that such measures were "appropriate" so far as he was concerned, the security plan theoretically meets the requirements of Part A.

Part A requires that a Ship Security Plan (SSP) be approved by the maritime administration of the flag state, and that the flag state issue an International Ship Security Certificate (ISSC) under SOLAS once implementation of the plan has been verified.[13] The ISSC serves as certification to the rest of the world that the ship is in compliance with the ISPS Code. Furthermore, even though the Ship Security Plan is required to be carried on board, no port control state has the right to review the plan to verify for itself that the ship is in fact in compliance with the Code.[14] Except in exceptional circumstances, the port control state will not be allowed to look beyond the four corners

[12] ISPS Code A/7.2
[13] ISPS Code A/19.1.1. It is the responsibility of the flag state to verify that the SSP has been properly implemented by the vessel before it issues the ISSC.
[14] ISPS Code A/9.8

of the ISSC.[15] Since different flag states may interpret the Code requirements differently, or be more lenient in their enforcement, any given port control state, such as the U.S., may consider a particular SSP approved by a particular flag state to be insufficient. However, without "clear grounds to believe that the ship is not in compliance with…Part A" the port control state may not review the SSP.[16] This has become a significant bone of contention for some members of Congress as far as the MTSA is concerned, which requires that *all* vessel security plans of ships over 100 gross tons on international voyages calling at U.S. ports be reviewed and approved by the U.S. Coast Guard.[17]

Not only are the security measures and procedures for ships and port facilities for each security level not specified in Part A of the Code, the format and content of the ship or port facility security plan is also not detailed. The operator or owner must only "take into account the guidance given in part B,"[18] and for ships, the plan must be written in the working language or languages of the ship.[19] If the language used in not English, French or Spanish, a translation into *one* of these languages must be included in the plan.[20] The only other requirement is that the plan must "address at least the following:"

1. Measures designed to prevent weapons, dangerous substances and devices intended for use against people, ships or ports and the carriage of which is not authorized from being taken on board the ship;

[15] The MTSA *requires* U.S. approval of *all* ship security plans for covered vessels calling at its ports.
[16] ISPS Code A/9.8.1
[17] 46 U.S.C. 70103(c)
[18] ISPS Code A/9.4
[19] Id.
[20] The U.S. Coast Guard may take the position that it is entitled to review the security plan for any ship calling in the U.S. and, if so, will most likely demand an English translation even though one is not required under the ISPS Code. If the vessel does not have an English translation onboard, it may be detained until such time as one can be obtained.

2. Identification of the restricted areas and measures for the prevention of unauthorized access to them;
3. Measures for the prevention of unauthorized access to the ship;
4. Procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;
5. Procedures for responding to any security instructions [member states] may give at security level 3;
6. Procedures for evacuation in case of security threats or breaches of security;
7. Duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;
8. Procedures for auditing the security activities;
9. Procedures for training, drills and exercises associated with the plan;
10. Procedures for interfacing with port facility activities;
11. Procedures for the periodic review and updating of the plan;
12. Procedures for reporting security incidents;
13. Identification of the ship security officer;
14. Identification of the company security officer including 24-hour contact details;
15. Procedures to ensure inspection, testing, calibration, and maintenance of any security equipment provided on board;
16. Frequency for testing or calibration of any security equipment provided on board;
17. Identification of the location where the ship security alert system activation points are provided; and

18. Procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting, and limiting false alerts.[21]

Since these are the *only* matters, according to Part A, that *must* be addressed, the obvious question is, what does "address" mean? Part A doesn't say "adequately address," and if it did, what would "adequately" mean? There is a very real danger of a port control state, like the U.S., substituting its judgment for that of the shipowner or flag state. Under the Code, the SSP need merely "take into account" the guidance in Part B. It need only "address" the eighteen items listed in Part A. There is no requirement anywhere in the Code that the SSP pass muster by being considered or deemed adequate, operationally sound, or tactically feasible, and the first time a port state control government agency makes that determination and denies entry to a vessel, or detains her until a security plan is drafted that meets that agency's approval, litigation will most certainly ensue. It takes months to properly conduct a security assessment and write a security plan, and even longer to implement it. If a ship is declared to be in violation of the MTSA because her security plan[22] does not meet the expectations of the United States based upon an interpretation of the "requirements" of the ISPS Code, a fine could be levied in the amount of $175,000 per week until such time as a new security plan can be drafted and implemented. In two months the ship would incur a fine of $1.5 million, not to mention demurrage costs, wharfage and other expenses including loss of business.

