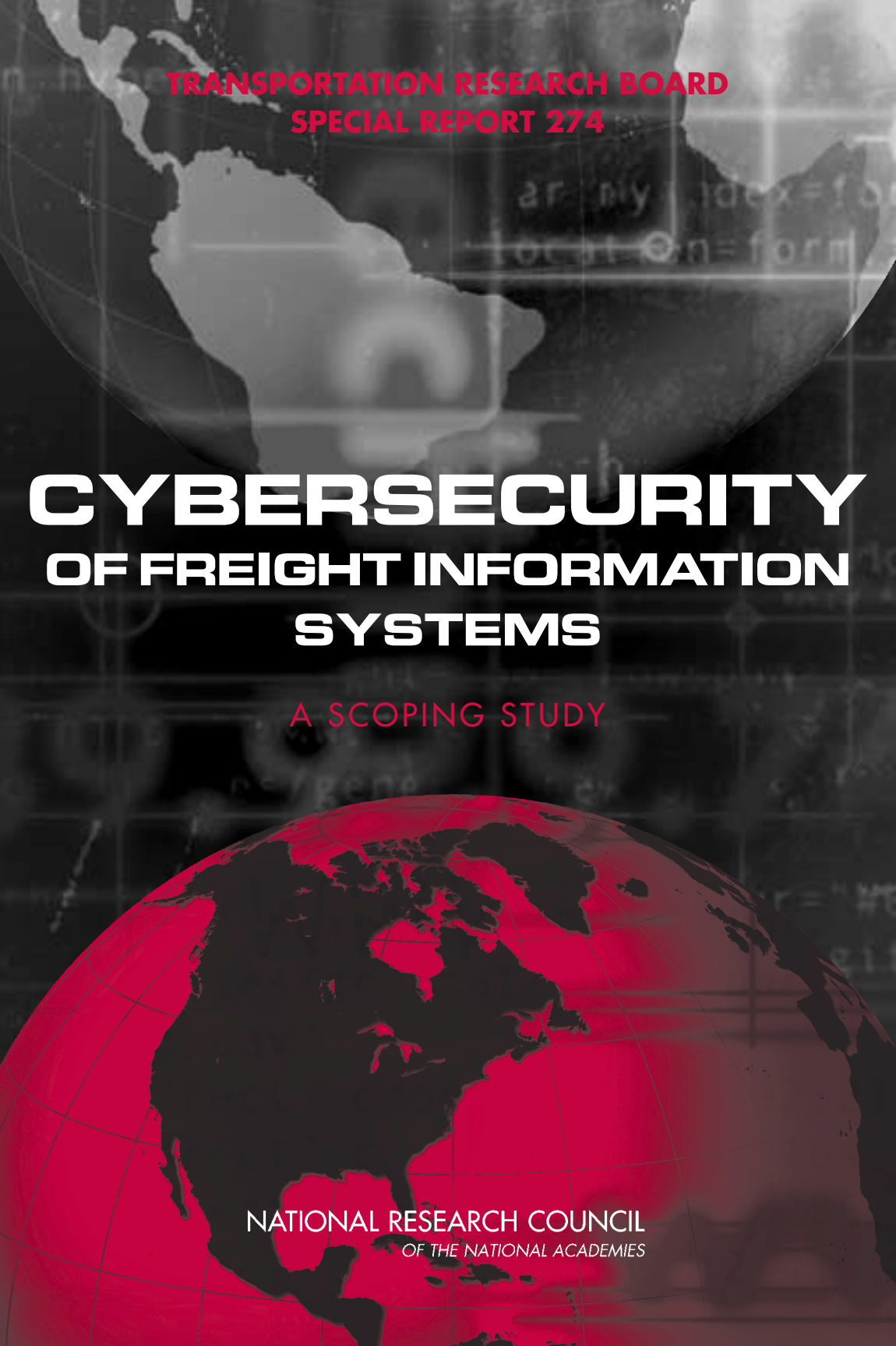


TRANSPORTATION RESEARCH BOARD
SPECIAL REPORT 274

CYBERSECURITY OF FREIGHT INFORMATION SYSTEMS

A SCOPING STUDY

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

TRANSPORTATION RESEARCH BOARD SPECIAL REPORT 274

CYBERSECURITY OF FREIGHT INFORMATION SYSTEMS

A SCOPING STUDY

Committee on Freight Transportation Information Systems Security

Computer Science and Telecommunications Board

Transportation Research Board

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

TRANSPORTATION RESEARCH BOARD
Washington, D.C.
2003
www.TRB.org

Transportation Research Board Special Report 274

Subscriber Categories
VIII freight transportation (multimodal)
IX marine transportation

Transportation Research Board publications are available by ordering individual publications directly from the TRB Business Office, through the Internet at www.TRB.org or national-academies.org/trb, or by annual subscription through organizational or individual affiliation with TRB. Affiliates and library subscribers are eligible for substantial discounts. For further information, contact the Transportation Research Board Business Office, 500 Fifth Street, NW, Washington, DC 20001 (telephone 202-334-3213; fax 202-334-2519; or e-mail TRBsales@nas.edu).

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competencies and with regard for appropriate balance.

This report has been reviewed by a group other than the authors according to the procedures approved by a Report Review Committee consisting of members of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine.

The study was sponsored by the Research and Special Programs Administration of the U.S. Department of Transportation.

Library of Congress Cataloging-in-Publication Data

National Research Council (U.S.). Committee on Freight Transportation Information Systems Security.
Cybersecurity of freight information systems : a scoping study / Committee on Freight Transportation Information Systems Security, Transportation Research Board of the National Academies.
p. cm.—(Special report)
ISBN 0-309-08555-1
1. Telecommunication—Safety measures. 2. Freight and freightage—Security measures. I. Title. II. Special report (National Research Council (U.S.). Transportation Research Board)

TK5103.2.N39 2003
388′.044′028558—dc22

2003056526

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. On the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Bruce M. Alberts is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. William A. Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, on its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both the Academies and the Institute of Medicine. Dr. Bruce M. Alberts and Dr. William A. Wulf are chair and vice chair, respectively, of the National Research Council.

The **Transportation Research Board** is a division of the National Research Council, which serves the National Academy of Sciences and the National Academy of Engineering. The Board's mission is to promote innovation and progress in transportation through research. In an objective and interdisciplinary setting, the Board facilitates the sharing of information on transportation practice and policy by researchers and practitioners; stimulates research and offers research management services that promote technical excellence; provides expert advice on transportation policy and programs; and disseminates research results broadly and encourages their implementation. The Board's varied activities annually engage more than 4,000 engineers, scientists, and other transportation researchers and practitioners from the public and private sectors and academia, all of whom contribute their expertise in the public interest. The program is supported by state transportation departments, federal agencies including the component administrations of the U.S. Department of Transportation, and other organizations and individuals interested in the development of transportation. **www.TRB.org**

www.national-academies.org

Computer Science and Telecommunications Board

David D. Clark, Massachusetts Institute of Technology, *Chair*
Eric Benhamou, 3Com Corporation
David Borth, Motorola Labs
John M. Cioffi, Stanford University
Elaine Cohen, University of Utah
W. Bruce Croft, University of Massachusetts, Amherst
Thomas E. Darcie, University of Victoria
Joseph Farrell, University of California, Berkeley
Joan Feigenbaum, Yale University
Hector Garcia-Molina, Stanford University
Wendy Kellogg, IBM T.J. Watson Research Center
Butler W. Lampson, Microsoft Corporation
David Liddle, U.S. Venture Partners
Tom M. Mitchell, Carnegie Mellon University
David A. Patterson, University of California, Berkeley
Henry (Hank) Perritt, Chicago-Kent College of Law
Daniel Pike, GCI Cable and Entertainment
Eric Schmidt, Google Inc.
Fred B. Schneider, Cornell University
Burton Smith, Cray Inc.
Lee Sproull, New York University
William Stead, Vanderbilt University
Jeannette M. Wing, Microsoft Research; Carnegie Mellon University (on leave)

