CAL MARITIME

A Campus of the California State University System

MARITIME SECURITY TRAINING CHALLENGES

In the Post ISPS Code and MTSA 2002 World

A White Paper

Prepared for

PREVENTION FIRST 2006

Long Beach, CA
September 12 & 13, 2006

California State Lands Commission

Primary Authors

CAPT Frank Whipple, USCG (ret)
Principal,
AMERGENT TECHS

CAPT Bruce G. Clark, USCGR (ret)
Director, Maritime Security Projects
The CALIFORNIA MARITIME ACADEMY

Maritime Security Training Challenges

Formalized security training within the marine industry is relatively new. Having developed quite quickly during the period of the International Ship and Port Security (ISPS) Code implementation, the enactment of the Maritime Transportation Security Act of 2002 and the US Coast Guard implementing requirements for maritime security measures, the USCG regulations contained in 33 CFR Subchapter "H", Parts 101, 103, 104, 105 and 106 have set the baseline specifications for security knowledge.

The maritime industry has had two years of experience in implementing the required security provisions of the ISPS Code and MTSA 2002. We have learned about the many practical and economic challenges facing companies in dealing with new security measures. Required internal and external security audits have provided insight in how well the programs are being developed and implemented, as well as through vital information obtained through the US Coast Guard security inspection and validation process. Since maritime security vulnerabilities, threats -- and therefore the risk -- from these factors on both a national and international basis continues to change and provide continuing challenges to our ports, terminals, ships, boats, marinas and the personnel who either work or utilize the facilities, the necessity to periodically reassess the quality, quantity and efficacy of security training is also required.

Each of us engaged in the Maritime Transportation System (MTS) – which includes all modes of transportation that interface in the port environment – are working very hard to reduce security risk. Often these efforts are conducted in isolation from other stakeholders—focused only on my ship, my facility or my MTS operation. But without feedback on and sharing of our successes (or our failures), or a reasonable analysis as to whether the programs we have implemented are effective and are providing the results both expected and intended, we are operating in a vacuum without the capability to adapt and adjust to the changing conditions of a dangerous and hostile world.

Without training programs that reflect currency, capture and utilize important lessons learned and which extend beyond the regulatory baseline – we have no fundamental "metrics" by which to measure the long term value of the program. How for example do we "prove" that our actions have "prevented" a terrorism incident in the maritime environment? How do we measure and judge the value of criteria employed to properly identify suspicious persons – and if they are identified, is the mechanism in place to report these suspicions properly in place and being effectively used? Ultimately, will we continue to be free from actual maritime security incidents because we are "*doing the right things, in the right places, at the right time, for the right reasons"?*

To answer these questions, it is appropriate for us to take a brief look at where we are in overall implementation of maritime security training, the existing security requirements, and then to compare them to areas which may need addressing. This process can be considered an initial "gap analysis" for identification of training shortfalls and recommendation for improvements.

This paper will look specifically at the following topics and questions:

1. Review of Current Training Situation
2. Are existing Maritime Security training courses meeting industry expectations?
3. Who is the appropriate entity or entities responsible to ensure proper training?
4. How do you properly train a member of your security force who may only work for you 1 or 2 days a week?
5. Are the length and the content of existing security training sufficient to meet the qualification and knowledge requirements specified by code and by regulation?

Review of Current Situation:

The current maritime security training system is driven primarily by regulatory mandates based upon the very broad guidelines contained in the ISPS Code and through implementing legislation such as MTSA 2002 in the United States. Training programs arising from these sources for Vessel Security Officers, Company Security Officers and Facility Security Officers contain typically only what is required in terms of detail and content to meet these basic mandates. Knowledge requirements for each treaty signatory to the SOLAS Convention Annex that established the ISPS Code will apply ONLY to that specific countries' maritime industry and so, are not specifically defined but are general in nature by design.

Effectively this means that although the same generic baseline established by the ISPS Code is in use worldwide – specific requirements regarding training and knowledge vary from country to country dependent upon local prevailing opinions and political will.

Further, within countries and locations there may be additional variations and levels of enforcement that make comparison between training programs and validation of efficacy difficult. The following sections will describe some of the overarching requirements, impediments and concerns of the current maritime security training program:

1. Current FSO/CSO/VSO Responsibilities and Knowledge requirements
2. Identification of others with security duties
3. Review of current IMO & MARAD Model Courses
4. Review of Existing ISPS Code and MTSA 2002 Professional Development Training Courses
5. Absence of Definitions and Training Policy Standards for "Security Duty Positions"
6. What Implementation Challenges are being observed in the Field?