[21] ISPS Code A/9.4
[22] Referred to in the MTSA as a "vessel security plan" or VSP.

As an example of how easy it will be for a ship to be considered or declared not in compliance with the Code by a port control state inspector who doesn't know what he is doing, we can look at the requirements under Part A relating to the designation of shipboard restricted areas. Paragraph A/9.4.2 states that:

> [The plan shall address] identification of the restricted areas and measures for the prevention of unauthorized access to them.

Most readers of the Code will assume that this paragraph in Part A, when read in conjunction with the applicable sections of Part B, *requires* that restricted areas be physically designated on board. This is because paragraph B/9.20 states:

> The SSP should provide that all restricted areas should be clearly marked indicating that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security.

However, a closer reading to the two paragraphs clearly establishes that (a) only Part A is mandatory, that is, the SSP must merely "address" the identification of restricted areas and the measures the ship intends to use to prevent unauthorized access to them,[23] and (b) Part B merely states an opinion that the SSP "should" provide that all restricted areas "should" be marked; whatever that means. Thus, a shipowner will be well within his rights pursuant to the Code to decide that restricted areas will not be physically marked on board by simply addressing what, if any, restricted areas he wishes to identify in his SSP, and then state that he has taken the applicable sections of Part B into account and decided not to clearly mark them as *suggested* in Part B. However, a port state control inspector, relying on inadequate training or incorrect directives, may very well look for

[23] The Code never defines "address."

clearly marked restricted areas as part of his inspection checklist and declare the ship not in compliance with the Code when he fails to find them.

There are other ways of allegedly failing to be in compliance with the ISPS Code, however, besides not having a proper security plan. The Code requires, as an integral part of the new security scheme, that a security assessment be performed for the specific vessel or port facility concerned.[24] The security assessment then must form the basis on which the security plan is developed.[25] The security assessment must "be carried out by persons with appropriate skills to evaluate the security" of the ship or port facility.[26] Thus, if a Ship Security Assessment (SSA), upon which the SSP is built, is not carried out by a properly qualified individual, the threat conclusions contained in the SSA (which are all purely subjective and based upon experience, training, and opinion) may be invalid or incomplete and the SSP may then be declared noncompliant.

Additionally, a ship could have an adequate SSP and not be in compliance with it on any given day. For instance, the ship might simply be behind on its security training schedule, a piece of security equipment might be inoperable (the Code requires that all security equipment be 100% operational),[27] or the ship security officer might not have all the security experience the security plan requires.[28] Because the MTSA incorporates the ISPS Code, however, non-compliance with the Code is likely to be considered a violation

[24] ISPS Code A/8.1 and A/15.1.
[25] ISPS Code A/9.3 and A/16.1.
[26] ISPS Code A/8.2 and A/15.3.
[27] Theoretically, one inoperable padlock or light fixture will render the vessel non-compliant with the Code.
[28] Part B details the experience and training the SSO "should" have, but this is merely "guidance" that must be "taken into account" when drafting the security plan. It is the plan against which implementation is measured.

under the Act giving rise to a $25,000-per-day fine until the alleged non-compliance is corrected.

The MTSA

As stated *supra*, the Maritime Transportation Security Act[29] was passed and signed into law prior to the ISPS Code being adopted by the IMO, but nonetheless references the ISPS Code.[30] In passing the Act, Congress determined, among other things, that:

1. There are 361 public ports in the United States that are an integral part of the nation's commerce.
2. United States ports handle over 95 percent of United States overseas trade. The total volume of goods imported and exported through those ports is expected to more than double over the next 20 years.
3. The variety of trade and commerce carried out at such ports includes bulk cargo, containerized cargo, passenger transport and tourism, and intermodal transportation systems that are complex to secure.
4. The United States is increasingly dependent on imported energy for a substantial share of its energy supply, and a disruption of that share would seriously harm consumers and the economy.
5. The top 50 ports in the United States account for about 90 percent of all cargo tonnage. Twenty-five ports account for 98 percent of all container shipments.