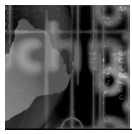
Marjory S. Blumenthal, Director

Committee on Freight Transportation Information Systems Security

Robert E. Gallamore, *Chair,* Director, Transportation Center, Northwestern University
A. Ray Chamberlain, *Vice Chair,* Vice President, Parsons Brinckerhoff, Inc.
Frank J. Anstett, Manager, Infrastructure Security, Raytheon Company
Samuel H. Banks, Senior Vice President, U.S. Customs Modernization Project, Sandler and Travis Trade Advisory Services
Richard A. Holmes, Jr., General Director, Security and Quality Assurance, Union Pacific Railroad
Barry Horowitz, NAE, Professor, Department of Systems Engineering, University of Virginia
John L. King, Professor and Dean, School of Information, University of Michigan
Lars Kjaer, Vice President, World Shipping Council
Art Kosatka, Chief Executive Officer, TranSecure LLC
Steven J. Lambright, Vice President, Savi Technology
Daniel Murray, Director of Research, American Transportation Research Institute
Frank M. Pittelli, President, Navius Technologies, LLC
Alan F. Spear, President, MRC Investigations (USA), Inc.
Karen Ryan Tobia, Manager, Technology Planning, Port Commerce Department, Port Authority of New York and New Jersey

National Research Council Staff

Alan T. Crane, Study Director
Steven Woo, Program Officer



PREFACE

The merger of information system technology and transportation infrastructure is transforming the freight transportation industry in a variety of ways. These changes are producing new ways to organize companies' supply chains as well as military logistics. As the new freight information systems become more fully integrated, they are expected to have great private and public benefits.

These systems, however, may be vulnerable to cyberattack. In accordance with the national initiative to increase security of critical infrastructure, the U.S. Department of Transportation (DOT) requested that the National Research Council (NRC) review trends in the use of information technology in the freight transportation industry and assess potential vulnerabilities to a cyberattack. In response, NRC formed the Committee on Freight Transportation Information Systems Security, under the Transportation Research Board (TRB) and the Computer Science and Telecommunications Board, to conduct a scoping study to develop an approach, study, or other process that DOT could use to address the vulnerabilities of freight information systems.

Specifically, the committee was charged with recommending how to conduct a study that would result in

1. A baseline description of the U.S. freight transportation communication and information systems, including interconnectivity with international carriers, government entities (U.S. and non-U.S.), customers, and other business partners;

2. A summary of ongoing and emerging efforts in such areas as electronic data interchange, telecommunications and data transfer, trends in the use of the Internet, business practices, customs, immigration and agriculture clearance processes, electronic letters of credit, integrated logistics software, positive train control, intelligent transportation systems, and all other information- and communication-based processes and technology improvements that affect transportation, shipping, and logistics;

3. A review of current industry practices addressing security (with emphasis on information technology–related dimensions); and

4. An identification and summary of the potential vulnerabilities that may be created by the interconnection/interface and possible integration of these new systems.

One of the complexities of a project such as this is that developers and operators of the relevant system will be reluctant to discuss or admit to specific security weaknesses publicly. Thus the committee had to recommend a process that would permit the problems to be identified and addressed.

The committee held its first meeting on November 25–26, 2002. The project, from committee formation to final report, took 7 months. During that time the committee met twice at NRC headquarters in Washington, D.C. In addition, its members and staff held numerous telephone conferences to discuss their findings.

After the start of the study, the Department of Homeland Security (DHS), which incorporates many of the relevant functions formerly performed by DOT, was created. Hence the committee directs many of its recommendations and comments to DHS as well as to DOT.

Acknowledgments

This report has been reviewed in draft form by individuals selected for their diverse technical expertise, in accordance with procedures approved by the NRC's Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making the published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments remain confidential to protect the integrity of the deliberative process.

The reviewers of this report were Noel D. Matchett, Information Security, Inc.; Steven B. Lipner, Microsoft Corporation; Peter Martin, Lakeville Motor Express; and David Zanca, Federal Express. The committee is grateful for the many constructive comments and suggestions the reviewers provided. The reviewers were not, however, asked to endorse the findings and conclusions, nor did they see the final draft before its release. Responsibility for the final content of this report rests entirely with the authoring committee and NRC.

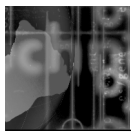
The review of this report was overseen by Lester A. Hoel, University of Virginia, Charlottesville. He was appointed by NRC to ensure that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Suzanne

Schneider, Associate Executive Director of TRB, managed the report review process. The committee appreciates the speed and efficiency of this review.

This study was managed by Alan T. Crane under the direction of the committee and the supervision of Stephen Godwin, Director of TRB's Studies and Information Services.

The report was written by the committee members and the NRC staff. The committee also appreciates the vital contributions of Jocelyn Sands, Frances E. Holland, and Amelia B. Mathis. Joedy W. Cambridge and Joseph A. Breen provided valuable suggestions while the committee was being formed. This report has been edited by Norman Solomon under the supervision of Nancy Ackerman, Director of Publications.

Robert E. Gallamore, Chair
A. Ray Chamberlain, Vice-Chair
Committee on Freight Transportation Information Systems Security



Acronyms and Glossary

ABI Automated Broker Interface.

ACE Automated Commercial Environment.

ACS Automated Commercial System.

AES U.S. Bureau of Customs and Border Protection's Automated Export System.

Airbill Receipt for carriage of air freight.

AMS U.S. Bureau of Customs and Border Protection's Automated Manifest System.

ANSI X12 Voluntary standards, maintained by the American National Standards Institute (ANSI), defining the structure, format, and content of business transactions conducted through electronic data interchange (EDI). ANSI X12 is produced by the committee ASC X12, supported by the Data Interchange Standards Association, Inc. (DISA).

APIS Advanced passenger information system.

ATIS Advanced traffic information system.

ATRI American Transportation Research Institute.

ATS Advance targeting system.

AVI Automatic vehicle identification.

BASSC Business Anti-Smuggling Security Coalition.

Bill of lading A statement of the nature and value of goods being transported, especially by ship, along with the conditions applying to their transport. Drawn up by the carrier, this document serves as a contract between the owner of the goods and the carrier.

CAMIR Customs Automated Interface Requirements.

CHCP Cargo Handling Cooperative Program.

CRM Customer relationship management.

CSTB Computer Science and Telecommunications Board of the National Academies.

CSI Container Security Initiative.

Cyberterrorism Terrorism related to computer and information systems.

DASD Direct-access storage device.

Denial-of-service (DOS) attack An attack on a computer network effected by overloading the access points, so that further access is slowed or stopped altogether.

DHS Department of Homeland Security.

DNS Domain name service.

DOT Department of Transportation.

Drayage Generally, carriage of freight, often by truck.

EA Enterprise architecture.

EDI Electronic data interchange.

ERP Enterprise resource planning.

ESCM Electronic supply chain manifest.

ExpressLink Proprietary system for interconnecting the corporate-level systems of four regional trucking companies.

FAA Federal Aviation Administration.

FAST Free and Secure Trade.

FBI Federal Bureau of Investigation.

FHWA Federal Highway Administration.

Firewalls Hardware and software systems intended to isolate a local area network from access.

FIRST Freight Information Real-Time System (for Port Authority of New York and New Jersey).

Forwarder A company that ships cargo for hire.

Freight brokers A company that arranges or consolidates freight shipments.

Freight forwarder See "forwarder."

GPS Global Positioning System.

Hazmat Hazardous material.

IBIS Interagency Border Information System.

INS Immigration and Naturalization Service.