What are the current Duties and Responsibilities of a Maritime Security Officer in the United States?

For MTSA Regulated Facilities:

33 CFR Subchapter "H", Part 101.105 defines the Facility Security Officer as "…*the person designated as responsible for the development, implementation, revision, and maintenance of the facility security plan and for liaison with the COTP and Company and Vessel Security Officers."* Facility Security Officer (FSO) qualifications in the United States are governed by 33 CFR Part 105.205. This section states that the designated FSO may perform other duties in addition to those required of the security officer and may serve as FSO for more than one facility ***provided*** *they are located within the same COTP zones and not more than 50 miles apart.* The FSO may designate specific security duties or functions to others but retains the overall responsibility for execution of these duties.

The FSO must demonstrate competency via general knowledge obtained *by training* ***OR*** *by equivalent job experience* for such things as:

a. Security organization of the facility;
b. General vessel and facility operations and conditions;
c. Vessel and facility security measures, including the meaning and the requirements of the different MARSEC Levels;
d. Emergency preparedness, response, and contingency planning;
e. Security equipment and systems, and their operational limitations; and
f. Methods of conducting audits, inspections, control, and monitoring techniques.

In addition to the above, the FSO must demonstrate competency in the following specific knowledge requirements **ONLY** *by successful completion of* ***documented training*** – "as applicable":

a. Relevant international laws and codes, and recommendations;
b. Relevant government legislation and regulations;
c. Responsibilities and functions of local, State, and Federal law enforcement agencies;
d. Risk assessment methodology;
e. Methods of facility security surveys and inspections;
f. Instruction techniques for security training and education, including security measures and procedures;
g. Handling sensitive security information and security related communications;
h. Current security threats and patterns;
i. Recognizing and detecting dangerous substances and devices;

j. Recognizing characteristics and behavioral patterns of persons who are likely to threaten security;
k. Techniques used to circumvent security measures;
l. Conducting physical searches and non-intrusive inspections;
m. Conducting security drills and exercises, including exercises with vessels; and
n. Assessing security drills and exercises.

33 CFR Part 105.205 (c) lists ***18*** *specific additional day-to-day FSO Responsibilities* that the designated security officer must perform as follows:

a. Ensure that the Facility Security Assessment (FSA) is properly performed and documented;
b. Ensure the development and implementation of a Facility Security Plan (FSP);
c. Ensure that an annual audit is conducted, and if necessary if the FSA and FSP are updated;
d. Ensure the FSP is exercised per Sec.105.220 of this part;
e. Ensure that regular security inspections of the facility are conducted;
f. ***Ensure the security awareness and vigilance of the facility personnel***;
g. Ensure adequate training to personnel performing facility security duties;
h. Ensure that occurrences that threaten the security of the facility are recorded and reported to the owner or operator;
i. Ensure the maintenance of records required by this part;
j. Ensure the preparation and the submission of any reports as required by this part;
k. Ensure the execution of any required Declarations of Security with Vessel Security Officers;
l. Ensure the coordination of security services in accordance with the approved FSP;
m. Ensure that security equipment is properly operated, tested, calibrated, and maintained;
n. Ensure the recording and reporting of attainment changes in MARSEC Levels to the owner or operator and the cognizant COTP;
o. When requested by the VSO, ensure that the Vessel Security Officers receive assistance in confirming the identity of visitors and service providers seeking to board the vessel through the facility;
p. Ensure notification, as soon as possible, to law enforcement personnel and other emergency responders to permit a timely response to any transportation security incident;
q. Ensure that the FSP is submitted to the cognizant COTP for approval, as well as any plans to change the facility or facility infrastructure prior to amending the FSP; and
r. Ensure that all facility personnel are briefed of changes in MARSEC conditions at the facility.

For MTSA Regulated Shipping Companies:

33 CFR Subchapter "H", Part 101.105 defines the Company Security Officer as "…*the person designated by the Company as responsible for the security of the vessel or OSC facility, including implementation and maintenance of the vessel or OSC facility security plan and for liaison with their respective vessel and facility security officer and the Coast Guard."* Company Security Officer (CSO) qualifications in the United States are governed by 33 CFR Part 104.210. This section states that a designated CSO may perform other duties in addition to those required of the security officer, may serve as CSO ***for more than one vessel*** and may also serve as a VSO so long as all functions required for those duties can be reasonably performed. The CSO may designate specific security duties or functions to others but retains the overall responsibility for execution of these duties.