[29] 46 USC 70101, *et seq*.
[30] November 25, 2002, the same date Congress established the Department of Homeland Security, and the one-year anniversary date of the passage of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, 18 USC 1.

Cruise ships visiting foreign destinations embark from at least 16 ports. Ferries in the United States transport 113 million passengers and 32 million vehicles per year.

6. Ports often are a major focus of Federal crime, including drug trafficking, cargo theft, and smuggling of contraband and aliens.
7. Ports are often very open and exposed, and are susceptible to large scale acts of terrorism that could cause a large loss of life or economic disruption.
8. Current inspection levels of containerized cargo are insufficient to counter potential security risks. Technology is currently not adequately deployed to allow for the nonintrusive inspection of containerized cargo.
9. The cruise ship industry poses a special risk from a security perspective.[31]

Congress went on to determine that United States ports are international boundaries that (a) are particularly vulnerable to breaches in security, (b) may present weaknesses in the ability of the United States to realize its national security objectives, and (c) may serve as a vector or target for terrorist attacks.[32] It then outlined the objectives of the Act by declaring it in the best interest of the United States:

A. To have a free flow of interstate and foreign commerce and to ensure the efficient movement of cargo;
B. To increase United States port security by improving communication among law enforcement officials responsible for port security;

[31] 46 USC 70101 note.
[32] Id. at note 12.

C. To formulate requirements for physical port security, recognizing the different character and nature of United States port facilities, and to require the establishment of security programs at port facilities;

D. To provide financial assistance to help the States and the private sector increase physical security of U.S. ports;

E. To invest in long-term technology to facilitate the private sector development of technology that will assist in the non-intrusive timely detection of crime at U.S. ports;

F. To increase intelligence collection on cargo and intermodal movements to address areas of potential threat to safety and security; and

G. To promote private sector procedures that provide for in-transit visibility and support law enforcement efforts directed at managing the security risks of cargo shipments.[33]

On October 22, 2003, the Coast Guard published a series of final rules promulgating the maritime security requirements mandated by the MTSA.[34] Those rules became effective on November 21, 2003.[35] Furthermore, even though not yet ratified, the ISPS Code will, according to the final rules, be used by the U.S. Coast Guard as an *indicator of compliance* with the MTSA.[36] In fact, the MTSA rules *require* any owner or operator of a U.S. flag vessel that is subject to SOLAS to be in compliance with Part A of

[33] Id. at note 13.
[34] 68 FR 60448-60570
[35] 68 FR 60448
[36] 68 FR 60449

the ISPS Code.[37] There are six (6) separate final rules. The first five (5) complete a new subchapter H in chapter I of Title 33 of the Code of Federal Regulations (CFR), and the sixth final rule involves vessel automated identification systems and carriage requirements found in parts 161, 164 and 165 of Title 33. The rules are broken down as follows:

1. Implementation of National Maritime Security Initiatives
2. Area Maritime Security (AMS)
3. Vessel Security
4. Facility Security
5. Outer Continental Shelf (OCS) Facility Security
6. Automatic identification Systems (AIS)

For each of the final rules, the requirements of the MTSA closely align with, but are not identical to, the requirements or language of the SOLAS Amendments and the ISPS Code. For one thing, the MTSA has a broader application that includes domestic vessels and facilities. The ISPS Code, for instance, applies only to SOLAS vessels engaged on international voyages that include:

1. Passenger ships, including high-speed passenger craft.
2. Cargo ships, including high-speed craft, of 500 gross tonnage and upwards.
3. Mobile offshore drilling units.
4. Port facilities serving such ships engaged on international voyages.[38]

The MTSA, however, applies to:

[37] 33 CFR 104.297
[38] ISPS Code A/3.1

1. Mobile Offshore Drilling Units, cargo, or passenger vessels subject to SOLAS;
2. Foreign commercial vessels greater than 100 gross register tons not subject to SOLAS;
3. Commercial vessels greater than 100 gross register tons subject to 46 CFR subchapter I, except commercial fishing vessels inspected under 46 CFR part 105.
4. Vessels subject to 46 CFR subchapter L;
5. Passenger vessels subject to 46 CFR subchapters H or K;
6. Other passenger vessels carrying more than 12 passengers that are engaged on international voyages;
7. Barges subject to 46 CFR subchapters D or O;
8. Barges subject to 46 CFR subchapter I that carry Certain Dangerous Cargoes in bulk, or that are engaged on an international voyage;
9. Tankships subject to 46 CFR subchapters D or O; and
10. Towing vessels greater than 8 meters in registered length that are engaged in towing a barge or barges subject to 33 CFR 104.[39]