ISAC Information Sharing and Analysis Center.

ISO International Standards Organization.

IT Information technology.

ITDS International Trade Data System.

ITS Intelligent transportation systems.

Jones Act The Merchant Marine Act of 1920 and related statutes, requiring that vessels used to transport cargo and passengers between U.S. ports be owned by U.S. citizens, built in U.S. shipyards, and manned by U.S.-citizen crews.

Just-in-time (JIT) A business system of supplying to each process what is needed at the time it is needed, and in the quantity needed, to minimize production lead times and reduce inventory.

LIA Logistics Integration Agency.

Load bidding For carriers, the practice of negotiating for freight.

Merchant haulage Transport of cargo in shipping containers arranged by the owner or possessor of the goods.

MTMC Military Traffic Management Command.

NHS National Highway System.

NOA Notice of arrival.

NRC National Research Council of the National Academies.

NVMC National Vessel Movement Center.

NVOCC Non–vessel operating common carrier.

OSC Operation Safe Commerce.

Positive train control The use of digital data communications, automatic positioning systems, wayside interface units (to communicate with switches and wayside detectors), onboard and control center computers, and other advanced display, sensor, and control technologies to manage and control railroad operations.

Red teaming Acting as an adversary for the unauthorized access to a physical or computer system to expose the system's vulnerabilities.

RFID Radio frequency identification.

R&D Research and development.

SCADA Supervisory control and data acquisition.

Sim-Tag Simulator for RFID tags.

SSTL Smart and Secure Trade Lanes.

TECS Treasury Enforcement Communications System.

Third-party logistics provider (3PL) Provider of logistics services for hire.

TRB Transportation Research Board of the National Academies.

TSA Transportation Security Administration.

TSWG Trucking Security and Anti-Terrorism Working Group.

TWIC Transportation worker identification card.

USDOT U.S. Department of Transportation.

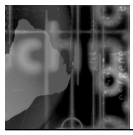
VHF Very high frequency.

VPN Virtual private network.

Waybill Shipping document.

WCO World Customs Organization.

XML Extensible markup language.



CONTENTS

Executive Summary **1**

1 The Evolving Freight Industry **13**
How Efficient Transportation Creates Economic Growth 13
Differences Among Modes 16

2 Freight Information System Technologies **19**
Existing IT Applications 20
IT Trends and Emerging Technologies 26

3 Planning a Full Study **39**
Assessing Security Issues 40
Study Plan 43

Appendixes
A Information Management Systems in the International Liner Shipping Industry 47
B Security Initiatives and Programs with Cybersecurity Relevance 55
C Protecting International Trade Corridors: The Operation Safe Commerce Initiative 63
D U.S. Bureau of Customs and Border Protection Use of Information Technology 69

Study Committee Biographical Information **75**

Executive Summary

The potential vulnerability of freight transportation information systems to terrorist attacks is a serious concern for homeland security. In this report the groundwork is laid for a study of the cybersecurity of the information systems on which freight transportation depends to facilitate efficient delivery of the goods and materials that drive the economy.

The development of computer security system designs and strategies for the freight transportation industry must be accomplished within a framework that is sensitive to the following important attributes of the industry:

1. It consists of different carrier modes (i.e., truck, rail, sea, air, and pipeline). Its companies cover a wide range of characteristics, including size, economic condition, technical know-how, cargo types, and geographical location. This diversity makes it difficult to develop a uniform security design concept with managed implementation schedules. Instead, evolutionary steps tailored to the different parts of the industry on a case-by-case basis must be developed to address identified vulnerabilities.

2. The existing freight transportation information system is a confederation of company-to-company information system integrations constructed to permit more efficient operation. The design is not uniform, not specified, not documented, not evaluated, not tested, and not under configuration control. These features make security design analysis and evaluation extraordinarily difficult.

3. Many potential cyberattacks on the freight transportation industry would result in consequences to stakeholders other than the industry itself. For example, (*a*) customers that depend on the freight industry for tightly managed supply delivery schedules can suffer significantly when deliveries are delayed; (*b*) safety-related attacks, such as an attack on a hazmat freight vehicle, would affect the general public directly; and (*c*) political attacks, such as threats to import a nuclear weapon into the United States, would affect the

government's policies on imports. Consideration of possible measures to address such scenarios, and their costs, should reflect these facts.

As a result of this situation, a focused, evolutionary process for identifying and prioritizing security enhancements will be required. Development and implementation of such a process are likely to be slower than one might like, so there is a need to focus efforts on the most critical areas. Otherwise, unnecessary expense will be incurred, and, under some conditions, the efforts might even be counterproductive—every change to the system introduces the risk of new vulnerabilities.

Types of Threats

Cyberattacks on transportation and logistics networks could take several different forms, with varying consequences and probabilities. Reducing vulnerability requires consideration of all plausible types, including those discussed here. The first one is a direct attack on the information systems, while the latter two use information technology (IT) to enable or amplify a physical attack. It should be noted that a physical attack on the IT systems coordinated with a cyberattack could cause far more damage than either type alone. This report, however, is concerned only with cyberattacks, which would not differ much if they were accompanied by physical attacks. The full study should consider all types of threats involving cyberattacks, and their consequences.

Denial of service: Cyberattacks, whether by terrorists or hackers, might bring down information systems with what is known as a "denial-of-service" attack. For example, the perpetrator might gain entry to a large number of unprotected computers on the Internet and program them to access selected websites simultaneously. The computers controlling these websites might then crash. Companies in other industries have been subjected to denial-of-service attacks on their websites and servers, which were probably perpetrated by individual hackers. Such attacks are not the subject of this report, which focuses on large-scale, organized attacks intended to inflict maximum economic damage over a long period of time. No massive, coordinated attacks have yet been launched on any network, but if directed at freight information systems, such attacks could disrupt freight service, causing significant damage to the economy.[1] A related concern is delib-

[1] Economic damage from the 12-day shutdown of West Coast ports in October 2002 due to labor–management issues probably exceeded $1 billion (Anderson and Geckil 2002). Damage was limited because the shutdown was widely anticipated. A cyberattack might have different consequences.

erate disruption of a military mobilization during a national crisis. Although individual freight companies may not be unusually vulnerable to such attacks, the interconnections of the industry's information systems and the increasing role of the Internet suggest the potential for widespread damage. One individual system whose loss could result in significant economic harm is that of the Bureau of Customs and Border Protection (Customs; formerly the U.S. Customs Service), because it is vital for the orderly flow of imports and exports.[2] The full study suggested by this report should also consider how quickly the system could recover from an attack and how well the freight system could operate in the interim. Of the three types of attacks, denial-of-service attacks probably are the easiest to perpetrate but the least damaging.

Hazardous material shipments: More than 800,000 hazmat shipments occur daily in the United States. Some are potential targets for terrorists trying to harm people or seeking materials for making weapons. Terrorists could hack into and misuse information systems to identify and track such shipments in order to attack them at high-consequence locations. Under some conditions, the malefactors might actually cause an accident resulting in the release of hazardous materials purely through a cyberattack, for example by seizing control of railroad switches or signals. Alternatively, terrorists might commandeer the supervisory control and data acquisition (SCADA) system of a pipeline network carrying dangerous material to maximize the damage following a physical attack.

Weapons of mass destruction: Terrorists trying to bring a weapon of mass destruction (chemical, biological, or nuclear) into the United States could disguise it as ordinary freight. They could exploit vulnerabilities in transportation information systems to mask and track their shipments, thus reducing the risk of detection. This approach is likely to become more attractive to terrorists as physical security requirements become more stringent. Terrorists also might use unauthorized access to freight information systems to move weapons around in the United States or export them to other countries. This type of attack could have extremely serious consequences, but it also may be the least likely, and the IT role in the attack may not be central. Information systems could, however, play a role in reducing physical vulnerability to such use of the freight transportation system.