Company Security Officer qualifications contained in 33 CFR Part 104.210 are virtually identical to those specified for FSO's – but are tied to company level responsibilities *SPECIFIC to VESSEL AND OFFSHORE OPERATIONS* -- with the exception of the additional requirement for experience related to :

a. Techniques for security training and education, including security measures and procedures.

Unlike the FSO, the CSO can meet the following additional specific knowledge requirements by demonstrated competency either through ***either direct knowledge (equivalent job experience) OR*** *successful completion of* ***documented training.***
Similarly and addition to the requirements for designation as an FSO, the CSO must be cognizant of:

a. Responsibilities and functions of other security organizations;
b. Methodology of Vessel Security Assessment;
c. Methods of vessel security surveys and inspections;
d. Methods of physical screening and non-intrusive inspections;
e. Security drills and exercises, including drills and exercises with facilities; and
f. Assessment of security drills and exercises.

33 CFR Part 104.210 (c) lists ***14*** *specific additional day-to-day CSO Responsibilities* that the designated security officer must perform as follows:

a. Keep the vessel apprised of potential threats or other information relevant to its security;
b. Ensure a Vessel Security Assessment (VSA) is carried out;
c. Ensure a Vessel Security Plan (VSP) is developed, approved, and maintained;
d. Ensure the VSP is modified when necessary;
e. Ensure vessel security activities are audited;
f. Arrange for Coast Guard inspections under 46 CFR part 2;

g. Ensure the timely or prompt correction of problems identified by audits or inspections;
h. Enhance ***security awareness and vigilance*** within the owner's or operator's organization;
i. Ensure relevant personnel receive adequate security training;
j. Ensure communication and cooperation between the vessel and the port and facilities with which the vessel interfaces;
k. Ensure consistency between security requirements and safety requirements;
l. Ensure that when sister-vessel or fleet security plans are used, the plan for each vessel reflects the vessel-specific information accurately;
m. Ensure compliance with an Alternative Security Program or equivalents approved under this subchapter, if appropriate; and
n. Ensure security measures give particular consideration to the convenience, comfort, and personal privacy of vessel personnel and their ability to maintain their effectiveness over long periods.

For MTSA Regulated Vessels:

33 CFR Subchapter "H", Part 101.105 defines the Vessel Security Officer as "…*the person designated by the Company as responsible for the security of the vessel or OSC facility, including implementation and maintenance of the vessel or OSC facility security plan and for liaison with their respective vessel and facility security officer and the Coast Guard."* Vessel Security Officer (VSO) qualifications in the United States are governed by 33 CFR Part 104.215. This section states that a designated VSO may perform other duties in addition to those required of the security officer, may serve as VSO ***for more than one UNMANNED vessel***. The VSO of a **MANNED vessel** must be the Master or a member of the assigned crew. The VSO may designate specific security duties or functions to others but retains the overall responsibility for execution of these duties.

Vessel Security Officer qualifications contained in 33 CFR Part 104.215 are virtually identical to those specified for CSO's – but are tied to responsibilities *SPECIFIC to VESSEL OPERATIONS*. These requirements include **ALL of the items included in Part 104.210 (b) (1) (Qualifications) and (b) (2) (General Knowledge) required for the CSO** and the additional requirements for experience related to:

a. Security administration and organization of the company's vessel(s);
b. Vessel, facility, and port operations relevant to that industry;
c. Vessel layout;
d. The VSP and related procedures, including scenario-based response training;
e. Crowd management and control techniques;
f. Operations of security equipment and systems; and
g. Testing and calibration of security equipment and systems, and their maintenance while at sea.