Like the ISPS Code, the MTSA rules require each vessel covered by the Act to develop and implement a vessel security plan (VSP).[40] However, the requirements for a VSP do not exactly match those for an SSP under the ISPS Code. For example, the VSP must be written in English,[41] which is not a requirement under the Code.[42] Also, the VSP

[39] 33 CFR 104.105(a)
[40] 33 CFR 104.400(a)
[41] 33 CFR 104.400(a)(2)
[42] ISPS Code A/9.4. "If the language or languages used is not English, French, or Spanish, a translation into *one* of these languages shall be included."

must consist of seventeen (17) sections specified in the rules,[43] and these seventeen sections do not fully comport with the eighteen (18) subjects that must be addressed according to Part A of the ISPS Code.[44] The most interesting anomaly, however, is that even though the MTSA requires every VSP or SSP to be reviewed and approved by the Coast Guard, and even though the requirements for an SSP under the Code are different than for a VSP under the MTSA, the Coast Guard has declared that any foreign vessel that has a valid International Ship Security Certificate (ISSC) on board that attests to the vessel's compliance with SOLAS and the ISPS Code Part A "having taken into account the relevant provisions" of Part B, need not submit a VSP to the Coast Guard for approval.[45] This is a huge exception, and one with which, as stated *supra*, certain members of Congress are less than enamored. However, since the MTSA contains no authorization whatsoever for the U.S. Coast Guard to consider compliance with the ISPS Code as compliance with the MTSA, vessel owners are not relieved from complying with the MTSA, and a valid ISSC may well not insulate a ship from being fined, denied entry or detained if found in noncompliance with the Act.[46]

The MTSA final rules establish certain vessel security requirements.[47] In accordance with these requirements, each vessel owner or operator *must*:

1. Define the security organizational structure for each vessel *and provide* all personnel exercising security duties or responsibilities within that structure with *the support needed to fulfill security obligations* [emphasis supplied];

[43] 33 CFR 104.405(a)
[44] ISPS Code A/9.4
[45] 33 CFR 104.400(b)
[46] Even though it may be in compliance with the CFR.
[47] 33 CFR 104.200

2. Designate, in writing, by name or title, a Company Security Officer (CSO), and a Vessel Security Officer (VSO) for each vessel, and identify how those officers can be contacted at any time;
3. Ensure personnel receive training, drills, and exercises enabling them to perform their assigned security duties;
4. Ensure vessel security records are kept;
5. Ensure that adequate coordination of security issues takes place between vessels and facilities; this includes the execution of a Declaration of Security (DOS);
6. Ensure coordination of shore leave for vessel personnel or crew change-out, as well as access through the facility of visitors to the vessel, with facility operators in advance of the vessel's arrival;
7. Ensure security communication is readily available;
8. Ensure coordination with and implementation of changes in MARSEC levels;
9. Ensure that security systems and equipment are installed and maintained;
10. Ensure that vessel access, including the embarkation of persons and their effects, is controlled;
11. Ensure that restricted areas are controlled.
12. Ensure that cargo, vessel stores and bunkers are handled in compliance with 33 CFR 104;
13. Ensure restricted areas, deck areas, and areas surrounding the vessel are monitored;

14. Provide the Master or CSO with (a) the names of the parties responsible for appointing vessel personnel, such as vessel management companies, manning agents, and concessionaires, (b) the names of the parties responsible for deciding the employment of the vessel, including time or bareboat charterers, and (c) the contract details of any charter parties; and
15. Give particular consideration to the convenience, comfort, and personal privacy of vessel personnel and their ability to maintain their effectiveness over long periods.[48]

These are things that, under the MTSA, the owner or operator *must* do. In fact, the VSP must "describe in detail" how these requirements will be met.[49] Some of them may well be problematical. For instance, the owner must "provide all personnel exercising security duties or responsibilities…with the support needed to fulfill security obligations."[50] Presumably, this includes both money and manpower, items that historically have been inadequately dispensed to security operations within the private sector. Thus, if the security operation is, in the opinion of the USCG inspector, undermanned or under-funded or under-equipped, the owner or operator may be considered in violation of the Act, giving rise to a $25,000 per day fine until rectified. Violation of the Act may also give rise to a *negligence per se* argument in any negligent security litigation, as well as a potential unseaworthiness argument.