All major industries are vulnerable to cyber- and physical attacks. **The freight transportation industry appears to offer unusual potential for *both***

[2] Loss of the air traffic control system could be even more devastating, but that is not included in this study because it is not an interconnected system and does not rely on the Internet. Therefore, it is much less vulnerable to terrorist cyberattacks than are freight information systems.

economic *and* physical damage from terrorist cyberattacks.[3] These concerns may grow because freight transport is increasingly dependent on IT. As long as the threat of terrorism remains, cybersecurity in the freight transport sector will be an important issue, although it is impossible to define the threat exactly or quantify it.

Key Characteristics of the Freight Transportation Industry

A cyberattack could come at any time and hit any point of vulnerability in the system. A variety of measures to reduce vulnerability are being implemented or considered. The factors discussed here and in more detail in Chapters 1 and 2 should be taken into account when such measures are considered.

Industry Scale and Complexity

Freight transportation is handled by a great many individual companies operating different modes of transport (e.g., ship, truck, train, air) in a large and complex global system. The industry uses millions of trucks, rail cars, containers, and so forth and employs millions of people to move billions of tons of freight annually. Some modes (e.g., air, rail, pipelines) are concentrated, with relatively few companies. Others (e.g., trucking, international shipping) include many companies, ranging from large and highly sophisticated organizations to "mom and pop" operations using manual or low-technology systems. The fragmented and changing nature of the industry, the diversity of the modes, and the lack of overall system security coordination can lead to vulnerability. Intense competition keeps profit margins low for companies in all modes, which limits their ability to fund new infrastructure, technology, and procedures if the return on investment is not readily apparent.

Public-Private Interactions

Freight operations in the United States are essentially all in the private sector, but they are intimately connected with the public sector. In addition to using government-owned facilities such as highways, ports, and airports, the freight

[3] For example, large parts of the electric network could be shut down by cyberattacks, but these probably would not cause much physical damage to system components. The system could then be restarted quickly. See *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (NRC 2002). It also should be noted that as systems become more automated, it may become easier for cyberattackers to cause physical damage.

transportation industry is affected by many aspects of government regulation—federal, state, local, and regional. Government monitoring (e.g., customs clearance, truck weighing, and even first responder monitoring of hazmat shipments) provides opportunities for unauthorized access to information systems, including the electronic cargo declarations submitted to Customs, because any entry point provides a potential vulnerability for cyberterrorists.

Information Systems Complexity

Freight information systems are a significant factor in the steadily improving efficiency of the industry. These systems also help provide highly reliable delivery, which, among other benefits, permits customers to operate with lower inventories, including "just-in-time" inbound materials strategies. The transport/logistics system functions globally, but it is made up of discrete and varied subsystems among the different modes and even among the companies within a mode. The system is not integrated; instead, the subsystems are only interconnected at many different points and in different ways. Many transport and logistics firms also connect with their customers and government agencies such as Customs. Each interconnection represents a point of potential vulnerability to attack. In addition, the ever-changing mix of carriers, shippers, distributors, and freight forwarders who are or can be connected to the "system" makes it very difficult to identify and authenticate users. The complexity and diversity of these systems are a serious challenge in the development and implementation of a comprehensive cybersecurity strategy for freight transportation information systems.

Overall Coordination

Coordination of efforts to reduce cybervulnerability is a major challenge. No single government agency, private firm, or association is in a position to consider the whole transportation/logistics continuum as a complex system. Instead, many different organizations have influence over fragments of the system. They act where they can, but that is not necessarily at the point of highest priority.

Vulnerabilities, Security, and Technologies

Many factors create potential vulnerabilities to cyberattacks on freight transportation information systems, including the interconnection of systems, the increased reliance on the Internet for communications, and the emergence of

decentralized systems. These potential vulnerabilities and associated technologies are discussed here. A fundamental issue is whether the improvement in security is adequate to justify the cost.

Interconnections

The interconnection of systems across large transportation sectors allows carriers, shippers, and manufacturers alike to increase the efficiency of their operations. As the web of interconnected information systems grows, however, it can become more susceptible to denial-of-service attacks, improper use, and unauthorized access.

Large organizations in the transportation sector have interconnected their own information systems to create systems spanning the enterprise. Smaller companies have interconnected their systems to create "federated" or "cooperative" systems that allow them to compete more effectively with larger organizations. In addition, regulatory forces (some motivated by post–September 11 homeland security concerns) are driving the interconnection of commercial and government systems by requiring carriers, importers, exporters, and manufacturers to submit more information electronically to the government. For example, Customs' Automated Manifest System represents a vital link in the flow of information about imported goods.

Documents such as bills of lading and letters of credit are essential for the shipments of goods. They are increasingly sent in electronic form, but electronic documents can easily be altered or counterfeited if they are not appropriately protected. Electronic data interchange standards exist for the transportation sector, but the sector has generally not incorporated authentication technologies into its emerging systems and standards to ensure the authenticity of the document author and that the document can be exchanged privately with another party.

Internet Communications

The Internet is used increasingly as the primary communication method among transportation partners or transportation carriers and their customers. Freight transportation has benefited from a revolution in logistics based largely on improved communications through the Internet. In supply chain management and the optimization of logistics, the ability to transmit data across the Internet reliably is critical. Improvements in supply chain efficiency have been an important factor in economic growth, as discussed in Chapter 1. The most critical security concern of the Internet is that attacks can come at any time and from

virtually anywhere in the world. It is inherently difficult to prevent such attacks or to identify the perpetrators afterwards, as noted in Chapter 2.

The Internet itself provides only minimal levels of access control and protection against eavesdropping. Virtual private network technology incorporates encryption and other security mechanisms to provide enhanced security for remote user-to-system and system-to-system communications over the Internet, but only for prearranged situations involving a small number of systems. In general, the lack of a widely accepted encryption infrastructure significantly impedes improved security.

Decentralized Systems

Since the introduction of Web-based application techniques in the early 1990s, system architects have been shifting the design of information systems from primarily centralized systems toward decentralized systems (networks that—like the Internet—operate without central control).

The most significant challenge for the use of wide-scale decentralized systems is that of developing the infrastructure needed to authenticate all of the users in the system. In the decentralized model, no central authority can resolve such issues, which makes security control more difficult, though still possible.

Other Developments

Many technologies now being implemented or tested for potential use in the freight transportation industry may have cybersecurity implications.

Embedded processors are, to varying degrees, being used or tested by the transportation sector, primarily for the identification and monitoring of shipments. *Radio frequency identification (RFID) tags* automatically identify an asset or its declared contents, or both. *E-sensors* detect and document environmental changes to a shipment along its route. *E-seals* are the electronic version of mechanical seals; they can be placed on shipments or structures to detect an unauthorized entry or deter intrusions because of the fear of detection. These devices are being studied in pilot programs (see Appendix B). They are intended to address aspects of physical security, not cybersecurity, but their links to transportation information systems suggest that they should be part of a study of IT vulnerability. For example, terrorists might hack into e-seals to conceal tampering with a container.

Several enabling technologies may become part of the transportation sector's IT infrastructure. *Wireless communications* (i.e., RF, infrared, terrestrial, satellite-based) can transmit information with mobile units. Wireless tracking systems already are used in the trucking industry, often for critical, high-value ship-

ments. Almost all of the embedded devices that may be used in the transportation sector rely on wireless communications. *Cryptography* is intended to maintain the privacy and integrity of information exchanged between two entities over a network and contributes to the verification of sender authenticity. *Smart cards* (or *smart tokens*) and digital certificates help to authenticate users. *Biometric devices* help to authenticate human beings through a physical attribute such as a fingerprint or voice pattern.

