U.S. Department of Transportation

Research and Special Programs Administration

Office of the Secretary of Transportation

CONFERENCE REPORT

Conference on U.S. Marine Transportation Systems Vulnerability
May 28-29, 1997
Leesburg, Virginia

Prepared by:

Volpe National Transportation Systems Center
Research and Special Programs Administration
U.S. Department of Transportation

U.S. Department of
Transportation

Office of the Secretary
of Transportation

June 13, 1997

Dear Colleague:

The attached report presents the results of the U.S. Department of Transportation (DOT) meeting to discuss marine transportation security held at the Xerox Conference Center in Leesburg, Virginia on May 28-29, 1997. Included are:

- the conference agenda
- an executive summary of conference results
- detailed reports of the five breakout groups addressing key vulnerability areas
- copies of the slide presentations of conference speakers
- a comprehensive list of conference attendees.

Later this summer, you will also be receiving a copy of the final report of the maritime system vulnerability assessment currently underway under the direction of the Volpe Center.

On behalf of the several agencies of DOT which cosponsored the conference -- the Secretary of Transportation's Office of Intelligence and Security, the Maritime Administration, the U.S. Coast Guard, and the Research and Special Programs Administration -- I thank you for your continued interest and collaboration in working to preserve and enhance the security of our nation's marine transportation.

Sincerely,

Paul J. Pluta
Director
Office of Intelligence and Security

Conference on U.S. Marine Transportation Systems Vulnerability
May 28-29, 1997
Leesburg, Virginia

Contents

Conference on U.S. Marine Transportation Systems Vulnerability
May 28-29, 1997
Leesburg, Virginia

Agenda

Wednesday, May 28

1:00	Welcome	Ms. Patricia Hammar, RSPA
1:15	Opening Remarks	VADM A. J. Herberger, USN- Ret. Maritime Administration
1:30	Surface Transportation Vulnerability Assessment	Ms. Patricia Hammar, RSPA
1:45	Volpe Maritime Assessment Summary	Rod Cook, Volpe Bob Pray, Capt. USCG-Ret., Volpe
2:30	Break	
2:45	Breakout Session #1, Vulnerability Identification	

a. Passenger Vulnerabilities
b. Cargo Vulnerabilities
c. Infrastructure Vulnerabilities
d. Smuggling
e. Organized Crime

4:15	Day One Summary	Ms. Patricia Hammar, RSPA
4:45	Day One Closing Remarks	RADM Paul Pluta, USCG

Thursday, May 29

8:00	Day Two Welcome	Bob Pray, Capt. USCG-Ret., Volpe
8:15	Day Two Opening Remarks	Mr. Thomas Falvey, Commissioner, President's Commission on Critical Infrastructure Protection

8:45 Breakout Session #2, Vulnerability & Impact Identification

a. Passenger Vulnerabilities
b. Cargo Vulnerabilities
c. Infrastructure Vulnerabilities
d. Smuggling
e. Organized Crime

10:30 Break

11:00 Breakout Session #3, Countermeasure Identification

a. Passenger Vulnerabilities
b. Cargo Vulnerabilities
c. Infrastructure Vulnerabilities
d. Smuggling
e. Organized Crime

12:30 Lunch

1:30	Coast Guard Perspective on Maritime Security	Capt. Scott P. Cooper, USCG
2:15	Breakout Session Reports	Group Representatives
4:00	Break	
4:15	Workshop Summary	Ms. Patricia Hammar, RSPA
5:00	Adjourn	

Conference on U.S. Marine Transportation Systems Vulnerability
May 28-29, 1997
Leesburg, Virginia

Executive Summary

The Research and Special Projects Administration (RSPA) of the U.S. Department of Transportation (DOT), Office of the Secretary of Transportation (OST) recently hosted the 1997 Conference on U.S. Marine Transportation Systems Vulnerability. The conference was held at the XEROX Document University in Leesburg, Virginia on the 28th and 29th of May, 1997. Approximately 65 people from government and the marine transportation industry attended the conference. The conference format consisted of several brief presentations from other supporting government agencies and five breakout or workshop sessions on selected topics.

The guest speakers included:

- Mr. Thomas Falvey, President's Commission on Critical Infrastructure Protection (PCCIP)
- VADM A. J. Herberger, USN-Ret., MARAD
- RADM Paul Pluta, USCG, OST
- Captain Scott Cooper, USCG
- Ms. Patricia Hammar, RSPA
- Mr. Rodney Cook, Volpe Center
- Capt. Bob Pray, USCG-Ret., Volpe Center

The remarks and/or slides presented by the individual speakers are included in this document with their permission. We regret that Mr. Falvey's presentation was not available for inclusion in the report.

The topics of the five breakout sessions were:

- Passenger Vulnerabilities
- Cargo Vulnerabilities
- Infrastructure Vulnerabilities
- Smuggling
- Organized Crime

Each session was provided with a professional facilitator to help the group stay focused and on track. The groups were asked to discuss the particular topic of their session, identify vulnerabilities in the system, and suggest countermeasures. At the conclusion of the conference, a spokesperson for each session presented the group's "findings." The facilitators prepared breakout session reports which are presented in this document.

SUMMARY OF BREAKOUT SESSIONS

The following is a brief discussion of the results of the five breakout sessions. Though each session was on a different topic, there were several recurring themes that reached across all five topics.

Threats

Cargo Theft
This issue was brought up by every group except for the Passenger Vulnerabilities group. The other four groups believed that it is currently the most significant problem facing the U.S. marine transportation system. The exact value of cargo stolen every year is not known but is estimated to be in the vicinity of $10 billion. Shipping companies may be reluctant to report all thefts for a variety of reasons centered around competition with other shippers and other ports.

Illegal Use of the Marine Transportation System
The system is being used by criminals to transport drugs, illegal aliens, currency, stolen property, and counterfeit goods. Legitimate shippers and shipping companies are fined and suffer a loss of reputation when they are caught being used in this manner, by law enforcement agencies.

Extortion for Monetary Gain
Cruise ships, gambling cruise boats, and passenger ferries frequently receive bomb threats. Though some appear to have no basis, many are attempts to extort money from the ships' owners.

Vulnerabilities

Insiders are seen as the biggest vulnerability of the marine transportation system. Without the cooperation of people working in the system, cargo theft, smuggling, and extortion would not be nearly as significant a problem.

A lack of definitive data hampers the proper assessment of the magnitude and methods of the theft, smuggling, and extortion problems. This leaves many legitimate shippers without the information they need to take remedial action.

Failure to share intelligence data prevents industry and government alike from being fully informed on the level and seriousness of the threats arrayed against them.

The lack of a foolproof cargo tracking system makes it much easier for cargo, especially containers, to be vandalized, stolen, or penetrated by smugglers.

Points of Origin outside of the U.S. are seen as being particularly vulnerable to criminal activity, especially in some Caribbean, Latin American, and South American nations.

False Documents allow criminal elements to ship illegal cargoes as legitimate cargo.

Countermeasures

Employee Background Checks
Conduct background checks on all personnel working inside the marine transportation system that have the opportunity to aid and abet illegal activity.

Data Collection
Develop a data base on illegal activity that defines the seriousness of the problem and the methods employed by criminals. Make the database accessible to companies working within the system as well as government and law enforcement agencies.

Positive Cargo Checks
Develop a non-intrusive method for verifying the contents of containers.

Cargo Tracking System
Develop a foolproof system for tracking containers that can pinpoint missing/stolen containers.

Share Intelligence
Develop a system that allows government, law enforcement, and industry to share intelligence data.

Caller I.D./Employee Training
Train passenger-ship employees on how to handle extortion phone calls and equip incoming phone lines with caller I.D. in an attempt to identify persons calling in with bomb/extortion threats.

Increased Inter-Government Cooperation
Attempt to improve cooperation with foreign port of origin nations in an attempt to improve security at the point of origin.

Future Plans

RSPA has tasked the Volpe Center with developing a final report on the conference and moving ahead with some of the recommended countermeasures. Under the current Transportation Vulnerability Assessment Program, Volpe proposes to:

1. Continue attempts to collect data on the extent and methods of criminal and terrorist/saboteur activity.
2. Develop a shared intelligence network that can be accessed by all interested parties.

Volpe will also propose that funds be allocated to further investigate the following:

3. Develop a non-intrusive method of positive cargo identification.
4. Develop a foolproof cargo tracking system for containers.
5. Develop a database for background checks on people working within the system.

Conference on U.S. Marine Transportation Systems Vulnerability
May 28-29, 1997
Leesburg, Virginia

Breakout Group Reports

Each of the breakout groups discussed threats for its subject area, identified resultant vulnerabilities and their impacts, and developed a set of recommended countermeasures to address the identified vulnerabilities. The resulting reports each have a slightly different structure reflecting the actual dialogue which took place.

- Passenger Vulnerabilities
  Prepared by: Ann Kelly, Session Facilitator

- Cargo Vulnerabilities
  Prepared by: Laird Smith, Session Facilitator

- Infrastructure Vulnerabilities
  Prepared by: Gary Hobday, Session Facilitator

- Smuggling
  Prepared by: Bob Pray, Session Subject Matter Expert

- Organized Crime
  Prepared by: Steve Losier, Session Facilitator

Conference on U.S. Marine Transportation Systems Vulnerability
May 28-29, 1997
Leesburg, Virginia

Summary of Results - Passenger Breakout Sessions

Participants

Patrick J. Andrich
Manager of Los Angeles Cruise Ship Terminals
Metropolitan Stevedore Company

Charles N. Dragonette
Senior Analyst, Civil Maritime Analysis Department
U.S. Navy

Dwight Fender
Director of Operations
Canaveral Port Authority

Donald J. Kerlin
Chief, Passenger Vessel Security Division
National Maritime Center, United States Coast Guard

Patrick J. Lennon
Director of Technical Security
Vance International Investigative Services, Inc.