As with the CSO, demonstration of competency can be attained either by ***direct knowledge (equivalent job experience)*** ***OR*** ***through*** successful completion of ***documented training***

33 CFR Part 104.215 (c) lists ***11*** *specific additional day-to-day VSO Responsibilities* that the designated security officer must perform as follows:

a. Regularly inspect the vessel to ensure that security measures are maintained;
b. Ensure maintenance and supervision of the implementation of the VSP, and any amendments to the VSP;
c. Ensure the coordination and handling of cargo and vessel stores and bunkers in compliance with this part;
d. Propose modifications to the VSP to the Company Security Officer (CSO);
e. Ensure that any problems identified during audits or inspections are reported to the CSO, and promptly implement any corrective actions;
f. ***Ensure security awareness and vigilance on board the vessel***;
g. Ensure adequate security training for vessel personnel;
h. Ensure the reporting and recording of all security incidents;
i. Ensure the coordinated implementation of the VSP with the CSO and the relevant Facility Security Officer, when applicable;
j. Ensure security equipment is properly operated, tested, calibrated and maintained; and
k. Ensure consistency between security requirements and the proper treatment of vessel personnel affected by those requirements.

In summary then – although significant broad requirements are placed on the FSO, CSO, and VSO under ISPS Code and MTSA 2002 mandates, ONLY the FSO is required to undergo documented formal training. Meeting knowledge requirements for designation of CSO and VSO personnel can be attained via job experience alone. FSO, CSO and VSO personnel can be "multi-hatted" and perform other activities and duties concurrent with their security functions. In addition to general knowledge and qualifications, the regulations require compliance and oversight of anywhere from 11 to 14 specifically defined and described "day-to-day" responsibilities for FSO, CSO and VSO personnel as applicable.

Identification of "Others" with Security Duties:

The MTSA 2002 regulations contained in 33 CFR Subchapter "H" specify several other categories of required ***demonstrated job experience and/or formal documented training*** as follows:

- Company or Vessel Personnel with Security Duties (33 CFR Part 104.220)

- Security Training for ALL Other Vessel Personnel – including contractors and whether FULL, PART TIME, TEMPORARY or PERMANENT (33 CFR Part 104.225)
- Facility Personnel with Security Duties (33CFR Part 105.210)
- Security Training for ALL other Facility Personnel – including contractors and whether FULL, PART TIME, TEMPORARY or PERMANENT (33 CFR Part 105.215)

The regulations require the MTSA Security Officer to ***designate*** those with specific security duties at a regulated facility or vessel. However, there is little regulatory policy or guidance which describe the ***types of duties*** which may require training – leaving this determination to the individual responsible in each location. Clearly, in the maritime mode, these definitions will be influenced and largely set by the requirements stipulated in each ***facility or vessel security plan*** as it addresses the required changes in security posture driven by changes in the MARSEC level. Therefore the number of individuals requiring specific training and the type of training required will likely vary from facility to facility, ship to ship and from security level to security level.

Once the responsible Security Officer has determined who falls within these categories, the regulations specify that the Security Officer must ensure those with such defined security duties be "trained" or have documented job experience that meets the minimum standards. At today's complex terminals where job duties and descriptions are becoming more and more intertwined, there are many persons who have designated security duties as a part of their overall job functions – but not as a primary duty function. These personnel might include operations and maintenance crews, engineering staff, computer technicians and even office reception personnel in addition to guards, watchman and roving patrols.

Given these various positions – how does one determine exactly what training and to what level of sophistication is necessary to meet the regulatory requirement, to add necessary value to the overall security capability, and to maintain balance between the dynamic forces of business commerce and workable security practices?

An example of a typical terminal employee requiring specific security training would be ***an assigned entry access gate guard*** – who may or may not be 100% employed in this job function.

EXAMPLE #1: What exactly does a *"gate guard"* need to know?

Modern port terminals utilize a variety of techniques and technology to maintain basic security at the entry location. These access measures may – or may not - include the physical presence of a watchman or security guard "at the gate" but might also include the use of CCTV access measures, motion sensors, gates and physical barriers, biometric card readers, fingerprint scanners or other control technology – or combinations of all of

these and more. As the MARSEC level changes and as required by the FSP or VSP for the facility or ship, the specific functions and duties of the "gate guard" will change and become more restrictive as the security level increases from MARSEC Level 1 to 3.