Assessing Potential Policy Options

Given the damage potential from cyberattacks on freight transportation IT systems, public and private options for enhancing cybersecurity should be identified and developed. The actual vulnerabilities, risks, and consequences of such attacks have not yet been determined, analytically or otherwise, for the various modes. Furthermore, no mechanism now exists for determining how much security is enough or which steps could be identified as having the highest priorities. Additional study as suggested here is intended to lead to a strategy for these issues.

A strategy to reduce vulnerability must account for the company composition and structure in each mode and the operations the companies perform. It must be based on an analysis of security gaps, the costs and benefits of current and emerging technologies and processes that could be implemented to enhance cybersecurity, and the ability of transport companies to implement them. The analysis that would permit such a strategy to be developed has not yet been conducted.

Some security measures may improve the efficiency of operations and pay for themselves as normal investments. Although they may not necessarily be a company's investment of choice, such measures would at least be of interest and should be a special focus of the proposed study. Other measures are expensive but may be effective in reducing the likelihood or consequences of a cyberattack. In such cases, the main beneficiary may be the public rather than the company that implements the measure. Since the risk of an attack cannot be specified and factored into the costs and benefits of preventing it, prioritizing potential steps to reduce vulnerability to cyberattacks is important.

The purpose of this report is to determine how such a study should be structured and the issues that it should address. It does not present a plan for implementing cybersecurity measures. As far as possible within the limited scope, the measures that might be considered and how they might apply to the freight transportation system are reviewed. Several concepts for further study are then suggested in order to develop a strategy for possible steps to reduce the sector's

potential vulnerability to cyberattacks in the least costly and disruptive way. More detail can be found in Chapter 3.

Task 1. Determine the chief vulnerabilities of freight transportation information systems. The first step is to identify and describe the main information systems used in the transportation sector and to understand the role they play in normal operations. These systems should then be analyzed for potential cybervulnerabilities. Much of this analysis would reflect IT vulnerability studies in general, but the specific use of the technologies in the freight industry would have to be reviewed in depth. Detailed information might be obtained with a series of interviews and perhaps a survey (if consistent with current administration requirements). The objective would be to develop a sufficiently detailed system description in a format appropriate for security analyses.

A variety of plausible attack scenarios would then be used to assess the systems as they exist now and as they may evolve, and the consequences should they be attacked successfully. The purpose would be to develop a full understanding of the kinds of vulnerabilities that should be accorded the highest priority. Analyses are then required of the expected costs (including interference with normal operations) in countering these specific types of potential vulnerabilities within each modal setting. Prioritization might be determined by combining the consequences of a successful exploitation of a vulnerability, the likelihood that such an attack could be mounted, the costs of reducing the vulnerability, and the impact on normal operations. While this prioritization could be done subjectively, it might also be possible to develop a methodology to do so more analytically. In either case, it is important that a system-level perspective be used to identify, assess, and compare the security issues at the level of components, subsystems, and the overall system.

Task 2. Review current industry and government practices addressing IT security. Security practices will be difficult to obtain in detail. Most companies will be understandably reluctant to discuss their practices and protective hardware and software because of concerns that any revelations could compromise security. It may be possible, as in Task 1, to obtain the information by interviews conducted under stringent assurances of nondisclosure. Companies and government agencies might be presented with a menu of security options and asked what they use. The effectiveness of these options, however, often lies in the stringency with which they are implemented. That

information will be even more difficult to procure. Interviewers must be well versed in the technology and its use, and they must be prepared to probe for details. The main purpose of this effort is to determine how the vulnerabilities and risks identified in Task 1 are being addressed.

Task 3. Determine the potential for IT-related security enhancements in the sector. This task is, in part, a follow-up to Task 2. Current and emerging technologies and practices should be examined to determine what role, if any, they could play in addressing identified security gaps and deficiencies. Integral to this assessment should be an understanding of the characteristics of the industry and an analysis of how realistic and attractive these technologies and practices would appear to decision makers. A key part of the study should be to research the costs and benefits of security measures as they might be implemented in the freight transportation sector. Other concepts might require government support because the benefits do not outweigh the costs to the company. Because IT costs may decline over time and with increasing scale of deployment, this task should also consider the feasibility of strategies that might make promising security measures more attractive.

Task 4. Analyze policies to reduce cybervulnerability. The U.S. government could play a useful role in disseminating information on new security options and best practices. It also might evaluate the extent to which these options were being implemented. This task could include the development of a set of cybersecurity guidelines and recommendations and consideration of how to promote their use most effectively in the freight transportation industry.[4] Part of the task might be to cooperate with companies in performing security audits, perhaps including "red teaming" to test security, and in other joint private–public initiatives. The same tests should be applied to the government's connections to the private-sector IT systems.

Task 5. Assess the economic impact of cost increases in the freight transportation industry. Some cybersecurity measures may supply economic benefits as well as security, as illustrated in Figure ES-1. For example, the use of digital signatures might reduce costs related to fraud detection and manage-

[4] The Administration released a national cybersecurity plan in February 2003 (see news.com.com/2100-1001-984697.html).

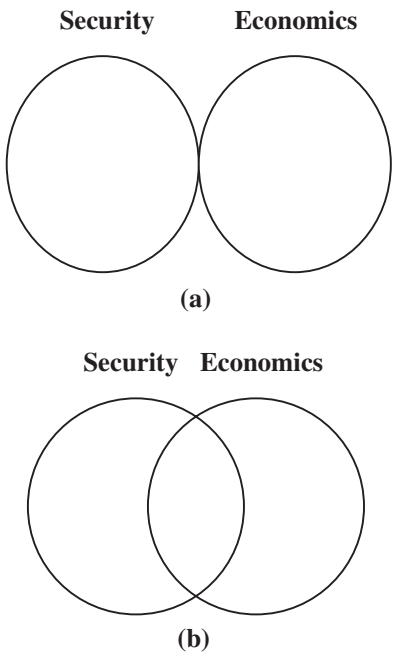


FIGURE ES-1 Relationship between security and economic benefits: (*a*) little or no economic benefit to security enhancements; (*b*) significant economic benefit to security enhancements.

ment and increase customer confidence. Other measures might protect against low-likelihood but very high-consequence events—for example, involving weapons of mass destruction. Such measures may have a high public value without significantly benefiting the company that implements them, which could result in economic inefficiency for the industry and the national economy.

This task should deal with but not be limited to the following issues:

1. At what levels and distribution of costs for security does the economic impact become a concern, both for the freight industry itself and its users?
2. On the basis of existing models for relating economic inputs and outputs, what changes in economic outputs might result from varying levels of investment in security?

3. Given the tight profit margins associated with the freight industry, is there a significant possibility of economic damage to the companies that constitute this industry?
4. For investments that may be needed for national security purposes but that provide little or no advantage to the company implementing the measures, what form of government participation (e.g., tax credits) would be most effective?

Results should be quantitative and be developed for a wide set of assumptions in order to permit consideration of a significant range of possible outputs.

References

Abbreviation

NRC National Research Council

Anderson, P. L., and I. K. Geckil. 2002. *Flash Estimate: Impact of West Coast Shutdown*. Anderson Economic Consulting Group, Lansing, Mich., Oct. 15.

NRC. 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. National Academies Press, Washington, D.C.

The Evolving Freight Industry

The nation's freight industry moves agricultural products and raw commodities to factories and finished goods to domestic and international markets. A major role is the handling of huge volumes of imported finished goods, much of it in containers. The industry's weight in the modern economy is only hinted at by its size—hundreds of billions of dollars in revenues and millions of employees (BTS 2002, Appendix A). The various modes carried more than 15 billion tons of merchandise, valued at more than $9.4 trillion, in 1998 (Figure 1-1). Freight transportation has enabled the rise of new logistics and supply chain systems. The new systems have led to explosive growth of world trade in the past decade, from which all consumers have benefited. Cheap and responsive transportation makes it possible to acquire parts and components from geographically diverse sources, manufacture and distribute goods without the need for expensive warehouses, and give customers wider choices of products and services. Overall, these advances have fueled economic growth.