Karen Martini
Regional Sales Manager
Control Screening LLC

Dorothy M. Schulz, Ph.D.
Associate Professor
John Jay College of Criminal Justice

Herman S. Wilkins
Lieutenant
Maryland Port Administration Police Department

Facilitator:
Ann Kelly
Management Consultant
Unisys Corporation

Subject Matter Expert:
CDR Jeffrey Gabrielson
United States Coast Guard

General Discussion

This group examined vulnerabilities of passengers of cruise ships, passenger ferries, and riverboat gambling vessels. The group consisted of a diverse mix of law enforcement, security operations, equipment manufacturers, military, and educational representatives. Conspicuously absent, however, were actual operators of cruise lines, passenger ferries, or riverboat gambling vessels. The outputs presented reflect the relatively optimistic views of the participants present. If operators had been present, the views expressed may have been different.

The group began with a short identification of items posing threats to passengers and proceeded quickly to a dialogue about vulnerabilities to passengers of the identified vessels. For each identified vulnerability, the group established a criticality ranking of high to low reflecting the relative probability and impact of its occurrence. Finally, the group developed a list of recommended countermeasures to address the identified vulnerabilities.

Threats

The major cause of threat to passengers of cruise ships, ferries, and gambling vessels is that of extortion for monetary gain. Terrorism and bomb threats for political purposes are also problems. Generally, threats to passengers are considered greater outside the United States than within U.S. borders.

Vulnerabilities

The following was identified as a vulnerability of **High** criticality:

Marine rapid transit services. The unregulated access of ferry services makes them highly vulnerable to all forms of threat. A bombing incident could totally disable local passenger service in areas where alternate travel modes are not available. Ripple effects could be felt throughout a region from the destruction of one node in cases where no facility redundancy exists.

The following were identified as vulnerabilities of **Medium to High** criticality:

Ramifications of criminal activities gone bad. In the event of a terrorist attack which devolves into the taking of hostages on board, ships are vulnerable because they do not typically possess hostage-negotiation and related skills which would be required to handle the incident.

Cruise themes. Cruises which offer theme packages designed to target segments of the cruising population may also inadvertently attract the attention of terrorists who view the theme as opposite to their political views. For example, a cruise on the QE2 to celebrate the 50th anniversary of the founding of Israel may not be such a good idea.

The following were identified as vulnerabilities of **Medium** criticality:

Large amounts of cash on board. Traditionally, crews of passenger vessels are paid in cash, necessitating the carrying of significant amounts on cash on board at predefined intervals. Additionally, casino activities on cruise ships and riverboat gambling vessels require large amounts of cash to be carried. Both factors make ships tempting targets for potential extortionists.

Industry and passenger focus on "fun". Cruises are packaged and advertised as recreational activities. Extensive mention or application of security measures might lessen their appeal to customers. The group felt that this vulnerabilty may be receding in criticality as travelers become accustomed to the levels of airline security which typically exceed those applied to cruise ships.

The following were identified as vulnerabilities but were considered to be of **Low** criticality:

Media exposure. Widely distributed films, books, newscasts, etc. showcasing high-violence activities onboard cruise ships may suggest ideas and opportunities to potential criminals.

Turnaround-time consciousness. Ships face considerable pressure to minimize time spent in port rather than at sea. This may lessen the ability of operators to provide thorough security before departure. Conversely, however, lengthening in-port time could present additional time and opportunity for crimes to occur.

Different sources and levels of security. Over the course of a cruise, various security providers - public, private, and vessel sources - have security responsibility. Potential terrorists may target the weak links in the chain.

Known vessel schedules and itineraries. Cruise ship schedules and itineraries are published well in advance, making the vessel an easily targetable object for potential terrorists.

Seaside access. Current vessel security plans focus almost exclusively on preventing landside security intrusions. Other than providing perimeter lights on ships, little is done to prevent potential terrorist access from the water.

Passenger baggage. Current baggage screening techniques are inconsistently applied and often do not include checked as well as hand-carried luggage.

Passage of security responsibility enroute. As cruise ships move out to sea and back to port, they traverse zones which fall under the jurisdiction of differing security providers. This presents a potential for possible confusion as to who is responsible should an incident occur as well as the possibility of inconsistently applied security measures.

Countermeasures

The following were recommended as countermeasures to combat the perceived vulnerabilities identified above. In the list below, the countermeasure is shown beneath the vulnerability to which it is linked.

Vulnerability: Marine rapid transit services.

- Convene a meeting of state departments of transportation who operate marine transportation systems to share information on ferry operation.

Vulnerability: Ramifications of criminal activities gone bad.

- Improve the preparation and coordination for vessels and facilities to deal with incidents in progress through both planning and training.

- Establish a standing working group within the Maritime Security Council to receive, collate, analyze, and publish lessons learned on security incidents.

Vulnerability: Large amounts of cash on board.

- Review procedures for cash transport and storage. Move increasingly to non cash-based transactions.

Vulnerability: Industry and passenger focus on "fun".

- Cast security measures in terms of passenger safety (a positive) vs. pure security (a potential negative).

Vulnerability: Seaside access.

- Include underwater and seaward security in vessel security planning.

Vulnerability: Passenger baggage.

- Increase screening of all passenger baggage.

Summary

From review of the vulnerabilities identified, the group concluded that passengers are primarily vulnerable when they are on the vessel, rather than in port facilities. Additionally, the group felt that most of the identified vulnerabilities were highly localized and not systemic in nature and therefore were judged to be of low criticality. Participants acknowledged that there are probably many threats made against cruise lines that we never hear about and felt it would have been beneficial to have had the representation of vessel operators in the discussion.

Conference on U.S. Marine Transportation Systems Vulnerability
May 28-29, 1997
Leesburg, Virginia

Summary of Results - Cargo Breakout Sessions

Participants

Edward V. Badolato
Contingency Management Services

Captain B. A. Bowditch, Jr.
Manager, Compliance Department
Lykes Bros. Steamship Co., Inc.

Nancy A. Cooney
Intermodal and Logistics Systems Division
Volpe National Transportation Systems Center

Paul F. Duffy
Security Manager
Birdsall, Inc. - Agent for Tropical Shipping

Michael J. Jukoski
National Institute of Justice
Office of Science and Technology

RADM Paul J. Pluta
Office of Intelligence and Security
U.S. Department of Transportation

Dorothy M. Schulz, Ph.D.
Associate Professor
John Jay College of Criminal Justice

John Short
Director of Studies and Analysis
Analytic Systems Engineering Corp.

Barry Tarnef
Marine Loss Control Consultant
Chubb & Son

John Tichenor
Marine Surveyor
Cigna Insurance

Tony Velazquez
Federal Bureau of Investigation

Facilitator:
Laird K. Smith
Unisys Corporation

Subject Matter Expert:
Thomas Morelli
Coordinator for Maritime Intelligence & Security
Maritime Administration

General Discussion

The group was guided through a discussion of threat and vulnerability elements, and used subgroups to develop countermeasures for the most important vulnerabilities.

For the purposes of the discussion, a vulnerability was defined as a weak or missing control or process which could be exploited by a threat source. The group focused primarily on criminal activity threats. The breakout group felt strongly that cargo security considerations must be discussed in a system context (Threats to cargo must be mitigated over the entire process, from the shipper, through intermodal links to the port, during transit, through the arrival port, and during intermodal delivery to the recipient). Many crimes happen outside the port.

The group hoped that results of the discussion would:

- Aid coordination among participating organizations
- Provide near term assistance to law enforcement (e.g., Port of Miami) by addressing the intelligence problem. More information is needed on where criminals are getting information on cargo targets and the methods used to penetrate controls.
- Provide rationales to help organizations allocate resources and secure funding
- Lead to follow-up activities associated with this conference

- Generate ideas for technology transfer, leveraging existing R&D programs, e.g.,
  - Tracking cargo
  - Container locks and seals
  - Non-intrusive detection
  - Physical security integration
- Contribute to requirements for new technology

Vulnerability Elements

The group briefly summarized the most important assets targeted by criminals or terrorists and the controls which are frequently penetrated.

Assets:

- Containers (portability is a weakness as well as a transportation system strength)
- Advanced technology cargo (e.g. "dual use" technology desired by other governments)
- High-value cargo which can be easily disposed of and that is difficult to track, e.g.,
  - Cash
  - Clothing
  - Food
  - Liquor
  - Computer chips
  - Perfume
- Petrochemical shipments (possible terrorist target with environmental impact)
- Packaged hazardous materials (possible terrorist target)
- Arms shipments

Control Weaknesses:

- Container seal integrity
- Lack of cellular telephones for law enforcement
- Security procedures at all levels
- Current level of understanding about how theft is occurring
- Physical security controls (e.g., gate personnel/procedures)
- An attitude that some losses are just "a cost of doing business"
- Existing terminal configurations which limit security options

Issues

The group also discussed issues which should be addressed when designing solutions for intermodal marine transportation security problems.

- Fragmentation of operations results in a number of issues:
  - Security responsibilities by the modes involved in a shipment are unclear
  - Law enforcement jurisdictions can be unclear, depending when and where a crime occurs
  - Responsibility for insurance coverage can be unclear
  - The number of reported crimes may be too low if only official port figures are used
  - It is difficult to determine where the loss has occurred
  - The definition of a port is dynamic
  - Law enforcement personnel lack information about current industry security products and services.
- Losses (even those occurring outside a port) can damage a port's reputation.
- Commercial organizations are reluctant to release information on cargo thefts if that information is considered proprietary.
- Assessments, research, and countermeasures implementation efforts should be focused on the most important locations, e.g., Ports in Miami, Southern California, and New York/New Jersey.

Vulnerabilities

The group identified the following vulnerabilities as the most important to address with countermeasures (numbering does not indicate a ranking - the group believed that all should be addressed):

1. Ignorance and/or apathy toward proper security procedures/processes/equipment on the part of shippers, carriers, terminals, and law enforcement organizations.
2. Lack of knowledge about the specifics of cargo theft (how, why, where) even when data exists.
3. Physical security of containers (e.g., gates, seals), especially when intermodal shipments are involved.
4. Unauthorized access to cargo and shipment information.
5. Collusion with criminals by people working in the transportation system (internal conspiracy).
6. Fragmented operations which make it difficult to coordinate planning, intelligence and prevention.
7. Limited and/or ineffective funding for marine transportation security activities by government and industry.

