5th Annual Symposium, Mary Kay O'Connor Process Safety Center
"Beyond Regulatory Compliance: Making Safety Second Nature"
Reed Arena, Texas A&M University, College Station, Texas
October 29-30, 2002

A Coastal Perspective on Security

Steven D. Emerson
Emerson Technical Analysis, LLC
921 N. Chaparral St.
Corpus Christi, TX 78401, USA
(361) 880-8145,
Emersonanalysis@aol.com

LCDR John Nadeau[1]
US Coast Guard
Marine Safety Office Corpus Christi
555 N. Carancahua St.
Corpus Christi, TX 78478, USA

Abstract

This paper examines security issues from the unique perspective of our nation's coastlines and associated infrastructure. It surveys ongoing efforts to secure offshore shipping lanes, as well as the transportation systems and huge capital investments on the narrow strip of land intersecting with coastal waters.

The paper recounts the extraordinary demands recently placed on the Coast Guard, port authorities and other agencies charged with offshore security. New federal requirements such as port assessments continue to be mandated, while solutions to funding are still unfolding. An up-to-date summary of maritime security functions is provided.

Those requirements are compared and contrasted with security guidelines and regulatory demands placed upon mobile and fixed assets of the Chemical Process Industry (CPI) in coastal environs. These span the gamut from recommendations by industry groups and professional organizations, to federal and state requirements, to insurance demands, to general duty obligations.

Introduction

It has been estimated that more than 95% of our country's commercial tonnage is shipped on our nation's ports and waterways. During the next 20 years that total volume of goods is expected to double. With over 95,000 miles of shoreline and 25,000 miles of navigable waterways, the US represents a formidable presence to be secured. When coupled with the enormous production infrastructure that has grown up in coastal areas to access waterborne shipping, the task of maintaining security for the combination is enormous.

---

[1] The views expressed herein are the opinions of the author and not necessarily those of the Department of Transportation or the US Coast Guard.

The sudden reach of terrorism into our midst on September 11, 2001 forever changed the way that waterways, ports and on-shore facilities are secured. In certain cases, governmental agencies have been charged with more responsibility. In others, legal and regulatory obligations place increasing emphasis on corporations and private ventures to secure their assets and to protect the public.

PART 1 – ON-SHORE SECURITY

Before September 11th

Concern with security is not new. Over the last several years, federal and state agencies created emergency organizations to respond to terrorist threats. A partial list of federal agencies charged with some aspect of counter-terrorism is shown below.

FEMA Rapid Response Information System (RRIS)	Coordinates major federal chemical and biological emergency response resources
National Response Team (NRT)	Coordinates 16 federal agencies with responsibilities, interest and expertise in various aspects of emergency response to pollution incidents
National Domestic Preparedness Office (NPDO)	Aware of federal assets and expertise on "Weapons of Mass Destruction" (WMD)
Interagency Task Force on Domestic Terrorism	Concept of Operation Plan, developed through 6 federal agencies, outlining response to WMD attack
EPA Chemical Emergency and Prevention Office	Administers EPA's Risk Management Planning (RMP) regulation
EPA Office of Emergency Response	Coordinates response to spills of hazardous substances
EPA Office of Water	Coordination to ensure safety of nation's water supplies
EPA Emergency Response Team	For nationwide deployment
DoD U. S. Army Soldier and Biological Chemical Command's Homeland Defense Unit	To enhance response capabilities of military, federal, state and local emergency responders
FBI Awareness of National Security Issues and Response Program (ANSIR)	FBI office for espionage, cyber and physical infrastructure protection, and national security issues

Table 1. Federal governmental agencies with counter-terrorism responsibilities.

Before September 11th it was safe to say that prevention of accidental releases received far more attention than did securing process chemicals against intentional release. In the mid-1990's, EPA's *Accidental Release Prevention and Risk Management Planning* regulation (40 CFR Part 68) mandated that much of the nation's process industries evaluate and publish "offsite consequences" from worst case scenarios of releases of certain regulated chemicals. It also required a five-year accident history, along with documentation of management systems employed in safety, accident prevention, emergency preparedness and response.