Below are some of the typical duties which might be expected of persons performing these job functions and the level of knowledge and/or training required:

1. Access control measures
   - TYPES of *Identification Cards Approved and Accepted*
   - *TYPICAL Variations in state issued Drivers Licenses*
   - *TECHNIQUES for Identification and Handling of Suspected Forged Documents*
   - *Log Keeping Requirements*
   - *Inspection and Screening of Personnel*
   - *Inspection & Screening of Vehicles/Trucks/Containers and Cargo*
   - *PROCEDURES for Handling Illicit or Prohibited Materials or Items*
   - *Specific Access Control System Requirements UNIQUE to the Facility or Vessel*
   - *PRECEDURES to Implement should someone decide to Violate Access Control*
2. Emergency procedures for notification
3. Handling ship stores and screening
4. Handling ships crews and visitors
5. Security monitoring procedures
6. Security for restricted areas
7. Telephone/Radio communication procedures
8. General security awareness
9. Maintenance procedures and corrective action
10. CCTV systems and controls
11. Actions to be taken in the event of a leaking product
12. Reporting of security breaches and incidents
13. Weapons handling

These job elements may very well differ for each job station assignment, at each terminal location, and for each vessel -- therefore the training required must be flexible and tailored to the specific facility or vessel application and operational environment.

EXAMPLE #2: What does a *Roving Patrol* need to know?

Some terminals are so large or complex that the use of a physical security element which patrols the grounds & observes security measures throughout the facility is necessary. This requirement may be tied only to increased MARSEC levels or may be in place as a routine element of security at MARSEC Level 1. Sometimes random roving patrol duties may be an additional responsibility of the access gate guard. Additionally, ***ANY*** individual moving through the terminal can serve as an augment to security as additional "eyes and ears" and therefore should have sufficient baseline knowledge and "awareness"

to add value to the terminal security measures. The following elements are typically included as guidance for roving patrol activities:

1. Physical security including;
   Open or Inoperable Gates and/or Fencing Damage
   Inadequate or Non-Operational Lighting
   Observation Techniques & Reporting Procedures
   Required Personnel ID Badges on Display
   Required Vehicle Passes and Requirements
   Enforcement Procedures
   Emergency Management Procedures
   Initial responder HAZWOPER requirements – Notification, Isolation, and Containment if properly trained and capable.
2. Identification and management of facility support contractors, ships crews, visitors and chandlers/contractors and vendors
3. Security monitoring procedures
4. Designation and Location of Restricted Areas and Measures; Procedures for Entry and Management
5. Telephone/Radio Communication Procedures
6. General Security Awareness
7. Maintenance and Corrective Action Policies and Procedures

Basic questions associated with these examples – as well as other training categories where formal documented training is an OPTION rather than a requirement – include the "yardstick" metric by which one measures and determines *"competency" originating only from job experience* and by what *means and methods* the USCG uses to *validate that level of competency*?

Further -- What standards apply to other personnel (maintenance, computer technicians) who may have basic collateral duties that involve security –What do they REALLY need to know? Who decides and how is this accurately measured and validated?

The job elements and descriptions for the many of these "other personnel" – and the knowledge and/or training sophistication required of them -- that the regulations stipulate and requires for those with "security duties" have yet to be determined, validated or tested as a functional part of the overall security umbrella in the MTS in many instances.

Beyond managerial and operational considerations, these factors become even more critical since the regulations provide civil penalties up to $25,000 per violation (and each occurrence can be counted as a separate violation) for failure to "comply" with the provisions of 33 CFR Subchapter "H". Therefore in the absence of specific guidance to the contrary – the potential confusion, implementation errors, program inefficiencies, inadequacies and the resultant major likelihood for both operational and liability exposure for facility and vessel operators is clear.

Review of IMO ISPS and MTSA 2002 Model Courses:

During the beginning of the maritime security program development, Model Courses were developed for training FSO, CSO and/or VSO personnel -- first by the International Maritime Organization (IMO) for the ISPS Code and later by MARAD and the USCG for MTSA 2002 compliance - which provided *only the most general most basic of content outlines* acceptable by these entities to meet the necessary training requirements. Both the IMO and MARAD/USCG Model Courses are guidelines that if followed -- and properly approved via authorized agencies of government -- will result in "certification" of the curriculum. However, there is no current regulatory mandate that requires training for FSO, CSO or VSO be accomplished through a *"certified" curriculum*. Any *"compliant" curriculum* – and by definition this is one that includes all topical aspects of the model course outlines regardless of depth of detail or the efficacy of the training provider -- is typically being accepted regardless of the source of the training.