Countermeasures

1. Ignorance and/or apathy toward proper security procedures/processes/equipment on the part of shippers, carriers, terminals, and law enforcement organizations.

   a) Educate law enforcement, shippers and industry representatives
   b) Recommend national standards for cargo security
   - *Some level of employee background screening*
   - *Interchange controls*
   - *Photo ID of drivers, stevedores, etc.*
   - *Cargo documentation*
   - *Container equipment detection, responses, and post-operations activities*
   - *Seal control and integrity*

Needs	Existing Resources	Benefits
• A mechanism to coordinate available intelligence and update it regularly based on new information (e.g., cargo theft analysis, product offerings).	Some information is available in DOT publications and by the NCSC, insurers, steamship lines, etc.	• Puts state-of-the-art cargo security ideas into the hands of those who need it.

2. Lack of knowledge about the specifics of cargo theft (how, why, where) even when data exists.

   a) Establish a central clearinghouse for reporting, collating, analyzing, and disseminating cargo theft data and threat information
   b) Establish a standard for the timely reporting of cargo theft on an intermodal basis
   c) Make reporting mandatory (allowing some flexibility in formatting may be advisable)
   d) Establish a method to disseminate needed information

Needs	Existing Resources	Benefits
• A commitment from Industry to support the initiative • Funding for design, development, and maintenance of the system • Selection of an "honest broker" to safeguard the database	Data currently exists from law enforcement agencies, AIMU, and others. Cargo theft reports are being done by NCSC, shippers, state police, NFC/NSC and others. Computer capacity should be available within government or industry.	• Develops a credible cargo theft database to help awareness • Provides data to help funding efforts • Increases the interest in cargo security R&D

• An incentive for industry R&D to address the problem		

3. Physical security of containers (e.g., gates, seals), especially when intermodal shipments are involved.

   a) Establish a method to collect and disseminate security product and services information for securing containers.
   b) Establish seal integrity procedures.
   c) Establish a security working group with representatives from container manufacturers, lessors, steamship lines, insurers, and marine surveyors.

Needs	Existing Resources	Benefits
• A mechanism to gather, store, and disseminate product and service data • Funding for the initiative and assignment of responsibilities	Product literature is available from vendors. The Los Alamos National Laboratory has a Vulnerability Assessment Team which can assess container seal vulnerabilities for organizations.	Facilitates educated, cost-effective decision-making on container security controls.

4. Unauthorized access to cargo and shipment information.

   a) Establish a recommended security platform for computerized cargo data.
   b) Recommend methods and procedures to control/restrict access to cargo data.

Needs	Existing Resources	Benefits
• Establish a working group encompassing interested parties (shippers, transport carriers, software vendors, etc.)	Transportation industry EDI, Information Technology groups exist today. Industry and government organizations have developed Internet security procedures.	• Greater security and integrity of critical cargo and shipment data • Documentation which will reinforce physical security measures

5. Collusion with criminals by people working in the transportation system (internal conspiracy).

   a) *Require some level of background screening on employees, union members, etc. (see Countermeasures for 1.0).*
   b) *Monitor data transfer activity.*

Needs	Existing Resources	Benefits
• Establish standard industry practices for background checks • Coordinate background checking with Unions • Develop a data transfer monitoring checklist	New York currently does some background checking. Monitoring practices are informal.	• Decreases the risk of internal conspiracy

6. Fragmented operations which make it difficult to coordinate planning, intelligence, prevention, detection, responses, and post-operations activities.

   a) *Initiate multi-jurisdictional task forces to address critical coordination problems.*
   b) *Establish a database of shared information on cargo theft (see countermeasure recommendation for Vulnerability 2.0).*

Needs	Existing Resources	Benefits
• Establish a national shared database managed by an independent, highly trusted organization • Start with a pilot database prototype • Facilitate interjurisdictional data sharing • Encourage mandatory reporting of cargo theft	There is some recognition of the need for inter-jurisdictional task forces. Limited regional databases exist. A similar database exists for trucking. Many existing coordination efforts deal only with drug problems. Most efforts are focused on after the fact actions, rather than prevention.	• Faster dissemination of information which could lead to more effective prevention and detection • More effective working relationships.

7. Limited and/or ineffective funding for marine transportation security activities by government and industry.

   a) *Increase education efforts on the value of good security and "best practices" examples of effective controls.*
   b) *Increase education efforts on sound risk management techniques for cargo.*
   c) *Periodically brief government and industry representatives on the status of current initiatives and best practices.*

Needs	Existing Resources	Benefits
• Government support for the initiative must be developed. • This effort must receive attention in the budgeting process. • Materials must be collected, developed, and disseminated. • Lobbying efforts should be continued.	No similar education program has been identified. Some initial efforts are taking place in "stovepipe" fashion. Some government lobbying activities have included security aspects. Existing funds are frequently being spent on reaction activities, rather than prevention.	• More information will facilitate the development of credible proposals and the justification of improvement investments. • An overall effort may be more effective than stovepipe projects.

Additional Discussion - Bomb Threats

At the end of the final breakout meeting the participants briefly discussed bomb threats, as requested during the first Thursday morning combined session.

Participants felt that, in the cargo area, the potential loss could be high but the probability of a loss occurrence was extremely low. Cargo ships are difficult targets and are not as glamorous as other terrorist objectives. Labor disputes could be one source of problems. If a ship were bombed at a key location in a port (e.g., the Houston ship channel), significant interruption of traffic could result. It was noted that containers could conceivably be used to deliver a bomb to another target for detonation after delivery. Good intelligence is one of the most important countermeasures (even criminal elements may provide early warning information if a terrorist action might shut down a port).

Conference on U.S. Marine Transportation Systems Vulnerability
May 28-29, 1997
Leesburg, Virginia

Summary of Results - Infrastructure Breakout Sessions

Participants

Thomas J. Falvey
Commissioner
President's Commission on Critical Infrastructure Protection

Steven A. Masterson
Security Consultant

Bradford Walton
Director, Business Development, Systems Engineering
Information Systems Group
BTG, Inc.

Joan B. Yim, AICP
Program Manager for Marine Services
Parsons, Brinckerhoff, Quade & Douglas, Inc.

Facilitator:
Gary Hobday
Volpe/EG&G Dynatrend

Subject Matter Expert:
LT Michael Edgerton
United States Coast Guard

General Discussion

The group agreed that criminal activity threats were an ongoing primary concern to Port Operators and to the infrastructure. Less time was spent on terrorist activities or acts of disgruntled employees.

The group hoped that results of the discussion would:

- Provide information about specific issues and vulnerabilities
- Address intermodal security at ports
- Identify non-traditional threats
- Clarify the implications of terrorist threats at ports
- Clarify requirements of information security technologies
- Address port security; especially for petroleum facilities, tank farms, and terminals
- Provide information about port security police technology
- Compare governmental needs vs. private industry capabilities

The Maritime Infrastructure was defined as: "Hardware, software, and labor necessary to conduct the business of shipping, including the transition to other modes of transportation."

Vulnerability Elements

Infrastructure Components:

- Ships
- Channels (and buoys)
- Piers
- Container cranes
- Telecommunications
- Locks and dams
- Rail access
- Information systems
- Electronic Data Interchange (EDI) / Electronic Commerce (EC)
- Paperwork
- Facilities
- Companies
- Labor
- Electric power
- Highways
- Bridges

Stress Points:

- Overall command and control for planning, "Who's in charge?"
- Aging infrastructure stressed by new business strategies ("Fast Ship", rail consolidation, etc.)
- Private industry security firms (skills, resources, investment)
- Information systems (access, integration)
- Telecommunications (disruption, exploitation)

Issues

The group discussed issues of vulnerability for several key infrastructure components.

Ships Issues:

Issue 1: National Security

The infrastructure issues for ships were primarily those of U.S. and non-U.S. flag ships. Are there enough U.S. flag ships to provide for our national security? With global ownership and free trade economics as robust business drivers, the title "U.S. Flag" is now blurred. Whose perspective will be maintained during times of conflict?

Issue 2: Poor Quality/Low Maintenance

Non-U.S. flag ships sometimes reveal poor quality and low maintenance issues that could compromise the safety and security of a U.S. port.

Channels Issues:

The group discussed a variety of threats to channels, including:

- Blockage
- Oil Spills
- Removal/reorienting of navigational aids
- Intentional ship blockades (fishermen examples)
- Mines (threats or actual)
- Disruption of GPS/VTS systems
- Removal of pilots

Telecommunications Issues:

The group agreed on a difference of purpose between criminal and terrorist motivation when threatening the telecommunications infrastructure. Criminal intent is toward exploitation (via knowledge of cargo locations, schedules, access points, etc.), while the terrorist is more likely to disrupt maritime activity with the same information.

Areas of vulnerability were discussed:

- Cellular phones
- Operations centers (radio communications)
- Phone switches (due to fire, flood, explosions, and backhoes)
- Microwave systems

Information Systems (EDI/EC) Issues: (Electronic Data Interchange/Electronic Commerce)

- Limited company sharing - difficult to know if problem broadly exists
- Scarce data on past attacks
- Employees with access
- Company awareness (of risk) is low

Rail Issues:

- Derailment (vandalism or terrorism)
- Tunnels and bridges (not stressed for loads, no data sharing among parties responsible for various components of the infrastructure: e.g. Will they need to support something like M1A1 Abrams tanks?)
- Company mergers (automation interfaces, lack of integration and control)

Countermeasures

Command and Control - Who's in charge?

The need here is to go beyond a collection of jurisdictional points of view (Coast Guard Captain of the Port, port operators, company officials, utility operators, security company operators and employees, etc.) to a strategic point of view. Only then would the overall system security be considered and improved.

This higher level of port contingency planning could be accomplished with influence by the D.O.T. and the U.S. TRANSCOM. Port Readiness Committees (PRCs) charters could be broadened to include general port security and intermodal systems security. The group felt that the Coast Guard Captain of the Port could be used to initiate the security dialog among the various parties involved.

Information Systems and EDI/EC

The group recommends the D.O.T., either through its ITOP (contract) or Volpe Center vehicles, initiate a process to determine the significant information systems vulnerabilities and then recommend viable countermeasures. This could be accomplished through national conferences and cooperation with industry-based associations.

Non-U.S. Flag Ships

The group felt that construction and safety/operational standards should be augmented to minimize the hazards presented by non-U.S. flag ships to our maritime infrastructure. Also, incentives should be offered to promote construction of more U.S. flag ships.