How Efficient Transportation Creates Economic Growth

Commerce is an increasingly information-intensive process. Today's lean production methods and modern supply chain management require companies to forecast customer demand accurately; coordinate multiple suppliers (perhaps thousands); manage distribution of products and services; track and trace items in transit; and otherwise control the flow of materials through the organization, from raw materials to finished goods. These systems can be quite complex, and they all hinge on managing information (Chopra and Meindl 2001).

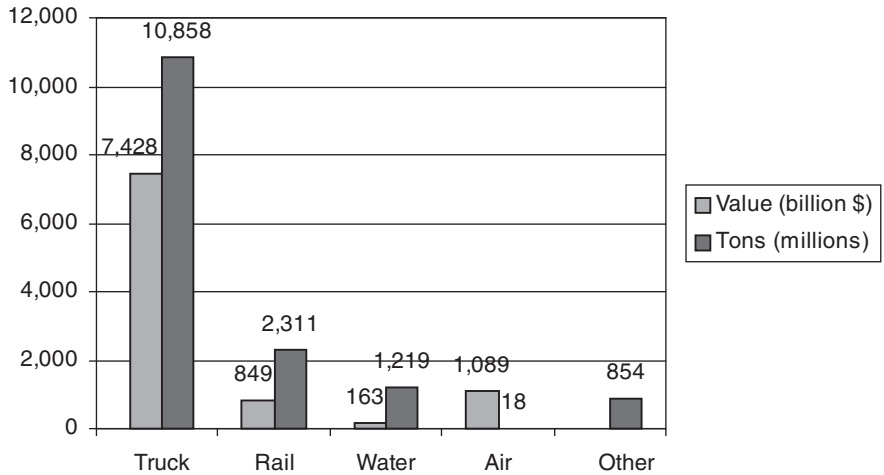


FIGURE 1-1 Value and tonnage of U.S. domestic freight shipments by mode; "other" is mainly pipelines, for which value is not available (FHWA 2000).

Supply Chain Management and World Trade

Manufacturers, retailers, and other users of transportation have grown accustomed to thinking of their supply chains (networks of manufacturers, wholesalers, distributors, and retailers, which turn raw materials into finished goods and services and deliver them to consumers) as important sources of competitive advantage. Supply chains increasingly are treated as integrated entities, and closer relationships between the organizations throughout the chain can produce competitive advantage, reduce costs, and help attract and maintain a loyal customer base.

Companies manage their supply chains to achieve strategic advantage, which often requires detailed models of the movements of goods and the flow of information between the organization and its suppliers and customers. The process of supply chain management is often called "logistics."

Today's supply chains are increasingly multinational, as companies seek the least costly suppliers consistent with efficient production. This shift has driven a remarkable rise in international trade. Merchandise trade worldwide has doubled in the past decade (Figure 1-2). The United States accounts for nearly one-fifth of the world market by value and a corresponding share of the demand for transportation. The Federal Highway Administration of the U.S. Department of Transportation (DOT) forecasts a further doubling by 2020 (FHWA 2002). This growth will offer economic opportunity but will strain the capacity of the nation's ports, other intermodal freight terminals, and highways.

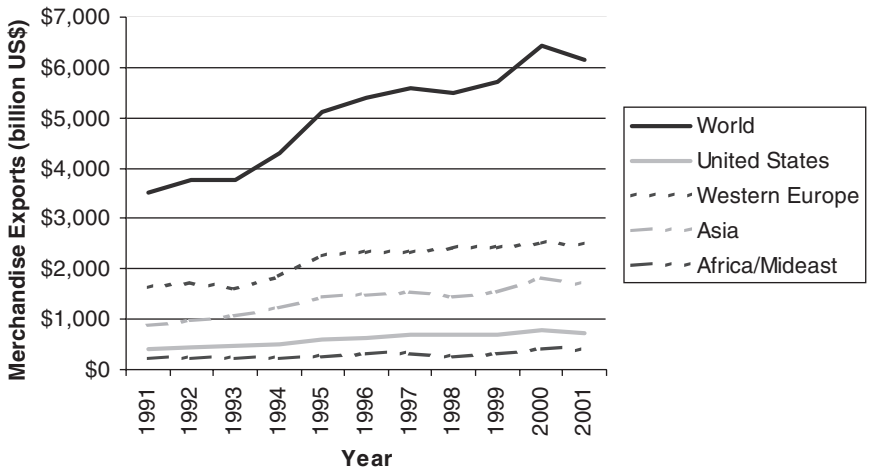


FIGURE 1-2 Merchandise exports by region, 1991–2001. (Source: World Trade Organization.)

The growth in foreign trade is even more striking in comparison with gross domestic product (GDP). Since 1970 U.S. merchandise trade has more than doubled as a proportion of GDP. The world as a whole has also seen healthy increases in this measure (Figure 1-3).

Growing Reliance on Information

Information is obviously a vital contributor to supply chain management. An automobile manufacturer, for example, must assemble all the parts and subassemblies for a run of a particular make and model. In doing so, it must coordinate the production schedules of perhaps hundreds of suppliers to ensure that the correct parts and subassemblies flow toward the final assembly plant as needed. With today's lean inventories, there is little "buffer stock" to make up for a supplier's shortfall and, often, nowhere to store buffer inventories if they existed. To manage its inventories, the company must forecast in real time its production of that model and communicate with all of its suppliers and transportation providers so that they may speed up or slow down their activities. These information flows are critical to industrial operations and profitability, and any threat to their integrity becomes a real concern.

For larger companies, supply chain management is a component of enterprise resource planning models. These models may include transportation as well as human resources, finance, and other core functions. Specialized logistics

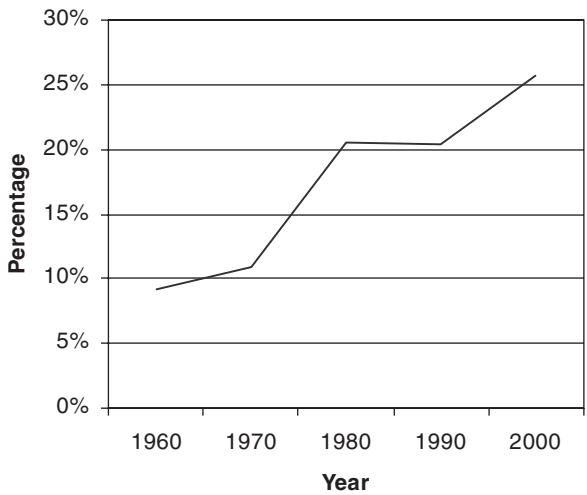


FIGURE 1-3 U.S. trade in goods and services (exports plus imports) as a percentage of GDP, 1960–2000 (Bureau of the Census 2001b).

management companies have proliferated in recent years to serve this need for small and medium-sized companies.

Differences Among Modes

Highway Freight

The nation's highway system is the giant of American transportation, carrying 71 percent of the total tonnage and 80 percent of the total value of U.S. shipments in 1998 (FHWA 2002). More than 550,000 separate trucking establishments carry freight locally, nationally, and internationally, according to the 1997 Economic Census survey of the transportation and warehousing sector. These companies shared total revenue estimated at $342 billion (including local and long-distance trucking and courier services) (Bureau of the Census 2001a).

The companies range from tiny concerns with one or two employees to major national networks with revenues of $2 billion to $3 billion or more (and the biggest of all, UPS, with 2001 revenues of more than $20 billion). In all, their 4.7 million employees were responsible for more than 1 trillion ton-miles of freight movement. Highway freight movement grew robustly in the late 1990s (BTS 2002).