Currently, "acceptable training" can be accomplished via "in house" capability where a senior "experienced" person designs and delivers the training to those less experienced personnel; via a "compliant" training course that has NOT been vetted or approved by the cognizant governmental agency; or via a "certified" course that HAS been vetted through an agency approval process. This situation establishes conditions where major variations in course delivery, accuracy and validity can occur, where the traditional academic vetting process is not being applied and where independent control of the content and currency of the materials does not occur UNLESS the course has been "certified".

Review of existing courses offering training in maritime security:

Currently, courses approved and "certified" by the Maritime Administration and the US Coast Guard for FSO, CSO, VSO security officers are 2-3 days in length and undergo scrutiny for content, approval of instructor qualifications and the mechanics of delivery. These courses typically are validated and documented by a testing requirement upon completion of the course. This process matches the IMO and MTSA Model Course outlines, policies and procedures. As stated above, however – non-certified courses ARE allowable so long as they *comply* with the basic course outline and need not include a testing requirement. These courses are not subjected to any further scrutiny or evaluation upon review of documentation that the course was performed and this can be accomplished through completing and filing a roster of attendance and participation.

There are *no established IMSO or USCG model courses or approved certified curriculums* for training individuals with "other security duties" or for those personnel who routinely perform work on regulated facilities or vessels – particularly for training at the lowest – or "awareness" – level. Compliance with awareness level training typically is performed "in house" by the company or via contract with an outside vendor and

typically is one to two hours in length. These courses may or may not involve validation by testing at the completion of the training, but documentation of the training through use of an attendance roster is typical.

Some states such as California have implemented specific, targeted training requirements for security positions. California has a mandatory course for ***LICENSED*** Security Guards which is four hours in length and follows a model course outline. This course has similarities to a general security awareness course under current maritime security requirements. However, in California – where there are both licensed and unlicensed security officers and guards comprising about a 50%-50% ratio – only the licensed guards require training as of this writing.

In general, all currently available courses offered to meet ISPS Code and MTSA 2002 requirements *lack elements that provide for the* ***transition of "theory into practice".*** Practical training, examples of field techniques, methods, employment of equipment and the actual conduct of security operations and tactics in the field ARE not typically included as a component of the current training regimen.

CMA and its training partners – AMERGENT TECHS and BlueWater and Associates -- are working to develop the next generation of practical, applied security training that extends beyond the basic regulatory framework, history and theory of maritime security. These courses will be intensive, modular formats of one to two days that will include "practical laboratories" that will demonstrate capabilities and provide hands-on experience for the attendees that can be readily employed at their facility or vessel. Other courses – such as a more sophisticated Maritime Security Awareness course -- are tailored for delivery on-line via the internet and is available now. This format allows attainment of vetted minimum standards at the awareness level on a flexible 24/7 delivery schedule where the student can enter and leave the site at any time.

Some of the MARSEC courses being developed are:

- Practical Maritime Security for Land-Based Emergency Response Personnel
- Applied Maritime Security Planning for Land-Based Emergency Planners
- Physical Security Methods, Techniques and Tactics for the Port and Maritime Environment
- Security Preparedness, Detection, and Deterrence Strategies in the Commercial Port Environment for Attainment of Rapid Continuity of Business Operations
- Applied Drill and Exercise Strategies That Actually Work and Add Value – Integrating the "ALL HAZARDS" and "SECURITY" Preparedness Process.

These courses will begin to build upon the current minimum training baseline and will advance the competency and capability of the entire preparedness and response community.

What Training IMPLEMENTATION CHALLENGES are being Observed in the Field?

Where are shortfalls in security being observed in the field?