Conference on U.S. Marine Transportation Systems Vulnerability
May 28-29, 1997
Leesburg, Virginia

Summary of Results - Smuggling Breakout Sessions

Participants

Edward J. Alford
Manager of Contraband Prevention and Safety
Crowley American Transport, Inc.

C. David Gelly, CPP
Manager of Security
Sara Lee Knit Products

Robert E. Perez
Senior Inspector
United States Customs Service

Paul Rodgers
Physical Security Specialist
U.S. Immigration & Naturalization Service

Facilitator:
David L. Damm-Luhr
Chief, Change Management Division
Volpe National Transportation Systems Center

Subject Matter Expert:
Robert L. Pray, Capt. USCG-Ret.
Volpe/EG&G Dynatrend

General Discussion

The group was well rounded and diverse though small in numbers. There was a representative from an overseas manufacturer and exporter, a shipping line and representatives from Coast Guard, INS and Customs. This gave the group a look at the issue of smuggling in the Marine Transportation system from several different viewpoints. Each participant got a new perspective on the issue of smuggling. The industry representatives described the procedures they follow to cut down on smuggling and avoid being fined by the government, or worse; having assets seized. The government representatives discussed their methods of detection and enforcement. Both groups made suggestions to the other on improvements that could reduce smuggling. The group identified four main smuggling threat areas. They are:

- **Drugs**
- **Stowaways** (Illegal aliens)
- **Counterfeits** (Brand name and copyright infringements)
- **Reverse Smuggling** (Sending illegal currency, stolen cars and etc. out of the US)

Vulnerability Elements

The group briefly summarized the most important vulnerabilities targeted by criminals in their attempts to conduct smuggling activities in the four main threat areas listed above.

- **Insiders**

The group believes that people working within the system, or insiders, are a key vulnerability to smuggling in the marine transportation system. With the help of knowledgeable insiders, smuggling can be very easy. Insiders can give criminals access to storage areas and containers. They can track shipments and identify what cargo is in what container. They can also falsify bills of lading and other important documents. They may be working for personal profit, or they may be part of a larger organized crime syndicate.

- **Points of Origin**

Most inbound smuggling begins at the cargo's point of origin. Criminal elements gain access to containers, bulk cargo or even the ships through illegal means and insert the cargo to be smuggled. Occasionally the shipper himself is the criminal. He/she may be shipping illegal cargo such as drugs or illegal aliens billed as something else that is legal to export/import. Conscientious manufacturers, shipping agents and shipping companies, must go to great lengths to reduce the likelihood of their cargo, or ship, being used as a medium for smuggling.

- **Containers**

Most smuggling is done surreptitiously by inserting the illegal cargo into a container. Once inside the container, the illegal cargo is normally safe until it is opened at the receiving end. Containers are rarely opened for inspection. There is currently no means for detecting contents via a high tech or low tech (dogs) piece of equipment without opening the container. Even the containers themselves are being used as hiding places for contraband through the use of false bulkheads, floors, or ceilings. Containers are frequently used in reverse smuggling operations.

- **Cargo**

Bulk cargo is not as vulnerable as a container but is still frequently used as a medium for smuggling. Fruit and vegetable shipments from South American and Caribbean ports are often targeted, and contraband is hidden in the bulk loads. Clothing manufacturers ship bulk finished goods from many ports in the Caribbean and South America. Smugglers also try to penetrate these cargoes. Other targeted cargoes include gravel, asphalt, bauxite, cement, and animal hides.

- **Fraudulent Documentation**

Phony shipping companies can dummy up documents to show that contraband is a valid cargo. This is a particularly vulnerable area for reverse smuggling. Documents are also falsified to show that containers were not opened illegally, when in fact they were. Legitimate companies may also falsify documents in an attempt to beat tariffs or other taxes.

Impacts

The group believes that threats and vulnerabilities are closely linked in the smuggling business and are normally part of the same system within a category (i.e., drugs, aliens, etc.) and also among and between categories. The impacts of smuggling are universal across the various categories of smuggling. They are thought to be:

- Costs - Lost revenues both direct (loss to the shippers) and indirect (loss to the government).
- Reputation - Shippers, manufacturers, and ports suffer when it becomes known that they have been involved in smuggling even if they were they victims and not the perpetrators. Their reputations are tarnished, and as a result they may lose business.
- Feeding the cycle of crime - Successful smuggling operations lead to more revenues for the criminal elements, and that allows them to continue and/or expand their operations.
- Health and Safety - People working legitimately can be unnecessarily exposed to dangers and health problems. They may be intimidated, abused, or threatened by organized crime elements. Illegal cargoes and illegal aliens may be carrying

communicable diseases. Containers or cargo that has been tampered with may break loose at sea or during load/off-load operations.

- Delays in delivery.
- Increased costs to manufacturer and shipper either through front-end protection or fines at receiving end.

Countermeasures

The group believes that most countermeasures will have universal application against smuggling among the various categories. The group developed four general categories as first steps to implement anti-smuggling countermeasures with several subcategories to each one. They are:

- **Identify the links, responsibilities, and leads in the chain or system.**
  1. Identify where responsibilities begin and end or overlap in the marine transportation system.

- **Identify the potential or criteria for expanding partnerships.**
  1. Identify partnership potentials, and develop a business case for pursuing the partnership.
  2. Work with unions to better regulate the cargo handling work force, in port and at sea. Include suitability checks, licensing, and/or bonding.
  3. Involve unions, port operators, and shippers in partnerships with government agencies.

- **Identify the costs and benefits of joint ventures and investments in anti-smuggling operations.**
  1. Identify ways to leverage the different players' investments in security or anti-smuggling operations.
  2. Evaluate a system of incentives for companies that participate in international anti-smuggling operations.
  3. Identify locations where reverse smuggling is most prevalent. Take steps to target specific individuals and weak points in the chain.
  4. Evaluate cost/benefits in further investments in assistance to foreign industries and governments, especially in cooperation with the private sector.

- **Identify methods to facilitate information exchanges.**
  1. Collect information that is of maximum use to all who are responsible for links in the chain.
  2. Develop a classification scheme that will allow for expanded information sharing.
  3. Fine tune information networks to identify targets as specifically as possible.

4. Identify "best practices" in consortia approaches to multi-jurisdictional situations.
5. Improve intelligence and speed of appropriate responses.

Issues and Impediments to Implementation of Countermeasures

The group also identified five possible impediments to implementation of countermeasures that will have to be overcome in developing any countermeasure scenario. They are:

- Infighting centered around information sharing.
- Perceptions of sharing information among the different links in the chain.
- Keeping abreast of the shifting nature of threats and vulnerabilities.
- Overlapping jurisdictional controls.
- Difficulty of doing front-end work or affecting any change at all in foreign ports.

Summary

The group theorized many good ways to break up smuggling but believed that there will be many impediments in the implementation phases because of multi-national jurisdictions. Many of the countries in the Caribbean and South America, where smuggling operations originate, do not have the resources or political will needed to take precautions against smuggling. Some companies will not wish to share information with other companies or government agencies, fearing that they or their information will be compromised. Positive foolproof controls on containers from the packing point to the unpacking point would eliminate many of the opportunities for smuggling. Smugglers are very clever and will shift modes of transportation at the first hint of trouble. Staying abreast of the latest smuggling techniques will be important. Whatever countermeasures are taken, they should be evaluated closely to ensure they will not adversely affect business. The cost vs. benefit of any proposed countermeasure should be examined closely before being put into operation.

Conference on U.S. Marine Transportation Systems Vulnerability
May 28-29, 1997
Leesburg, Virginia

Summary of Results - Organized Crime Breakout Sessions

Participants

Ronald Casey, Ed.D.
Senior Consultant
Educational Security Safety Consultants, Inc.

Robert DelCore
Manager, Police Training and Education
International Association of Chiefs of Police

Jeffrey B. Hirsch
Ports & Intermodal Representative
Maritime Administration

Anthony Infante
Police Operations Captain
The Port Authority of NY & NJ

Thomas Morelli
Coordinator for Maritime Intelligence & Security
Maritime Administration

Facilitator:
Steve Losier
Unisys/SRC

Subject Matter Expert:
Rodney L. Cook
Office of Systems Engineering
Volpe National Transportation Systems Center

General Discussion

Organized crime infiltrates all segments of the international shipping cycle in order to steal cargo and smuggle drugs, currency, weapons, automobiles, and other valuable goods. Organized crime works behind the scenes to identify weaknesses in the marine transportation system that can be exploited. Common targets are people who are susceptible to bribes and coercion, such as those with gambling debts or drug problems. Since people with these types of weaknesses may be employed anywhere within the shipping cycle, the marine transportation system is vulnerable to organized crime almost everywhere.

Theft of cargo occurs when organized crime targets and hijacks containers of goods that have arrived in a port. The theft can occur at the port itself or after a container is trucked away from the port facility. Organized crime uses traditional intelligence gathering methods through its well established networks to identify its cargo targets. They also employ cyber hackers to gain access to valuable shipping data and forge documents that can be used to get unsuspecting individuals to release cargo containers to their custody.

Smugglers illegally use the marine transportation system to transport goods in and out of the country. Typically drugs and aliens are smuggled into the U.S. while arms, currency, and stolen goods, such as automobiles, are smuggled out of the country. With smuggling, much of the crime activity occurs outside the borders of the U.S.

Impacts of Organized Crime Activities

Cargo theft and smuggling seriously impact the nation's transportation infrastructure and national security. The primary impact of cargo theft is the higher cost of goods, which is passed on to the consuming public. Each link in the shipping chain, which includes the manufacturer, the shipper, the port authority, and the workers at the port, is weakened in its ability to compete both in the domestic and foreign markets. The potential implications are manufacturers and shippers going out of business, ports losing traffic to competing ports, and workers losing their jobs.

The impacts of smuggling are enormous and can be felt at all levels of society. Illegal drugs sap the productivity of citizens, encourage criminal activity, and require huge outlays of federal, state, and local money to police. Illegal aliens are a drain on the nation's social services. Arms and currency smuggled out of the country enable conspiracies and actions against the U.S. and its allies.