Air Freight

All of America's 100 scheduled airlines carry freight to some extent. Scheduled airlines' revenues for domestic and international freight and express services totaled about $12 billion in 2001, and carriage of mail added another $1 billion. The airlines were responsible for nearly 22 billion revenue ton-miles in 2001. Freight and express specialists were among the few airlines to report consistent profits in recent years.

All of these activities declined substantially between 2000 and 2001, however, reflecting the uncertain security environment and the worldwide economic slump. The decline followed a period of very healthy growth (more than 10 percent per annum for several years).

Rail Freight

Railroad freight revenues in 2001 totaled $35 billion. The nation's railroads were responsible for nearly 1.5 trillion ton-miles of freight traffic. Nearly half of the tonnage (46 percent) was coal, which was followed by chemicals and allied products (8.7 percent), farm products (7.9 percent), nonmetallic minerals (7.0 percent), and food and kindred products (5.6 percent), according to the Association of American Railroads (2003).

The railroad industry is in a long-term process of consolidation. The United States has 571 railroads, but only eight are large (Class I railroads that have corporate revenues exceeding $266.7 million). Statistics for this group show a total employment of 178,000 in 1999. In that year the eight companies shared revenues of just over $32 billion. The Association of American Railroads (2003) reports that the top two (Union Pacific and Burlington Northern) accounted for more than two-thirds of that revenue in 2000 ($23 billion).

Waterborne Freight

The U.S. maritime shipping industry is diverse and complex. It includes a wide variety of vessel types offering many different kinds of service, calling on hundreds of ports on all of the seacoasts and the Great Lakes, as well as transiting inland waterways.

The volume of container freight moving through the nation's ports has doubled in the past decade and is expected to continue growing rapidly (BTS 2002; *The Economist* 1997). More than 15 million containers are in use globally; they account for about 90 percent of the world's internationally traded cargo by value (*The Economist* 2002). Virtually all oceangoing vessels that serve U.S. commerce are operated under foreign flags.

Measured by value, the cargo transported by the international liner shipping industry constitutes about two-thirds of the total U.S. foreign waterborne trade. In 2002, the liner shipping industry carried roughly 6 million containers of imported cargo to the United States and approximately 3.3 million containers of export cargo being shipped from more than 202,000 American businesses. The total is roughly $500 billion worth of goods, or more than $1.3 billion worth of goods per day through U.S. ports (World Shipping Council 2002). Some details on the information technology used by the international liner shipping industry are offered in Appendix A.

Data from DOT's Bureau of Transportation Statistics indicate revenues in 1999 of $24.5 billion for domestic and international freight (coastal waterways, Great Lakes, locks and channels, and inland waterways) (BTS 2002).

REFERENCES

ABBREVIATIONS

BTS Bureau of Transportation Statistics

FHWA Federal Highway Administration

Association of American Railroads. 2003. *Fact About Railroads*. Policy and Economics Department, Jan. 10. www.aar.org/PubCommon/Documents/AboutTheIndustry/Statistics.pdf.

Bureau of the Census. 2001a. *1997 Economic Census: Transportation and Warehousing*. EC97T48S-SM. March. www.census.gov/prod/ec97/97t48-sm.pdf.

Bureau of the Census. 2001b. *Statistical Abstract of the United States*. Washington, D.C.

BTS. 2002. *National Transportation Statistics 2001*. BTS02-06. U.S. Department of Transportation, Washington, D.C. www.bts.gov/publications/nts/index.html.

Chopra, S., and P. Meindl. 2001. *Supply Chain Management: Strategy Planning and Operation*. Prentice Hall, Upper Saddle River, N.J.

The Economist. 1997. Delivering the Goods. Nov. 13. www.economist.com/displayStory.cfm?Story_id=352733.

The Economist. 2002. Container Trade: When Trade and Security Clash. www.economist.com/displaystory.cfm?story_id=1066906.

FHWA. 2002. *The Freight Story: A National Perspective on Enhancing Freight Transportation*. U.S. Department of Transportation, Washington, D.C.

World Shipping Council. 2002. *Partners in America's Trade*. Brochure. Washington, D.C.

Freight Information System Technologies

Most freight transportation information technology (IT) is the same as in other industries. Differences arise because of the nature of the industry and the consequences of terrorist exploitation of potential vulnerabilities, as noted in the Executive Summary. The freight transportation industry uses IT in several ways:

- *Backroom management and integration*. Companies use a range of general-purpose business applications to manage internal processes and to link them by sharing information internally and with suppliers and customers (see, for example, Chopra and Meindl 2001; McDougall 2003; Radding 2000).

- *Mobile communications and tracking*. To keep track of the locations of trailers, trucks, rail cars, and other mobile assets and their contents, companies use everything from bar codes to Global Positioning System (GPS) receivers.

- *Internet applications*. The Internet plays a growing role for all freight companies. Electronic commerce of all kinds uses the Internet because of its wide accessibility and its flexibility in allowing companies to link various kinds of Web, client-server, and legacy systems. These properties make it easier for companies to develop distributed applications that can exchange various types of formatted data (Kiely 1999).

All of these technologies have cybersecurity implications. As companies make their operations more efficient by integrating their systems and those of their customers and suppliers, they also raise cybersecurity concerns. The purpose of this chapter is not to define specific information technologies into or out of the war on cyberterrorism. Rather, it is to provide a basic understanding of the range and

character of possible technology tools that might become valuable in that context. The committee believes that this will help the Department of Homeland Security (DHS) and the Department of Transportation (DOT) in the development of their cybersecurity strategies.

Existing IT Applications

Many kinds of IT are used by the freight transportation industry. The various modes (air, truck, rail, pipeline, and water), to varying degrees, use specialized, sector-specific technologies, but the ultimate goal is to get the shipment from its origin to its destination, which may involve multiple modes. The challenge is to get the shipment to its destination on schedule, with the appropriate degree of tracking en route; to minimize delays in transferring from mode to mode; and to do all of this at a competitive price without damage to the product shipped.

For most companies, transportation is a strategic asset. Large companies today are likely to have sophisticated models of their operations, known as enterprise resource planning (ERP) systems. ERP systems may include scheduling modules for manufacturing plants, which would allow the company to automate major portions of the decision processes in transportation or other aspects of the value chain for that plant. The use of such modules (in finance, logistics, manufacturing, human resources, or supplier management) helps the company improve the way it does business by increasing efficiency and reducing human error.

Freight transportation planning and operation decisions are often assisted by software that is designed to help analyze and determine how, where, when, and in what quantity materials should be transported. These systems also compare different carriers, modes, routes, and freight plans; include supply chain management software; and rely on sophisticated algorithms to analyze options and generate solutions that increase profitability. These applications can respond in real time to problems and emergencies—for example, by instantly rescheduling if a machine breaks down.

For any mode, freight operations can generally be categorized into the following tasks, each of which can be assisted or improved by the use of IT:

- *Matching a load with a carrier*. The cargo owner, or shipper, must identify and engage a carrier—truck, train, ship, air, or a combination of modes. Freight brokers, agents, and freight forwarders may be involved in this task. The technology involved can span the range from telephone and fax on the low end to Internet-based load bidding. If a multimodal shipment is involved,

the shipper or broker (agent) will either have to arrange each leg of the trip or request a carrier to arrange the entire intermodal movement.

- *Order acceptance*. It is necessary to establish a dated record of the carrier to which the load is assigned. This record is typically called a bill of lading (airbill or waybill). It is a statement of the nature and value of goods being transported and the conditions and terms applying to their transport. It serves as or evidences a contract of transport between the owner of the goods and the carrier. It may be paper, or it may take various electronic forms.

- *Routing/dispatching*. Choosing a course and directing the vehicle to its destination can be a matter of strictly human effort (for a simple truck trip) or it can be automated to nearly any extent desired.