However even before September 11th widespread publication of inventory details for these chemicals, along with their predicted worst-case offsite consequences, stirred genuine concern within the regulated community. Industry representatives made the case to Congress that such information should not be so easily available. On the other hand, environmental groups argued that publication served a vital public information role, and secondarily provided those being regulated with incentive to reduce inventories along with risk to nearby residents.

In 1999, Congress acted on the issue and passed Public Law 106-40, *The Chemical Safety Information, Site Security, and Fuels Regulatory Relief Act*, attached to the fiscal year 2001 Appropriations Bill. Among other requirements, it sharply restricted access to offsite consequence analysis information, mandated an overall review of industry's security measures and required an analysis of susceptibility to breach of chemical stores. The program was administered through the U.S. Department of Justice, which selected the Sandia National Laboratory to broadly evaluate security within the industry and come forward with a Security Evaluation Methodology. The DOJ later forwarded Sandia's report to Congress on their findings after review of selected facilities.

After September 11th

On October 8, 2001, President Bush signed Executive Order 13228 creating the Office of Homeland Security. Current press accounts question the eventual structure and status for the office, but its charter to consolidate the role of securing the nation continues to be pursued.

Apparently, President Bush's National Strategy for Homeland Security identified EPA as the lead federal agency for the so-called "critical infrastructure – chemical industry", and an official has been named Director – EPA Homeland Security Office. As of late summer 2002, EPA announced plans to add security requirements for all RMP regulated facilities. EPA envisions mandating the performance of "Vulnerability Assessments" according to standard methodologies. In addition, EPA is likely to mandate some measure of "inherently safe technology", not according to prescriptive standards but through a performance-based approach. One example frequently cited is to minimize inventories. Finally, EPA will expect third-party certification of the performance of a Vulnerability Assessment, adoption of specific security activities, and setting a timetable to address remaining identified issues. While EPA does not expect to perform compliance audits immediately they do plan some early field checks.

Congress is also getting into the act. On October 31, 2001, Senator Corzine (D, NJ) introduced S.1602, *The Chemical Security Act of 2001,* described as "a bill to help protect the public against the threat of chemical attack." In late July of this year, the bill was ordered to be reported favorably to the full Senate for vote.

The proposed act would apply to both accidental and intentional acts and cover RMP-regulated facilities, chemical storage and chemical transportation activities. It seeks less usage of "Substances of Concern", it would mandate inherently safer technology, and require improvements to security and mitigation. The act also invokes OSHA's General

Duty Clause to serve notice to owners of covered operations that they are obligated to identify workplace vulnerabilities and rectify shortcomings. The complete legislation is available through trade associations or through the Thomas service of the Library of Congress.

Industrial trade organizations have voiced serious concerns about the legislation in congressional hearings, with compelling arguments. For example, API pointed out that the act would essentially make it a crime to be the victim of a terrorist action, and that inherent safety, while laudable, may actually raise overall risk to society. Comments by the American Chemistry Council repeated some of the same themes, and pointed out the broad reach of the proposed language. Their statements are part of the public record and available through the respective institutes.

Methods of On-Shore Security Assessments

Since September 11th, substantial investments have been made in analytical procedures to explicitly define security risk. The tools are general enough to be applicable to all sorts of installations and facilities, and almost universally have common elements:

1. SCOPE
2. CHARACTERIZE INSTALLATION
   Hazards, consequences, etc.
3. IDENTIFY AND CHARACTERIZE THREATS
   Type, tactics, capabilities, likelihood
4. ANALYZE VULNERABILITY
   Likelihood that safeguards will be overcome
5. SPECIFY COUNTERMEASURES
   Evaluate layers of protection
   Delay, Detect, Respond, Mitigate
6. REPORT/ COMMUNICATE

The theme is to recommend a performance-based approach to application of limited risk analysis resources. Virtually all analytical procedures can be summarized as (1) look inside, (2) look outside, (3) look inside again. That is, the procedure is to (1) determine the chemical hazards present and calculate the consequences of a breach of containment, (2) enumerate malevolent forces with the capability to cause a breach and (3) consider how well safeguards thwart such a threat.

Obviously a high quality analysis requires experienced and professional evaluation.