Countermeasures

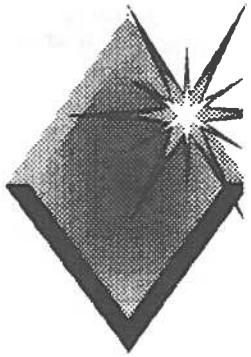
1. Declare War on Organized Crime – The nature and breadth of organized crime activities are not well known or understood by the general public. If high-ranking government official, such as the president, vice president, attorney general, or other cabinet officials were to present the case against cargo theft and smuggling activities to the public, the people may ask their representatives to apply more resources to solving the problem.
2. Assess Organized Crime Activity on a Port-by-Port Basis – Organized crime is market driven, and what is in demand at one port is likely different from what is in demand at others. Also, the traits and methods of crime organizations vary from one area to another based on a number of factors. Thus, profiles and solutions must be customized for each locale.
3. Establish a Multi-Jurisdictional Task Force – Longer-term undercover investigations are a proven method of fighting organized crime activities. Successful task forces require close coordination of jurisdictional elements with enhanced sharing of information.
4. Increase the Reporting of Criminal Activity – A major reason that theft and smuggling activities continue to flourish is that many of the crimes are never reported to law enforcement agencies. Shippers are reluctant to report crimes because they create a negative impression and may scare away customers. Also, shippers are compensated for their losses from insurance companies, so they see no incentive in calling attention to the problem. The insurers pay shippers for their losses without police reports because, despite frequent theft, insuring shippers is a lucrative business. In order to break the escalating cycle of shipping losses, the crime reporting rate must be improved. This can either be done voluntarily through and industry/law enforcement partnership or mandated via legislative action.
5. Capture and Disseminate Crime Data – In conjunction with the previous countermeasure, law enforcement agencies are very effective when their targets are identified. A national data base needs to be built to store theft and smuggling data which can be used analyze patterns of criminal activity. In addition to acquiring data from new sources, better use can be made of existing, "stove-pipe" data sources.
6. Seize Property of Crime Facilitators – People who "look the other way" when criminals use the maritime transportation system for illegal activities need to be shown that there is a penalty for abetting smuggling and theft. One solution may be to attach their assets.
7. Provide Security Training – An assessment needs to be performed to determine the security awareness training requirements for all marine transportation-related positions. Training should be provided that enables workers to better observe, detect, and identify situations where security breaches have occurred.
8. Foster a Federal and Industry Relationship – Government should work with industry groups to identify and disseminate "best business practices" that can be implemented more widely to reduce criminal activity.

Conference on U.S. Marine Transportation Systems Vulnerability
May 28-29, 1997
Leesburg, Virginia

Conference Presentations

- Volpe's Ports and Waterways Vulnerability Assessment
  Presented by: Bob Pray, Volpe Center

- Transportation System Vulnerability Assessment
  Presented by: Patricia Hammar, Research and Special Programs Administration



U.S. Department of Transportation

Research and Special Projects Administration (RSPA)

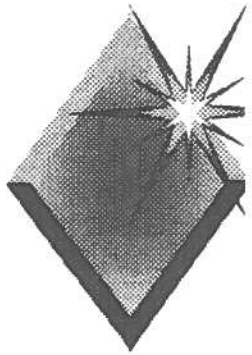
Conference on U.S. Marine Transportation Systems Vulnerability

Leesburg, VA 28-29 May, 1997

TOPIC:

Volpe's Ports & Waterways Vulnerability Assessment

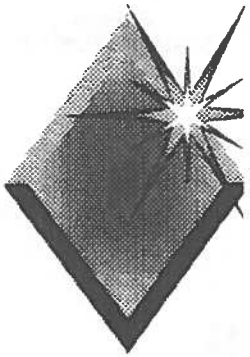
Volpe Team, DTS-72
May 1997



U.S. Ports & Waterways Vulnerability Assessment

Purpose:

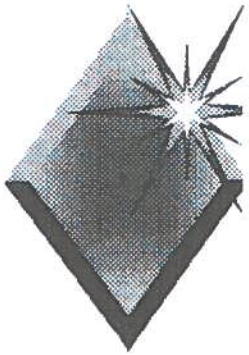
Propose a methodology for assessing possible threats to, and vulnerabilities of, the United States (U. S.) Marine Transportation System and recommending countermeasures to those threats



U.S. Ports & Waterways Vulnerability Assessment

Threats to the system can come from three separate areas:

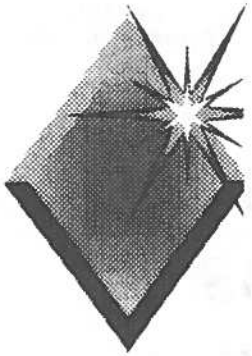
- Intentional Human Threats
- Accidents
- Acts of Nature



U.S. Ports & Waterways Vulnerability Assessment

Scope:

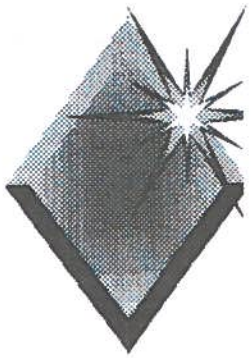
The Volpe assessment will consider all three areas, but will only recommend countermeasures for intentional human threats. Countermeasures for accidents and acts of nature are outside the scope of this assessment.



U.S. Ports & Waterways Vulnerability Assessment

The Assessment

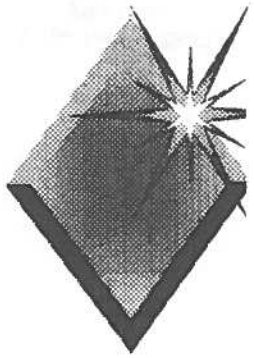
This Volpe assessment will be conducted by closely examining two robust port systems that appear to be representative of the U.S. Marine Transportation System.



U.S. Ports & Waterways Vulnerability Assessment

Criteria for Selecting the Ports

- One, an Ocean International Port
- One, an Inland Domestic Port
- In the Top 50 for busiest US Ports, by cargo weight
- Cargo and Passengers
- Significant Infrastructure
- Strategic Assets (for the ocean port)
- No known special issues



U.S. Ports & Waterways Vulnerability Assessment

Goals

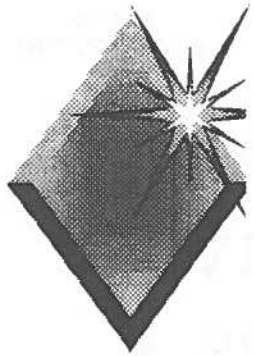
The assessment will attempt to identify new and potentially dangerous vulnerabilities of the U.S. Marine Transportation System that have not previously been identified by government or industry, and identify new countermeasures to protect the system.

U.S. Ports & Waterways Vulnerability Assessment

The Threat Matrix

Primary Threat Categories

- Criminal Activity
- Terrorism/Sabotage
- Civil Unrest

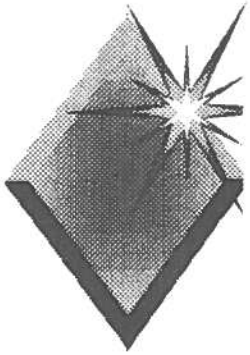


U.S. Ports & Waterways Vulnerability Assessment

THREATS

Criminal Activity

- Smuggling (Drugs, Aliens, Other)
- Theft (Hijacking, Piracy, Intelligence)
- Banking (money laundering, false letters of credit)
- Extortion

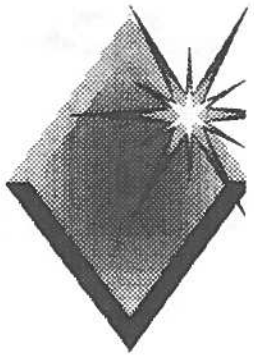


U.S. Ports & Waterways Vulnerability Assessment

THREATS

Terrorism/Sabotage

- Shooting
- Bombing
- Arson
- Operations Sabotage
- Biological/Chemical
- Mines
- Open/Guerrilla Warfare

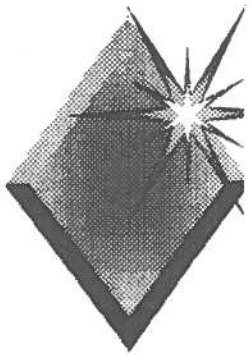


U.S. Ports & Waterways Vulnerability Assessment

THREATS

Terrorism/Sabotage (CONTD.)

- Cyber
- Environment
- Infrastructure
- Nuclear
- Communications

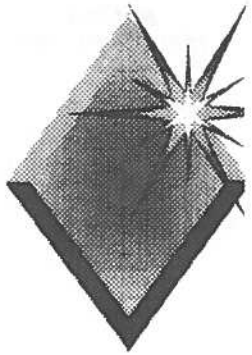


U.S. Ports & Waterways Vulnerability Assessment

THREATS

Civil Unrest

- Riot
- Protests
- Strike

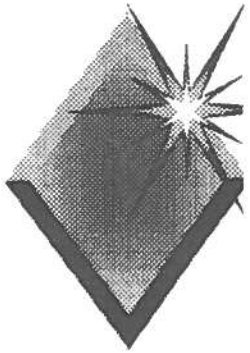


U.S. Ports & Waterways Vulnerability Assessment

The Threat Matrix

Primary Countermeasure Categories

- Planning
- Intelligence
- Prevention
- Detection
- Response
- Post Ops

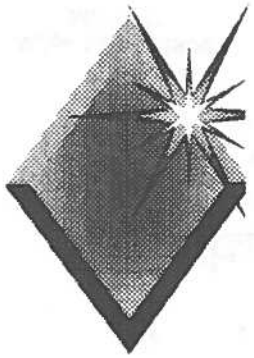


U.S. Ports & Waterways Vulnerability Assessment

COUNTERMEASURES

Planning

- Research and Development (R&D)
- Contingency Planning
- Training

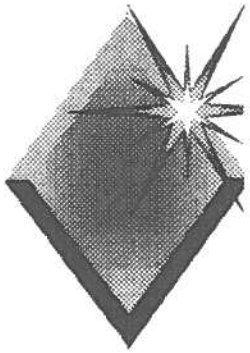


U.S. Ports & Waterways Vulnerability Assessment

COUNTERMEASURES

Intelligence

- Data
- Analysis
- Liaison
- Distribution

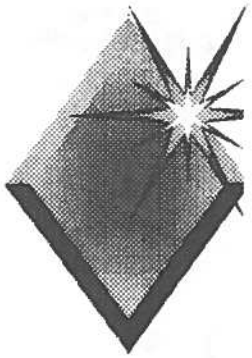


U.S. Ports & Waterways Vulnerability Assessment

COUNTERMEASURES

Prevention

- Clearance
- Intelligence Reaction
- Awareness
- Hardening
- Access/Perimeter Control
- Environment
- Communications