- The ISPS Code and MTSA 2002 regulations focus facility and vessel training, drill and exercise requirements inside their own footprint and de-emphasize external mutual aide and cooperative planning and response activities
- The application of the regulations do not differentiate according to the size of the operation beyond the baseline regulatory applicability – so if you meet the regulatory threshold, you are required to attain all of the requirements regardless of frequency of operation or personnel compliment. How then to establish an equitable and effective program to conduct drills and exercises for a facility in intermittent use with a personnel staffing of only 3-10 people?
- Most Exercises – particularly the regional or area exercises -- are focusing on *command and control, emergency response and mitigation capabilities* and not in *preventative security measure, training, tactics and logistics required to implement these additional measures in the commercial port environment*. The ISPS Code and MTSA 2002 drive the regulated community primarily towards development of preparedness and deterrence strategies rather than defense – and rightly so since these facilities and vessels have limited or non-existent self-defense capability.
- Facility and Vessel security guard staff failure to understand or be fully knowledgeable regarding new security responsibilities established by ISPS Code, MTSA 2002 and FSP/VSP provisions.
- Security Guard staff not receiving adequate practical training to meet facility or vessel needs.
- Job functions not well defined for gate guards and roving patrols. Some are over tasked with entry functions, log keeping, monitoring camera systems, delivery functions, directions, mail pickup/drop-off and maintenance functions in addition to vigilant security observations.
- First responder HAZWOPER training not provided where needed for roving patrols.
- Due to restrictive Sensitive Security Information being required & implemented under 33 CFR Subchapter “H”, security guards and supplemental staff are not authorized to access and utilize the FSP/VSP
- Companies are relying upon contract vendors to fulfill mandatory training with “compliant” curriculums without vetting the validity of the training and post

verification with individual personnel of their efficacy and value of the training once complete to assure it is meeting expectations and requirements.

- Failure of security staff to "positively ID" everyone entering the facility or boarding the ship and allowing entry to "known" persons they recognize without viewing proper identification
- Gate Guards are not provided information and training on the various state licenses, proper forms of identification and fraudulent documents.
- Documentation difficulty in recording which persons were randomly screened at the gate.
- Inability to confirm inbound and outbound traffic when there are multiple entry and exit gates. A person entering one gate can not be confirmed exiting another gate.
- Persons denied entry are not documented, recorded, photographed or the Security Officer notified.
- Gate Guards do not know how to use vehicle screening and inspection mirrors/equipment; are not randomly selecting vehicles for screening; are screening only first time arrivals and not subsequent trips; vehicles are allowed to depart without any screening; and in some cases are not well informed as to what to look for in screening
- Security staff has difficulty monitoring the many cameras and surveillance equipment now commonly installed and in-use.
- Facility security "boundary lines" are not well understood; are incorrect; or do not assume set back or blast radius characteristics.
- Waterside monitoring is non-existent, not well defined in the FSP/VSP, or has not been tested or validated for practicality or feasibility of operations.
- Planning assumptions in the FSP/VSP often defer to conventional 911 or USCG National Response Center triggering mechanisms for notification of a TSI, yet the practical aspects of assuring and validating the efficacy of these assumptions has often not been tested.

There are many other issues still being dealt with by security and regulatory agencies. We are still finding stowaways, illicit drugs and stolen cars moving in the maritime environment. We are still experiencing thefts at our terminals. This raises our concern over our present level of security capability and employment overall. If the occurrence of these incidents and illicit operations are continuing with all of the present emphasis on security – particularly TECHNOLOGY BASED SECURITY SYSTEMS - how easy will it be for others to conduct active terrorism in our ports? What else can and should be accomplished? Is improved training and leveraging of the "Human Element" the only way to improve effective security capability?

Unfortunately – under the current versions of the ISPS Code and MTSA 2002 – attaining *regulatory compliance by the maritime community has been the goal.* "Regulatory compliant" typically means meeting a minimum standard rather than attainment of optimum practical and workable security objectives that make the MTS and all of us safer.

Implementation timelines and the urgency of the security and terrorism problem have left enforcement entities at all levels – internal and external -- struggling with the rapid changes in maritime security. Selection and proper application of new security measures using a sliding scale reflecting the presumption of a properly conducted and accurate security assessment have taken precedence over long term strategic planning and development of protocols that are sustainable over time. Fortunately, the level of recognition, lessons learned and practical enforcement has been increasing as Security Officers are learning their jobs and shortfalls are being recognized.

KEY OBSERVATIONS: Conclusions and Recommendations

1. Often FSO's/CSO's are also Safety Officers, Health Officers, Environmental Protection Officers, Training Coordinators and Quality Assurance Representatives or some combination of the above. This dilutes the ability of a security officer to focus on the variety of security issues. While they may be meeting the knowledge requirements, they may be unable to meet the focus and demanding role of a security officer. With today's level of security, this may or may not be acceptable. As the maritime risk increases, so will the need to focus and improve maritime security. Unfortunately, waiting for these changes also makes facilities and vessels more vulnerable to security risks.