Elements of On-Shore Security

Operators of fixed facilities bear the responsibility to secure their assets against intentional breach. The conventional approach to security systems is to install rings or layers of protection, that is, successive hurdles that must be successively overcome before vulnerable assets are reached.

Security professional emphasize the four key steps to intercept and neutralize a threat:
DETECT/ DELAY/ RESPOND/ MITIGATE.

Detection typically features hardware coupled with human interpretation, such as cameras and sensors that feed information to security personnel. Delay of attack largely relies on geography, that is, buffering a facility with wide approaches, ringing assets with fence and locked gates and doors to impede approach. Response strictly requires personnel, in most cases trained operators who can either intervene between the threat and an asset or immediately act to thwart the attack. Mitigation needs preplanning, equipment design and trained operators, skilled at interpreting the nature of a breach and deciding on effective procedures to neutralize the impact. Examples include water deluge systems, and calling for shelter-in-place or evacuation of downwind populations. Mitigation also requires follow-up from law enforcement and emergency response organizations.

PART 2 – OFF-SHORE SECURITY

In contrast with on-shore where facility operators bear prime responsibility, the U. S. Coast Guard is tasked with safeguarding the nation's ports and waterways. Each year approximately 10,000 commercial vessels transit US waterways and visit our ports. In doing so, they often traverse near dense populations, pass under bridges carrying hundreds of thousands of motorists each day, and dock at thousands of facilities handling a wide variety of hazardous substances. Rep. Frank LoBiondo of New Jersey, Chairman of the House Subcommittee on Coast Guard and Maritime Transportation, put the Coast Guard's responsibility into perspective: "*Protecting our ports and maritime transportation system is of critical importance to our nation, as the maritime industry contributes $742 billion to the gross domestic product each year, and the ripple effects from an attack on one or more of our ports would be felt throughout the economy of the nation.*"

As a country, we have taken many steps to increase airports security, however these efforts may force terrorists to search for alternate means of inflicting harm. While airports are typically confined and protected on all sides with restricted access, ports are intended to promote the flow of commerce. Thus they are usually open and exposed on the coast, and not governed by any single national authority. Instead, a unique combination of federal, state and local governments, often with overlapping jurisdictions, manage each port.

Layered Defense Offshore

Commandant of the Coast Guard, Admiral Thomas Collins presented an interesting analogy when he compared efforts to protect a port to actions each of us may elect to secure our home. We feel safest living in a home located in a gated community with an active neighborhood watch and police force, surrounded by an electronic perimeter fence, protected by a monitored alarm system, with doors secured by a solid deadbolts, our valuables locked in a safe in our bedroom, and a mean, hungry dog roaming freely about the house.

This concept of "layered defense" can be applied to seaports. We must be aware of potential threats, possess the capability to deter them, inventory and protect our valuables, increase the visibility of our "police" force, and work together with our neighbors. For the Coast Guard, layered defense can be broken down into four zones: foreign ports, offshore, coastal, and dockside.

Layer 1 - Foreign Ports Zone

To best protect our ports, we must detect, intercept and interdict potential threats as far out to sea as possible. Defensive efforts can begin where the shipment originates, at the country of origin. Ideally, we mitigate security threats long before they arrive in US waters by working with other countries throughout the world. Fortunately, the International Maritime Organization (IMO), established by the United Nations in 1948, has 162 member nations that have pledged cooperation in maritime safety, navigation and pollution prevention.

Currently IMO is developing international standards for port, facility and ship security, under their most aggressive timeline ever attempted. A proposed *International Code for the Security of Ships and Port Facilities* (ISPS Code) will likely have the largest impact. It consists of two parts, one mandatory and the other recommended. Recognizing that ship and facility security is essentially risk management, the ISPS Code sets forth a standardized, consistent framework for risk evaluation, which facilitates meaningful information exchange between governments, companies, facilities, and vessels.

If adopted in current form, the ISPS Code will require each nation to set security or threat levels and communicate those levels to ships and facilities in its ports. For international consistency, three security levels will be used to describe the degree of risk associated with a security threat against a ship or port facility. Security Level 1 requires minimum protective security measures and must be maintained at all times. Security Level 2 introduces additional measures to meet heightened risk, while Security Level 3 is activated when a security incident is deemed probable or imminent.