---

[48] 33 CFR 104.200
[49] 33 CFR 104.405(b)
[50] 33 CFR 104.200(b)(1). This is similar to ISPS Code A/6.2 that requires the company security officer, master, and ship security officer all be given the "necessary support" to fulfill their security duties and responsibilities.

One final example of the various discrepancies between the MTSA rules and the SOLAS Amendments is the way potential conflicts between safety and security are addressed. Under the MTSA rules, safety may not necessarily take precedence over security concerns. The rules state:

> If, in the professional judgment of the Master, a conflict between any safety and security requirements applicable to the vessel arises during its operations, the Master *may* give precedence to measures intended to maintain the safety of the vessel….[51] [Emphasis supplied.]

However, Regulation 8, SOLAS Chapter XI-2, states:

> If, in the professional judgment of the master, a conflict between any safety and security requirements applicable to the ship arises during its operations, the master *shall* give effect to those requirements necessary to maintain the safety of the ship. [Emphasis supplied.]

The distinction may appear to be a small one, but it could be significant in a personal injury action where liability rests on the failure of the vessel to follow recognized international safety requirements. If the MTSA is applicable, a defense could be based upon security concerns. If SOLAS is applicable, such a defense is not available.

Freight Transport Security Issues

All freight transportation issues have historically focused on liability for loss of or damage to cargo, and the targets of such inquiries have always been the carriers. While a shipper might not be able to prove his *prima facie* case, or overcome certain COGSA defenses or bill of lading/tariff contractual provisions, he has rarely faced legal liability for the damages caused by the cargo itself. With the advent of the new world order in which weapons of mass destruction (WMDs) may be employed by terrorist groups to

[51] 33 CFR 104.205(b)

wreak death and destruction on any populace or infrastructure, shipper liability has now become a very real issue and a target for third party litigation in cases of negligent security claims against the carrier. The new security requirements mandated by the ISPS Code and the MTSA, and the potential for delay, detention, or refusal of entry for allegedly failing to meet those requirements, as well as broken seals and other breaches of container security for inspection purposes, raises the specter of all sorts of contract and tort claims that must now be addressed in charter parties, bills of lading and tariffs. Under SOLAS, the master of the loading vessel has the absolute right to refuse "to load cargo, including containers or other closed cargo transport units."[52] He also has the right to make or execute "any decision which, in the professional judgment of the master, is necessary to maintain the safety and security of the ship."[53] Presumably, this includes opening, stripping, and inspecting any suspect container and its cargo, all at the expense of the shipper. Tariffs and bills of lading need to provide for that eventuality. They also need to protect the carrier against the adverse results of government intervention. Since security measures and procedures are not clearly defined or delineated in the ISPS Code or the MTSA, tariffs and contracts of carriage need to do so in order to precisely establish carrier responsibilities and defenses.

Security is not an exact science. Like warfare, it is an art, and like any art, its effectiveness is subjective. Anything that is subjective is open to differing interpretations. This is one of the primary problems with the ISPS Code and the MTSA. If flag states and port state control states begin substituting their judgment for that of the

[52] SOLAS Chapter XI-2, Regulation 8-1.
[53] Id.

shipowner or facility operator, they will open the door for two arguments. First, that neither the ISPS Code nor the MTSA allows for such a substitution of judgment, and second, that if the owner or operator is forced to accept the flag state's or port state control state's micromanagement of its security, then it may well be legally relieved of all liability resulting from such micromanagement. As some 43,000 ship security plans are reviewed over the next six months by various government agencies and classification societies acting on their behalf, it is clearly expected that certain plans will be rejected as unsatisfactory. Such rejection may prevent the issue of an ISSC and thus the ability of the vessel to operate. If the security plans are rejected not because they allegedly fail to comply with Part A of the ISPS Code, or the MTSA rules, all of which are open to interpretation, but instead because the reviewer makes a subjective determination that the SSP or VSP is inadequate from an operational security standpoint, the agency making that determination is likely to be sued for huge damages.[54] Fines levied by the U.S. Coast Guard pursuant to the MTSA will likewise face the same challenge.