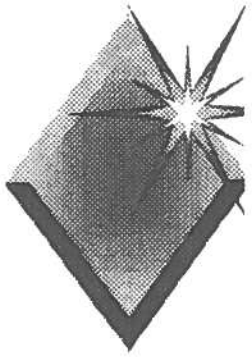


U.S. Ports & Waterways Vulnerability Assessment

COUNTERMEASURES

Detection

- Sensors
- Procedural Screens
- Evaluate Threats

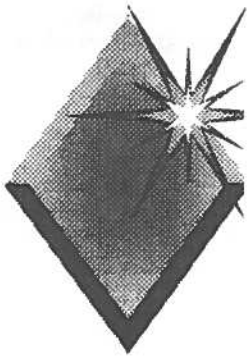


U.S. Ports & Waterways Vulnerability Assessment

COUNTERMEASURES

Response

- First Response
- Evacuation Plans
- Defusing Situations
- Coordination
- Crime Scene

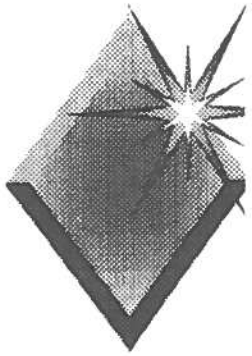


U.S. Ports & Waterways Vulnerability Assessment

COUNTERMEASURES

Post Ops

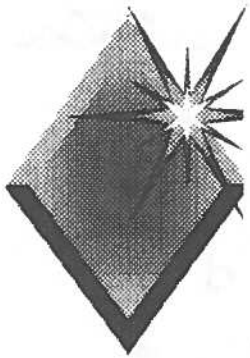
- Lessons Learned
- Evaluate Devices & Procedures
- Prosecution



U.S. Ports & Waterways Vulnerability Assessment

Progress to Date

- Background Research
- Data Collection
- Assessment Teams visit both ports
- Conference

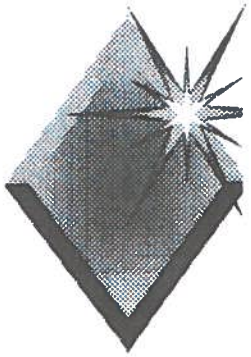


U.S. Ports & Waterways Vulnerability Assessment

ISSUES NOTED TO DATE

General

- Terrorists have largely ignored marine targets, hard to penetrate, not as attention grabbing as an airplane. As airplanes and airports become harder targets, will terrorists take another look at marine targets?
- Cargo theft, exceeded $2 Billion, worldwide last year.
- Smuggling of drugs, illegal aliens and other contraband

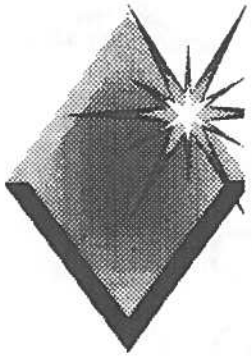


U.S. Ports & Waterways Vulnerability Assessment

ISSUES NOTED TO DATE

Ocean Port

- Cargo theft occurring primarily in the intermodal area.
- Gang/Mafia related activity
- Unions (Longshoremen, pilots)
- Competition
- Passenger Service Act
- Foreign Shipping Companies

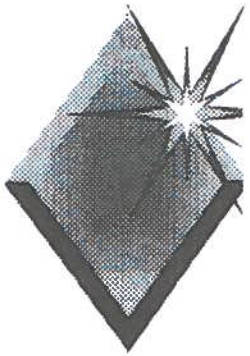


U.S. Ports & Waterways Vulnerability Assessment

ISSUES NOTED TO DATE

Ocean Port (CONTD.)

- Vulnerable Infrastructure
- Passenger Bomb Threats
- Nuclear Material
- Environmental Terrorism/Accidents
- Protests
- Strategic Assets

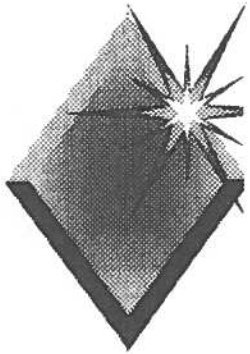


U.S. Ports & Waterways Vulnerability Assessment

ISSUES NOTED TO DATE

Inland Port

- Casino Gambling
- Bomb Threats
- Environmental Accidents
- Acts of Nature (flooding)
- Unions
- Cooperation & Contingency Planning
- Vulnerable Infrastructure



U.S. Ports & Waterways Vulnerability Assessment

Future Plans

- Conference results and recommendations
- Re-visit ocean port
- Publish results of conference
- Visit ports with special issues?
- Submit Assessment to DOT
- Follow on or follow up?

Transportation System Vulnerability Assessment

Assessment Goal

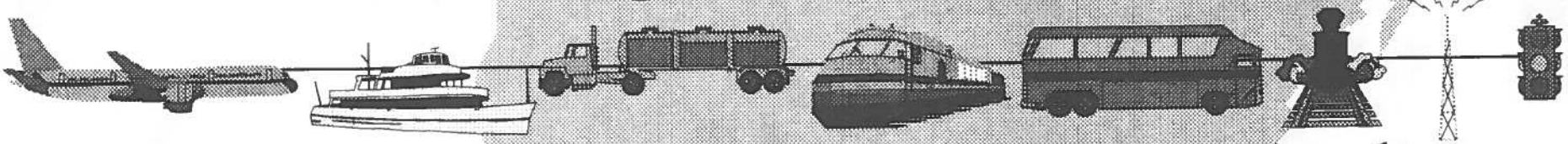
- To describe the current state of security in transportation
- To identify critical vulnerabilities that should be addressed by the department
- To evaluate how to address these vulnerabilities and to understand the costs of correcting these vulnerabilities

Transportation Security Objectives

Passenger v. Freight

Domestic v. Overseas

Looking across all modes



Looking at intermodal and cross modal technology

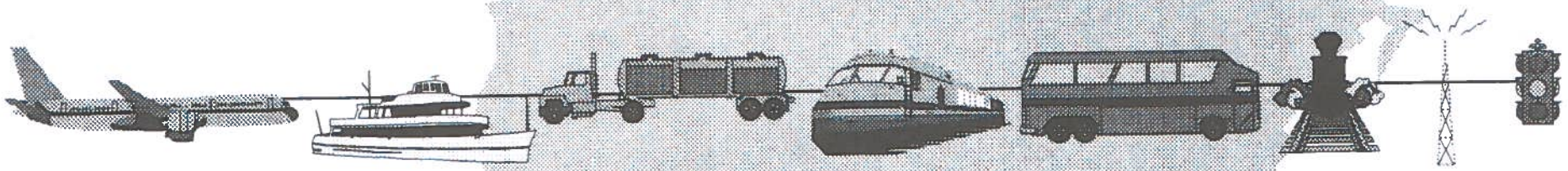
Private v. Government

Civil v. Military

Transportation Security Approach

Assessment

- Physical
- Information
- Interfaces
- Intermodal/Crossmodal/Modal



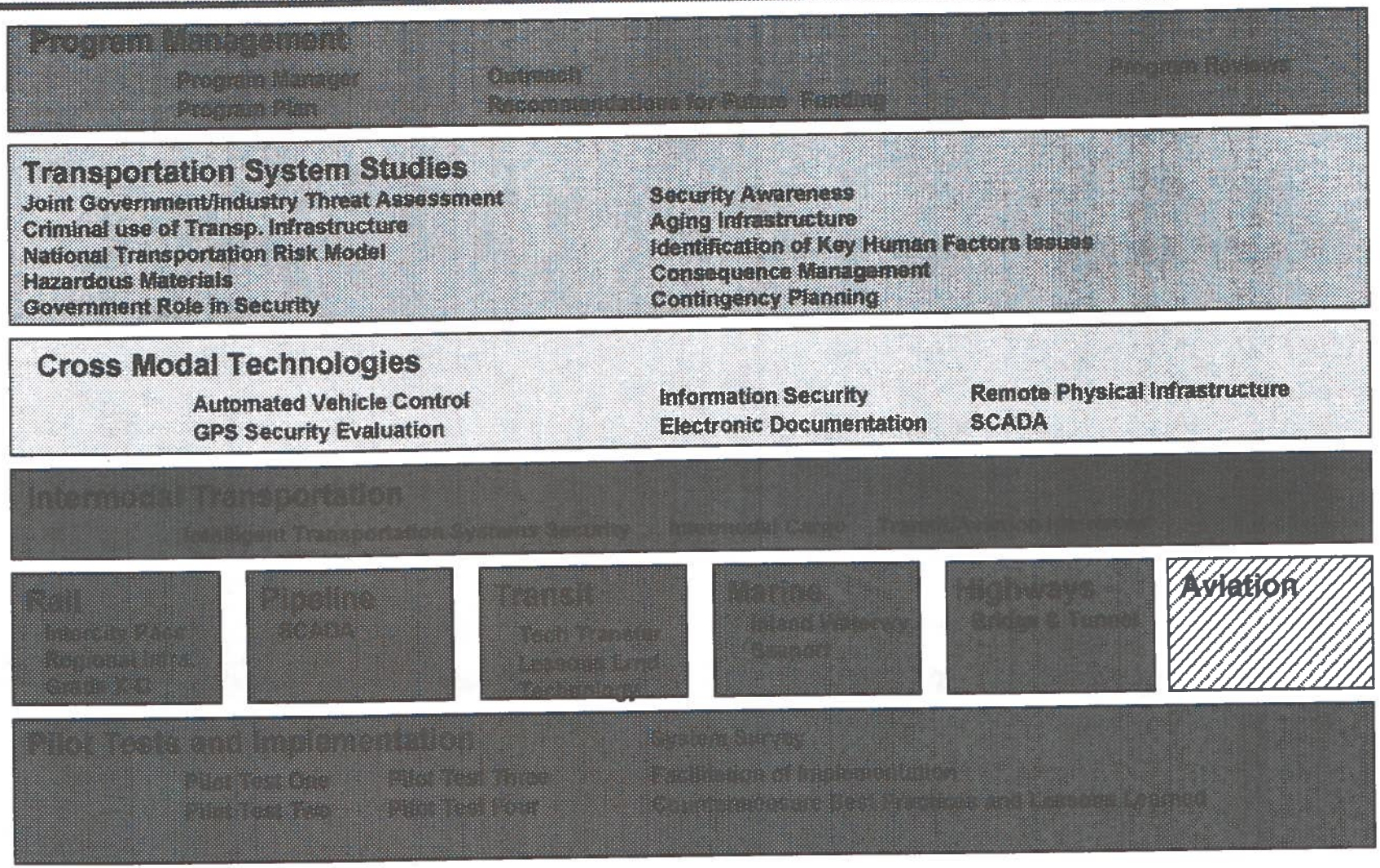
Solutions

- Organization
- Procedures
- Technology
- Information Collection, Management and Distribution