Vessels will be required to develop Ship Security Plans and employ Ship and Company Security Officers. Similarly, each port facility (defined as a location where interaction takes place between a ship and port) will craft a Port Facility Security Plan, and name a Port Facility Security Officer. Both sets of security plans must enumerate measures to maintain Security Level 1, and report those additional actions taken when moving to Security Levels 2 and 3. Additionally, both vessels and facilities must monitor and control access, and conduct general security training and drills.

Prior to developing the Port Facility Security Plan, each facility will perform a Vulnerability Assessment describing criticality, threat, and vulnerability of assets and infrastructure. Results are distributed only to those with a "need to know".

The ISPS Code will also allow governments to impose additional control measures on any visiting foreign ship if it has reason to believe the ship or cargo have not been secured for the entire journey. Similarly, the *Maritime Transportation Antiterrorism Act*

of 2002 (H.R 3983), passed by the U.S. House of Representatives, and a companion Senate bill, the *Port and Maritime Security Act of 2001* (S. 1214), contain provisions requiring the Coast Guard to assess effectiveness of antiterrorism measures at foreign ports. For a vessel arriving in the US from a port which has ineffective security measures, or any vessel carrying cargo originating from or transshipped through such a port, the Coast Guard may deny entry or prescribe conditions deemed necessary to ensure the safety of US ports and waterways. For example, if the Coast Guard believes that containers aboard a foreign flag ship were not secure while waiting to be loaded in a foreign port with ineffective security, the vessel and all of its cargo may be required to undertake additional security measures, which may include delays, detentions, restrictions on operations, or even denial of entry or expulsion.

IMO has also proposed that a security alarm be installed on each ship. When activated, the alarm would transmit a ship-to-shore security alert identifying ship, location and status of the threat or security breach. The alarm would sound continuously until deactivated by authorized personnel, but the alert would not be sent to other ships or alarm onboard.

Layer 2 - Offshore Zone

The offshore zone generally refers to waters inside the 200-mile exclusive economic zone (EEZ) but beyond the 12-mile territorial sea. In this zone, ships bound for the US are now required to provide Advanced Notice of Arrival (ANOA) at least 96 hours before entering port. The ANOA must identify vessel, cargo, owner, operator, and crew, including crewmember dates of birth, citizenship, gender, position or duties, passport numbers and visa numbers. The Coast Guard processes this information to identify vessels or crew that may pose a substantial security risk. Before entering port, vessels of interest undergo Port Security boardings conducted by armed Coast Guard members. In New York Harbor alone, over 2,000 vessels have been boarded since September 11th.

Fig. 1: Tank ship undergoing Coast Guard Port Security boarding prior to entering port.

Another Coast Guard initiative is in Maritime Domain Awareness (MDA). Admiral Collins has stated that MDA is "possessing comprehensive awareness of our

vulnerabilities, threats, and targets of interest in the water." It means that the Coast Guard's level of knowledge about ship cargo and crew is increasingly comprehensive and specific, as the potential threats move closer to the United States. A large part of detection and deterrence in this zone is accomplished by the increasing presence of Coast Guard and Navy ships, cutters, and aircraft.

Another new development to enhance MDA is installation of Automatic Identification Systems (AIS), designed to automatically provide information about a ship to shore stations, other ships, and aircraft. As of July of this year, each newly built vessel must be fitted with AIS, while IMO established a timetable to have AIS installed on existing vessels by July 2008 or earlier.

Layer 3 - Coastal Zone

The coastal zone is generally considered to extend inward from the 12-mile territorial sea to the docks and piers inside each port. Distances, transit times, threats, vulnerabilities, and potential consequences vary widely among US ports. For instance the voyage into Point Comfort, TX is 24 miles long, passing through relatively barren and sparsely populated areas. In contrast, the transit into Houston, TX is 50 miles, winding near approximately 50 chemical facilities. Similarly, tank ships loaded with liquefied natural gas pose a relatively low risk when they visit isolated ports in Lake Charles, LA, yet when these same vessels pass through downtown Boston, MA only a stone's throw from Logan Airport, they are considered a significant risk and receive a great deal of attention.