2. The US Coast Guard and other government entities are offering free "short term security officer seminars and workshops" as a public service which are sometimes being considered equivalent to full security officer courses by attendees – and they are using these to meet the "compliance" requirement. Attendees learn the absolute minimum necessary to be regulatory compliant but miss the intent of the regulations. These programs are intended to provide already qualified personnel with new information and local security concerns – not to fulfill the overall ISPS Code and MTSA 2002 mandate. Yet, if no one is validating and vetting the efficacy and applicability of this training – it will continue to be used to "get the ticket punched".

Other Observations Include:

- Existing MARSEC courses are not meeting the overall expectations of Industry
  - Industry has attended courses and provided feedback for improvement
  - The US Coast Guard has been issuing citations to facilities for non-compliance
  - The industry expects some standard guidance or policy defining positions and training elements for personnel with security duties – or ALL personnel will require training beyond the Awareness Level
  - Security knowledge – what works and what doesn't -- has improved since MTSA and but largely has not been incorporated into training standards

- Security positions rotate among many personnel, high turnover rates and collateral duties impact ability to maintain security
- Advanced Practical and Applied Security Courses are not available, but are being developed
- There is no "refresher training" for attaining currency available nor is it currently required by regulation.
- There is no impetus to improve the content or scope of existing maritime security training programs since "compliance" can be attained through many venues and pathways.
- The complex of organizations with stakeholder involvement – and sometimes directly competing interests -- including ports, terminal operators, PMSA, Union organizations, private security firms, USCG, and Customs officials are impediments to developing and implementing uniform, sustainable and workable security.

- Currently in the United States, ONLY FSO's are actually required to attend formal documented training

  - The regulations in 33 CFR specify training or equivalency for the FSO, CSO and VSO as well as those with security duties and all others on a facility.
  - The international standards establish no specific training requirements
  - CA State requires licensed "Security Guards" to attend a four hour course on terrorism and security awareness – but this only covers about 50% of the commercial security guard demographic. Unlicensed guards are not required to perform specialized security training
  - Where and How do the "other personnel with security duties" obtain their knowledge and documented experience? Who validates and accepts this criteria and against what standard?
  - What security duties are expected of "other facility and vessel personnel" and how will they be assessed and/or trained?

- The specified length of "training" or experience required to meet the job knowledge criteria is ill defined:

  - Today, everyone with even the most minimal experience is a maritime security expert in the absence of established "certification" requirements
  - Existing military courses on physical and maritime security are often weeks in length. The total training curriculum contained in these courses will not be necessary or fully applicable to a civilian business environment, but they make for an interesting comparison and skills inventory that can establish a new baseline for revised standards. Some examples of other training courses are:

    - US Army Physical Security Course alone is 80 hours and covers:

- Lock and Key Control
- Perimeter Barriers & Lighting
- Electronic Security Systems
- Physical Security Requirements For Arms & Ammunition Areas
- Physical Security Requirements For Facilities & Equipment
- Develop/Review Physical Security Plans
- Security Management System (SMS)
- Physical Security Inspections & Surveys

- US Navy Physical Security Training is a 3 credit course (3 week equivalent)

- American Society for Industrial Security (ASIS) ***Physical Security Course*** ALONE is 3 days in length.

- Supply chain security is still not a reality – Note continued thefts, pilferage, migrants, drug smuggling, etc
- Very little communication occurs between arriving ships and facilities beyond confirmation of arrival. All newly required NOA information stipulated by the 96 hour advance notification flows via the USCG and may or may not actually arrive at the facility in time to be of any use.
- Declarations of Security are required and completed for only a few vessels eliminating improvements by learning the security shortfalls during DOS conferences between the VSO and FSO.

In the near term, IMO plans to incorporate the requirements for VSO training into the licensing program governed by STCW. The target for this implementation is 2009 and the United States will meet this deadline. It is likely that similar requirements will be forthcoming for CSO and FSO training. When this occurs, all MARSEC courses will likely require vetting and approval through the STCW certification process or by similar venue.

To assure uninterrupted business operations and employment, it is strongly recommended that personnel, unions and companies utilize:

1. "Certified" training vendors who have been through the vetting process and attained IMO/USCG/MARAD designation
2. Reach out beyond the minimum compliance standard and seek practical applied training for sustainable, workable field operations.

Questions regarding certified FSO/CSO/VSO training and advanced practical training in MTS Security can be obtained by contacting:

The California Maritime Academy
(707) 654-1156 or by visiting our web site at www.maritime-education.com