Ongoing Infrastructure Vulnerability Efforts

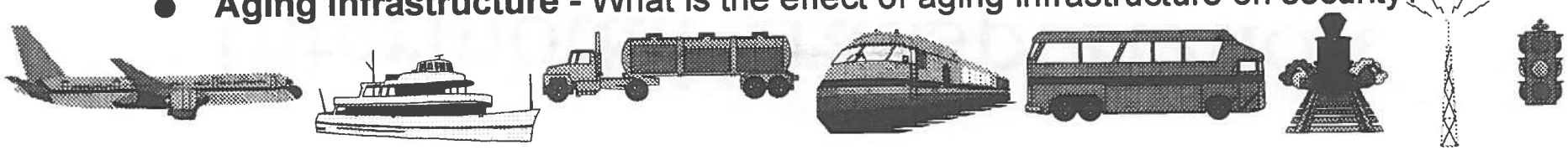
- President's Commission on Critical Infrastructure Protection and Infrastructure Protection Task Force
- NSTC Interagency Information Infrastructure Planning Team
- National Security Telecommunications Advisory Committee
- DOE Chem Bio Research Group
- Naval Surface Warfare Center Joint Program Office for Special Technology Countermeasures
- Technical Security Working Group, OSD Study on Information Infrastructure and Infrastructure Day After Games, National Defense University Information Warfare School, Transcom

Vulnerability Assessment -Program Activities



Transportation System Assessments

- Intermodal, Cross Modal, Modal
  - **Joint Government Industry Threat Assessment** - Describe to the industry and modes the current threat.
  - **Security Awareness** - Red teams and Table top Exercises to show need.
  - **Criminal Use of Transportation Infrastructure** - What is the effect of the misuse off transportation on the infrastructure?
  - **National Transportation Vulnerability Database** - Develop a means to maintain this information in the future.
  - **Government Role in Security** - How can government improve security in nonfederal infrastructure?
  - **Best Practices and Lessons Learned** - Demonstrate that the security countermeasures work in operation.
  - **Hazardous Materials** - Can hazardous material be used as a weapon against the infrastructure?
  - **Aging Infrastructure** - What is the effect of aging infrastructure on security?



Intermodal Transportation

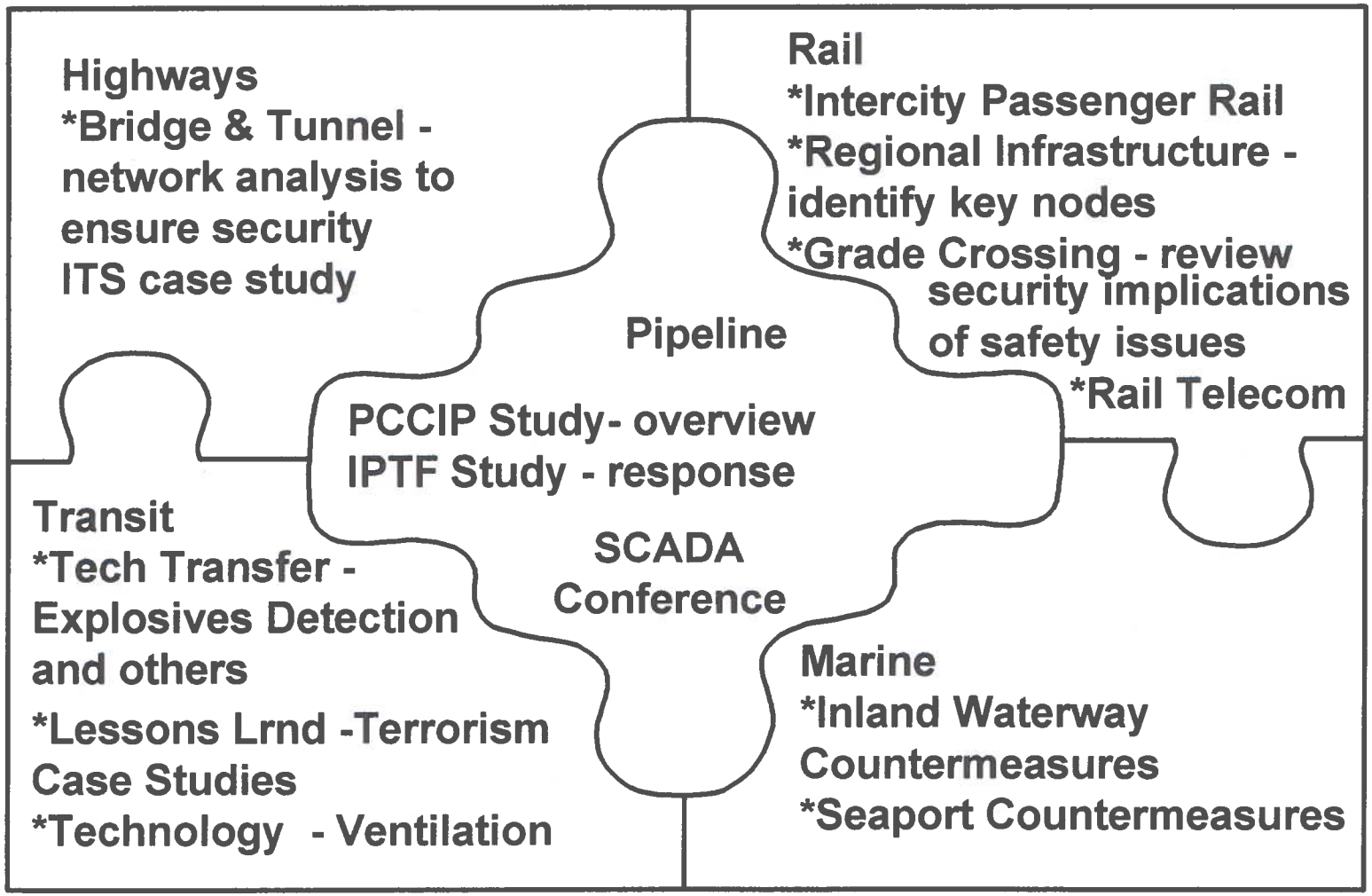
- Learning to include security in intermodal systems

- **Intelligent Transportation Systems Security**
  - » Information Infrastructure studies.
  - » Case study of new statewide infrastructure (e.g., MD)
- **Intercity Rail**
  - » Transit and Rail must coexist and ensure security on the same infrastructure.
- **Intermodal Cargo**
  - » Consider tracking, loss prevention and expedited cargo.
  - » Review Hijacking, terrorism and economic loss.
- **Surface/Aviation Interfaces**
  - » The security needs of aviation often drive the intermodal connections at airport - develop guidance for other modes.

Cross Modal Technologies

- Address Security Technology Issues common to multiple modes
  - **Automated Vehicle Control** - Evaluate security concerns as all modes move toward more vehicular automation.
  - **Information Security** - Leverage DOD knowledge in the development of the transportation information infrastructure.
  - **Remote Physical Infrastructure** - Address the need to secure remote elements of the infrastructure.
  - **GPS Security Evaluation** - What are transportation needs in GPS Security?
  - **Electronic Documentation** - Evaluate risks to Infrastructure from lack of confidentiality of documentation.
  - **Software Control and Data Acquisition (SCADA)** - Evaluate the responsibilities of operators when using software control.

Modal Tasks


Highways
*Bridge & Tunnel - network analysis to ensure security
ITS case study
Rail
*Intercity Passenger Rail
*Regional Infrastructure - identify key nodes
*Grade Crossing - review security implications of safety issues
*Rail Telecom
Pipeline
PCCIP Study- overview
IPTF Study - response
SCADA Conference
Transit
*Tech Transfer - Explosives Detection and others
*Lessons Lrnd -Terrorism Case Studies
*Technology - Ventilation
Marine
*Inland Waterway Countermeasures
*Seaport Countermeasures

Pilot Tests and Facilitation

- Use when best practices are not available
- Chosen to address key concerns
  - » The countermeasure has significant potential to reduce major impacts of priority vulnerabilities;
  - » Federal funding and facilitation will promote development and implementation of countermeasures which might not otherwise occur, or would be delayed;
  - » Large potential applications exist for the results of the pilot test and implementation by stakeholders is likely; and
  - » Public agency and private sector participants and contributions to the pilot testing are available.
- Facilitation used when industry is ready to implement but barriers exist

Conference on U.S. Marine Transportation Systems Vulnerability
May 28-29, 1997
Leesburg, Virginia

List of Attendees

Mr. Edward J. Alford
Manager of Contraband Prevention and Safety
Crowley American Transport, Inc.
P.O. Box 359004
Fort Lauderdale, FL 33335
Phone: (305) 470-4089
Fax: (305) 470-4064
E-mail:

Mr. Patrick J. Andrich
Manager of Los Angeles Cruise Ship Terminals
Metropolitan Stevedore Company
720 East E Street
P.O. Box 547
Wilmington, CA 90748
Phone: (310) 514-4049
Fax: (310) 514-4057
E-mail:

Mr. Edward V. Badolato
Contingency Management Services
2202 King's Garden Way
Falls Church, VA 22043
Phone: (703) 706-5311
Fax: (703) 821-7789
E-mail: bado@erols.com

Captain B. A. Bowditch, Jr.
Manager, Compliance Department
Lykes Bros. Steamship Co., Inc.
111 East Madison Street
Tampa, FL 33602
Phone: (813) 276-4731
Fax: (813) 209-4913
E-mail: bbowditchj@aol.com