Since September 11th, certain "high interest vessels" are escorted into port with armed Coast Guard members on board to prevent these vessels from being used as weapons of mass destruction. These boarding teams, serving as Sea Marshals, provide security to the pilot and crew during transit and diminish the potential for hijacking by maintaining positive control over the vessel's propulsion and steering.

Fig. 2: Sea Marshals secure the bridge of a vessel as it transits into port.

To prevent the possibility of a U.S.S. COLE-type attack involving a suicide strike from another boat, Coast Guard vessels escort some ships into port.

Fig. 3: The Coast Guard escorts a ferry in Seattle, WA.

Under the authority of the Ports and Waterways Safety Act (33USC1221), the Coast Guard may establish "security zones" to safeguard ports, waterways, vessels and waterfront facilities from destruction, loss, sabotage, or other subversive acts. To control vessel traffic and limit access to high consequence or vulnerable areas, approximately 115 different security zones have been implemented since September 11th in various ports throughout the US. Activities within each security zone are unique, but typically they restrict other vessels from nearing a particular facility, another vessel, or a specified geographic area. Similarly, Naval Protection Zones are implemented in all US ports. Unless specifically authorized by the US Navy, all vessels must stay at least 100 yards away from any naval vessel owned, operated, chartered, leased or under the operational control of the US Navy.

Lastly, vigilant presence also serves as a strong deterrent in the coastal zone. Since September 11th, the Coast Guard conducted over 35,000 Port Security patrols.

Fig. 4: Coast Guard members conduct a Port Security patrol.

Layer 4 – Port/ Dockside Zone

The last zone of defense is at our docks and piers. Regardless of what IMO ultimately adopts for international security requirements for ships and facilities, the United States will implement standards at least as stringent. Both the U.S. House of Representatives' *Maritime Transportation Antiterrorism Act of 2002* (H.R 3983) and the companion Senate bill, the *Port and Maritime Security Act of 2001* (S. 1214)[2], contain legislation requiring Port Vulnerability Assessments (PVA). The Coast Guard will be required to conduct these assessments for each port with high risk of catastrophic emergency, defined as "any event caused by a terrorist act that causes, or may cause, substantial loss of human life or major economic disruption in any particular area". Each assessment must list facilities located in the port, including any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction of the US.

Under the bills, the Secretary of Transportation shall prepare a National Maritime Transportation Antiterrorism or Security Plan, which will coordinate federal, state, and local efforts to deter and minimize damage from terrorist attacks. The results of the PVA will be employed in establishing the National Maritime Transportation Antiterrorism Planning System. The plan will designate geographic locations that must develop their own Area Maritime Transportation Antiterrorism or Security Plans. Vessels and facilities most likely to be subject to an act of terrorism will be designated by the Secretary and must submit security plans for approval. Each plan will require periodic renewal and must:

- Identify the Qualified Individual (QI) with authority to implement antiterrorism activities,
- Require immediate communications between the QI and appropriate authorities,
- Identify and, where necessary, contract resources for antiterrorism measures, and
- Establish employee training and drill requirements.

H.R. 3983 and S.1214 both offer financial assistance to enhance security. To receive federal funding, a project must be related to the Area Antiterrorism Plan. In most cases, federal funding shall not exceed 75% of the total cost unless the cost of the project is less than $25,000. It appears $75 million is to be appropriated each fiscal year from 2003 through 2005.

Local Port Security Committees (PSC), required by S. 1214, are being formed in each port. Each PSC, chaired by the local Coast Guard Captain of the Port, includes representatives from the port authority, federal, state and local law enforcement, and the maritime industry, including vessel owners, shipping companies, and facility operators. Each PSC will help coordinate local planning efforts, assist with the port's PVA, and assist with other port security activities.

---

[2] At time of this writing, Congress has recessed for the summer. A joint committee has been named to resolve differences between H.R. 3983 and S. 1214 when the legislators return in the fall.