Conclusion

Security can never be absolute. Any security system or combination of security procedures can be circumvented given enough time and resources. With the advent of world terrorism and increase in global security awareness, any terrorist attack can now be deemed foreseeable. As Robert F. Housman stated in his paper, "Birth and Development of Homeland Security Law":[55]

[54] See Berhad v. Canada, *supra*.
[55] *Homeland Security Law Handbook* (Government Institutes, 2003), Chapter 1, p.19.

> Post 9/11 polling shows that the community of Americans now view virtually any form of terrorist attack as reasonably foreseeable. These polls also show that Americans expect their government and the owners of the nation's infrastructure to protect them from such attacks.

So, the question becomes, "What is reasonable security under the circumstances?" Since security is an art and not a science, the question is clearly a subjective one that will be answered differently by various judges, juries, and security experts under different fact patterns. Part of this inquiry involves acceptable risk. What is the acceptable risk in any given circumstance? Is it always the same? Is no risk acceptable, or is the degree of risk dependent upon the nature of the enterprise. How much money should a private entity be forced to spend in order to do business in a secure manner? What does "secure manner" mean? To whom is a duty to do so owed?

The ISPS Code and the MTSA attempt to establish a maritime security regime that is workable within the industry. It does no good to mandate security measures that are so costly or restrictive that the industry cannot operate. The danger lies in the fact that both are clearly open to interpretation, and since serious consequences may befall those deemed to have not complied, a much clearer understanding of what compliance is must be developed. This is likely to occur only through litigation.

KENNETH GALE HAWKES, ESQ.

Gale Hawkes is a Florida Bar board-certified admiralty and maritime law trial attorney in private practice in Miami. He received his J.D. from the University of Miami in 1979 and is admitted to practice before the Supreme Court of the United States, the Fifth and Eleventh U.S. Circuit Courts of Appeal, and all federal and state courts in the State of Florida. He has litigated cases spanning the entire spectrum of admiralty matters including personal injury, collision, cargo damage, fisheries, Coast Guard regulatory and license actions, and negligent security.

Mr. Hawkes worked as Vice President, Maritime Security, for The Wackenhut Corporation from 1989 to 1995, founding his division years before maritime security became the focal point it has today. He also has worked as a commercial fisherman, commissioned officer in the United States Marine Corps (terminal rank: Captain), commercial marine surveyor, maritime private investigator, and expert witness. He is a former Chairman of the ASIS Transportation Security Committee for Seaports and Harbors, and is a Proctor member of the Maritime Law Association of the United States (1980) and a long-standing member of the Southeastern Admiralty Law Institute. Mr. Hawkes is the author of the only textbook on maritime security, *Maritime Security* (Cornell Maritime Press, 1989; Grade-A-Notes, 2003), as well as numerous papers and magazine articles. He is also the editor of several government-sponsored publications, including *Seaport Security* (OAS, 1996), *International Perspectives on Maritime Security* (Maritime Security Council/U.S. Department of Transportation, 1996), and *Port Security: Security Force Management* (U.S. Department of Transportation, 1998). He is an adjunct professor at the Global Maritime Transportation School of the U.S. Merchant Marine Academy, King's Point, New York, and has served as a special consultant and primary instructor on maritime security to the International Maritime Organization (IMO) and the American Bureau of Shipping (ABS). He practices law under his firm name of Kenneth Gale Hawkes, P.A. (kgh@sealawyer.net), 1717 North Bayshore Drive, Suite 4133, Miami, FL 33132, (305) 577-8949, and is affiliated with the maritime law firms of Underwood, Karcher & Karcher, P.A. (Miami) and Michael J. McHale, P.A. (Jensen Beach/West Palm Beach). He is also President and CEO of the maritime security consulting (ISPS Code and MTSA compliance/negligent security) firm of Global Hawks, LLC, and is Executive Vice President and General Counsel of MARSEC International, LLC, an international consulting firm specializing in port and port facility security.