Dr. Ronald Casey, Ed.D.
Senior Consultant
Educational Security Safety Consultants, Inc.
P.O. Box 245
Shrub Oak, NY 10588-0245
Phone: (914) 528-9175
Fax:
E-mail: ess@computer.net

Mr. Rodney L. Cook
Office of Systems Engineering
Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142
Phone: (617) 494-2203
Fax: (617) 494-3066
E-mail: cookr@volpe2.dot.gov

Ms. Nancy A. Cooney
Intermodal and Logistics Systems Division, DTS-36
Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142
Phone: (617) 494-2523
Fax: (617) 494-3013
E-mail: cooney@volpe1.dot.gov

CAPT Scott P. Cooper
United States Coast Guard
2100 Second Street SW
Washington, D.C. 20593-0001
Phone: (202) 267-1430
Fax: (202) 267-1416
E-mail: scooper@comdt.uscg.mil

Mr. David L. Damm-Luhr
Chief, Change Management Division, DTS-69
Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142
Phone: (617) 494-2102
Fax: (617) 494-3398
E-mail: dammluhr@volpe1.dot.gov

Mr. Robert DelCore
Manager, Police Training and Education
International Association of Chiefs of Police
515 North Washington Street
Alexandria, VA 22314-2357
Phone: (703) 836-6767, ext. 234
Fax: (703) 836-4543
E-mail: del3047@erols.com

Mr. Michael G. Dinning
Chief, Safety and Security Systems Division, DTS-38
Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142
Phone: (617) 494-2422
Fax:
E-mail:

Mr. Charles N. Dragonette
Senior Analyst
Civil Maritime Analysis Department
Office of Naval Intelligence
4251 Suitland Road
Washington, D.C. 20395
Phone: (301) 669-3261
Fax: (301) 669-3247
E-mail: sea-dragon@juno.com

Mr. Paul F. Duffy
Security Manager
Birdsall, Inc. - Agent for Tropical Shipping
4 East Post Road
Riviera Beach, FL 33404-6902
Phone: (561) 881-3962
Fax: (561-840-2840
E-mail: p.duffy@tropical.com

LT Michael Edgerton
Chief, Port Security Branch (G-MOR-3)
United States Coast Guard
2100 Second Street SW
Washington, D.C. 20593-0001
Phone: (202) 267-6439
Fax: (202) 267-4085
E-mail: medgerton@comdt.uscg.mil

Mr. Thomas J. Falvey
Commissioner
President's Commission on Critical Infrastructure Protection
P.O. Box 46258
Washington, D.C. 20050-6258
Phone: (703) 696-9395
Fax: (703) 696-9410
E-mail: Thomas.Falvey@PCCIP.GOV

Mr. Dwight Fender
Director of Operations
Canaveral Port Authority
P.O. Box 267
Cape Canaveral, FL 32920
Phone: (407) 783-7831
Fax: (407) 784-6223
E-mail:

CDR Jeffrey Gabrielson
U.S. Department of Transportation (S-60)
400 Seventh Street SW
Washington, D.C. 20590
Phone: (202) 366-6525
Fax:
E-mail:

Mr. C. David Gelly, CPP
Manager of Security
Sara Lee Knit Products
P.O. Box 3019
Winston-Salem, NC 27102
Phone: (910) 519-5057
Fax: (910) 519-4020
E-mail: david.gelly@slap.com

Ms. Patricia K. Hammar
U.S. Department of Transportation
400 Seventh Street SW
Room 8417
Washington, D.C. 20590
Phone: (202) 366-0375
Fax: (202) 366-3671
E-mail: hammar@volpe2.dot.gov

VADM A. J. Herberger, USN-Ret.
U.S. Department of Transportation
Maritime Administration
400 Seventh Street SW
Washington, D.C. 20590
Phone: (202) 366-5823
Fax: (202) 366-3890
E-mail: Albert.Herberger@MARAD.dot.gov

Mr. Jeffrey B. Hirsch
Ports & Intermodal Representative
U.S. Department of Transportation
Maritime Administration
26 Federal Plaza, Room 3737
New York, NY 10278
Phone: (212) 264-1300
Fax: (212) 264-1958
E-mail:

Mr. Gary Hobday
EG&G Dynatrend
Four Cambridge Center, 9th Floor
Cambridge, MA 02142
Phone: (617) 374-5065
Fax: (617) 494-1627
E-mail: hobday@volpe3.dot.gov

Mr. Anthony Infante
Police Operations Captain
The Port Authority of NY & NJ
Newark International Airport
Building #10, Tower Road
Newark, NJ 07114
Phone: (201) 961-6317
Fax: (201) 961-6383
E-mail:

Mr. Michael J. Jukoski
National Institute of Justice
Office of Science and Technology
633 Indiana Avenue NW
Washington, D.C. 20531
Phone: (202) 616-9805
Fax: (202) 307-9907
E-mail: jukoskim@ojp.usdoj.gov

Ms. Antoinette Kelly
Management Consultant
Unisys Corporation
Four Cambridge Center, 9th Floor
Cambridge, MA 02142
Phone: (617) 374-5829
Fax: (617) 494-1627
E-mail: kellya@volpe3.dot.gov

Mr. Donald J. Kerlin
Chief, Passenger Vessel Security Division
National Maritime Center, United States Coast Guard
4200 Wilson Blvd., Suite 510
Arlington, VA 22203-1804
Phone: (703) 235-1819
Fax: (703) 235-1062
E-mail: dkerlin@ballston.uscg.mil

Mr. Patrick J. Lennon
Director of Technical Security
Vance International Investigative Services, Inc.
10467 White Granite Drive, Suite 210
Oakton, VA 22124-2700
Phone: (703) 385-6754
Fax: (703) 359-8456
E-mail:

Mr. Lennart E. Long
Security Systems Programs Manager
Safety and Security Systems Division, DTS-38
Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142
Phone: (617) 494-2251
Fax: (617) 494-2684
E-mail: l.long@ieee.org

Mr. Steve Losier
Unisys/SRC
Four Cambridge Center, 9th Floor
Cambridge, MA 02142
Phone: (617) 374-5040
Fax: (617) 494-1627
E-mail: losier@volpe5.dot.gov

Ms. Karen Martini
Regional Sales Manager
Control Screening LLC
234 Industrial Parkway
Northvale, NJ 07647
Phone: (201) 784-1400
Fax: (201) 784-1583
E-mail:

Mr. Steven A. Masterson
Security Consultant
P.O. Box 33
Shrewsbury, MA 01545
Phone:
Fax:
E-mail:

Mr. Thomas Morelli
Coordinator for Maritime Intelligence & Security
U.S. Department of Transportation
Maritime Administration, Room 7201
400 Seventh Street SW
Washington, D.C. 20590
Phone: (202) 366-5473
Fax: (202) 366-6988
E-mail:

Dr. Robert Mullen
Office of Intelligence
U.S. Department of Energy, IS-30/OTA
1000 Independence Avenue SW
Washington, D.C. 20585
Phone:
Fax:
E-mail:

Mr. Robert E. Perez
Senior Inspector
United States Customs Service
Hemisphere Center, Rt. 1-9 South
Newark, NJ 07114
Phone: (202) 927-5601
Fax: (201) 645-3450
E-mail:

RADM Paul J. Pluta
Office of Intelligence and Security
U.S. Department of Transportation
400 Seventh Street SW
Washington, D.C. 20590
Phone: (202) 366-6525
Fax: (202) 366-7261
E-mail: paul.pluta@ost.dot.gov

Mr. Robert L. Pray, Capt. USCG-Ret.
Volpe/EG&G Dynatrend
Four Cambridge Center, 9th Floor
Cambridge, MA 02142
Phone: (617) 374-5061
Fax: (617) 494-1627
E-mail: pray@volpe5.dot.gov

Mr. Paul Rodgers
Physical Security Specialist
U.S. Immigration & Naturalization Service
Office of Security, 425 Eye Street NW
Washington, D.C. 20536
Phone: (202) 307-5816
Fax:
E-mail:

Ms. Dorothy M. Schulz, Ph.D.
Associate Professor
John Jay College of Criminal Justice
899 Tenth Avenue, John Jay Square
New York, NY 10019
Phone: (212) 237-8405
Fax:
E-mail:

Mr. John Short
Director of Studies and Analysis
Analytic Systems Engineering Corp.
3920 Lansing Court
Dumfries, VA 22026
Phone: (703) 441-0181
Fax: (703) 441-0205
E-mail: jshortasec@aol.com

Mr. Laird K. Smith
Unisys Corporation
1700 North Moore Street, Suite 1025
Arlington, VA 22209
Phone: (703) 812-3158
Fax: (703) 312-9026
E-mail: lsmith@volpe4.dot.gov

Mr. Barry Tarnef
Marine Loss Control Consultant
Chubb & Son
One Liberty Place
1650 Market Street
Philadelphia, PA 19103
Phone: (215) 981-8140
Fax: (215) 569-9418
E-mail:

Mr. John Tichenor
Marine Surveyor
Harborside Office, Cigna Insurance
745 Garfield Avenue
Jersey City, NJ 07305
Phone: (201) 434-7498
Fax: (201) 434-5971
E-mail:

Mr. Tony Velazquez
Federal Bureau of Investigation
16320 NW 2nd Avenue
Miami, FL 33169
Phone: (305) 787-6596
Fax: (305) 787-6538
E-mail:

Mr. Bradford Walton
Director, Business Development, Systems Engineering
Information Systems Group
BTG, Inc.
3877 Fairfax Ridge Road, 3E
Fairfax, VA 22030-7448
Phone: (703) 383-8682
Fax: (703) 383-4080
E-mail: bwalton@btg.com

Lieutenant Herman S. Wilkins
Maryland Port Administration
Police Department
P.O. Box 3908
Baltimore, MD 21222
Phone: (410) 633-1056
Fax: (410) 633-1064
E-mail:

Ms. Joan B. Yim, AICP
Program Manager for Marine Services
Parsons, Brinckerhoff, Quade & Douglas, Inc.
700 11th Street NW, Suite 710
Washington, D.C. 20001
Phone: (202) 783-0241
Fax: (202) 783-0229
E-mail: yim@pbworld.com