Similarly, in many ports, representatives from law enforcement agencies such as the Federal Bureau of Investigation, Department of Justice, U.S. Navy, Coast Guard, U.S. Customs, and state and local police have formed Port Intelligence Committees. In some cases, these intelligence committees may even include security managers from larger chemical and petroleum operations. These committees facilitate effective intelligence gathering and communication between all participants.

To restrict access within secure areas, a credentialing system is being established to limit access to those individuals holding valid security clearance. Under the proposed laws, the Secretary of Transportation is required to ensure that such clearance is issued only after individuals have been evaluated and criminal background checks completed. According to S. 1214, clearance will be denied if the background investigation reveals the individual has been convicted within the previous seven years or incarcerated within the previous five years, for committing murder, assault with intent to murder, armed or felony unarmed robbery, unlawful possession, sale or distribution of a weapon, or a similar offense.

In fiscal year 2003, six Coast Guard Marine Safety and Security Teams will be established to enhance domestic maritime security capabilities. Each team, with nearly 100 members and deployable Port Security Response Boats, will be charged with safeguarding the public, and protecting vessels, ports, facilities and cargo from destruction, loss or injury due to terrorist activity. Additionally, they will enhance deterrence "presence" in our ports, enforce Security Zones, and rapidly deploy overseas if called to support other Department of Defense agencies.

Fig. 5: Coast Guard aircraft patrolling over a facility in Houston, TX.

Finally, each Coast Guard Captain of the Port may implement additional local security measures within their respective ports. For example, in the Port of Corpus Christi, TX, all tank ships containing oil or chemical cargoes and tank barges carrying liquefied hazardous gases (LHGs) must provide continuous topside roving patrols while moored in port. Similarly, a moving safety zone, which is designed for safety or environmental

purposes, mandates that all watercraft under 50 feet length stay at least 500 yards away from tank ships carrying LHGs in the Houston - Galveston Port Zone.

Conclusion

In the past, the US was less prepared to detect and deter the enemy that we face today. As we have seen, terrorists are extremely adept at using our own tools as weapons against us. They are quick to learn from their own failures and successes, as well as the failures and successes of other terrorists.

As a nation, we have taken many significant steps to detect and deter future attacks. Taken together, a firm, dedicated public/ private partnership will be necessary to deal with these threats. With vigilance, cooperation, training and preparation that effort promises to be successful.

References:

1. Website for EPA Chemical Emergency Preparedness and Prevention Office (CEPPO), http://www.epa.gov/swercepp/
2. **Dr. Cal Jaeger**, Sandia National Laboratories, report to API Safety and Fire Protection Subcommittee on "Chemical Facility Vulnerability Assessment project Review", December 4, 2001.
3. *The Chemical Security Act of 2001,* S.1602, as passed by U. S. Senate.
4. Website for American Petroleum Institute, *www.api.org.*
5. *Website for American Chemistry Council, www.americanchemistry.org.*
6. American Chemistry Council, Site Security Guidelines for the U.S. Chemical Industry, (October 2001).
7. Center for Chemical Process Safety, *American Institute of Chemical Engineers*, Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites, (August 2002).
8. **Ragan, P. T., Kilburn, M. E., Roberts, S. H., Kimmerle, N. A.**, Chemical Plant Safety - Applying the Tools of the Trade to a New Risk, *Chemical Engineering Progress*, pp. 62-68, (February 2002).
9. **Hairston, D.**, Editor, Terror-Proofing CPI Plants, Chemical Engineering Magazine, pp. 27-33, (January 2002).
10. **Vice Admiral Thomas Collins**, U. S. Coast Guard, speech at the conference "Meeting the Homeland Security Challenge: Maritime and Other Critical Dimensions," Institute for Foreign Policy Analysis and The Fletcher School of Law and Diplomacy, Tufts University, (March 25-26, 2002).
11. Report of Maritime Security Working Group, Maritime Safety Committee of IMO, MSC 75/WP.18, (May 23, 2002).
12. *Maritime Transportation Antiterrorism Act of 2002*, H.R. 3983, as approved by the U.S. House of Representatives on June 4, 2002.
13. *Port and Maritime Security Act of 2001*, S. 1214, as passed by the Senate.