- *Pickup confirmation, en route tracking, and delivery confirmation*. Shippers and freight companies often desire to track the progress of their shipments. A variety of processes and technologies—depending on the transportation modes—can be used for this purpose, including GPS satellites, digital or analog wireless telephones, and bar code scanning. Some carriers use all of these devices, so customers may monitor the locations of their shipments in near real time by using the Internet.

- *Transmitting shipping documentation*. Paper documents are traditional here, but many carriers use electronic communications [e.g., the Internet and electronic data interchange (EDI)].

- *Cargo manifesting*. This step often uses special information software and systems.

The various transportation modes use different technologies, which reflect their recent histories. All, however, are moving toward greater computer-assisted systems and reliance on communication, frequently using EDI and the Internet. Yet they have far to go before truly intermodal transportation communications are possible.

Highway Freight

The trucking industry is a component in nearly every company's supply chain. Trucking companies use computing and communications technologies heavily

to improve their own efficiency and to meet the demands of their customers for cost-effective, efficient, and easily tracked logistics. The proliferation of small trucking companies over the past 20 years has been built on the use of low-cost IT such as mobile phones, fax machines, and the Internet.

Trucking companies and freight brokers increasingly use the Internet to match loads with the most appropriate carriers. Both independent brokers and some larger truck freight companies have websites on which drivers can bid for loads or use EDI, which is also commonly used by railroads and waterborne freight companies. Phone and fax, of course, are still vital, especially for the tens of thousands of smaller firms (i.e., those with fewer than 10 trucks).

To document the agreement to carry a shipment, many shippers use electronic means [such as the well-established EDI or the emerging and more flexible Extensible Markup Language (XML)], but smaller shippers use paper records.

Except for extremely time-sensitive operations, such as sophisticated logistics systems serving just-in-time manufacturing operations, the driver or human dispatcher is responsible for routing and dispatching the truck. The technology is available for automating these operations to nearly any extent desired (including special software for generating maps and trip schedules).

For confirming the pickup, en route tracking, and delivery confirmation, truckers use a variety of technologies, including GPS (satellites), digital or analog wireless telephones, and bar code scanning. New electronic automatic vehicle identification systems, much like those used in the electronic collection of tolls on highways, are used increasingly in busy ports and other intermodal transfer points. Some carriers use all of these devices, so customers may monitor the locations of their shipments in near real time by using the Internet.

In transmitting shipping documentation, paper documents are the norm, but some carriers use digital communications such as EDI.

Air Freight

The rapid growth of air freight in the past decade was made possible by advances in communications as much as anything else. Coordinating the worldwide movement of time-sensitive freight, from business documents to garments to fresh flowers, is a challenging and complex task.

Air cargo companies gain their competitive edge from technology innovation. They pioneered the generation and use of large databases that can be queried at will to monitor each of the millions of items that a large air freight company may have in transit at any moment. A vital part of the problem is to ensure that intermodal communication is efficient (Air Transport Association 2002).

Rail Freight

Rail freight is increasingly supported by information systems and communications technologies. Typical trains a decade or so ago had a crew of four, compared with two today. Rail companies have made growing use of onboard computers, local area networks, automated equipment identifiers, GPS tracking, automatic reporting of work orders to headquarters, car scheduling and train order systems, and two-way wireless connections (Association of American Railroads 2003).

Signaling and monitoring systems are also more automated, taking advantage of commercial fiber-optic communications cable that has been laid along rights-of-way. The rails themselves are used as communications channels for signal controllers and trackside signals. Wayside "hotbox" detectors take infrared readings on the bearing boxes of passing rail cars and automatically report overheated journals over VHF voice networks. In arranging transfers to and from other modes, railroads have long used EDI.

To help track shipments, nearly all locomotives and rail cars are tagged with automatic identification transponders, which automatically record car locations. This technique allows automatic verification of the standing order of cars in each train and faster, more accurate reporting of car locations to railroad service centers and customers.

Waterborne Freight

Waterborne freight has many of the same information needs as other modes. The carrier must identify cargo, make intermodal handoffs efficiently, and get the cargo to the agreed destination as quickly and securely as possible. The types and sizes of typical cargo (mainly containerized freight, petroleum and other fluids, motor vehicles, and various bulk cargo) are somewhat different from those of other modes, but the types of information needed are essentially the same.

The focus of the remainder of this section is on the international liner shipping industry (that is, ocean carriers that offer scheduled services on fixed routes), since this type of shipping activity involves the greatest need to manage information and communicate with others. Further detail can be found in Appendix A.

Business Data Systems

The heart of a company's information and communication processes is usually a legacy mainframe computer system, which is generally accessible over the Internet (with various levels of access to users inside and outside the company). Access is secured by passwords or a virtual private network with different levels of security

for, and access to, the centralized mainframe systems. Many global carriers also have company intranets.

Central Dispatch/Redirection

Central to liner shipping companies' activities in this area is keeping track of containers and truck chassis. Shippers (cargo owners) must arrange with the line for the specific types and numbers of containers needed, the pickup date, and which vessel is to carry the containers. To do this, the shipper either directly contacts the line's booking agent or enters the necessary information (including origin, destination, port of loading, commodity description, shipper's name, and type of container) using the appropriate transaction section of the line's website. In either case, the information goes into the company's mainframe system and becomes available to dispatchers of containers and to vessel operators and terminal operators, who make the necessary preparations for the movement, loading, and stowage of containers on the vessel and for the availability of needed equipment. At the destination port, the terminal operations staff—also working from the company's mainframe system—will access information needed for off-loading the containers and handing them off for the next leg of the journey.

Information Flow Among Collaborators

Multiline alliances and other vessel-sharing arrangements are central to liner shipping. Because a vessel may carry the cargo of various container lines, it is necessary to exchange significant amounts of information among alliance members. Most of this information exchange is handled via EDI, which in turn requires that each alliance partner's information system be programmed to accept data from the other partners' systems.

They also must share information with truckers and rail carriers to ensure efficient intermodal transfers. The EDI protocol or Web tools, or both, are generally used with "house" truckers or railroads; with smaller trucking companies, the transactions are handled by fax or e-mail.

Information Flow to Governments

The freight industry has innumerable electronic links, mandated or voluntary, with local, state, and federal agencies. These include manifest filings, operating authorities and permits (e.g., permits to carry hazardous materials), route filings, electronic funds transfers, and personnel files, to name a few. For example, ocean carriers must post information on imported cargo with the Automated Manifest System (AMS) of DHS's Bureau of Customs and Border Protection (formerly

U.S. Customs Service). The Customs databases and systems are discussed in more detail in Appendix D. Customs recently promulgated the so-called 24-hour rule (see Box 2-1), which requires that advance cargo declarations be submitted 24 hours before loading of U.S.-bound cargoes in foreign ports. AMS and the Customs' Automated Targeting System are becoming the preeminent centralized government data management system for security prescreening of import cargoes to the United States. In addition, many ocean carriers and shippers are participating in Customs' Automated Export System for electronic submission of

Box 2-1

New Cargo Security Regulations from Customs and Border Protection

The U.S. Bureau of Customs and Border Protection in late 2002 issued the so-called "24-hour rule," which requires ocean carriers to submit advance cargo declarations (CF 1302) 24 hours before loading U.S.-bound cargo in foreign ports. Under this rule, Custom's Automated Manifest System (AMS) is becoming the main federal data management system for security screening of waterborne imports.

The carrier sends data on inbound cargo to Customs via AMS, and Customs makes the appropriate checks using AMS and its Automated Targeting System, according to an established list of risk factors. Customs can thereby determine whether a container should be held pending further investigation at the foreign port and whether containers should be physically inspected. Containers for which no hold has been issued can be loaded 24 hours after submission of the data.

Section 343 of the recent Trade Act of 2002 (P.L. 107-210) requires that information on all imports and exports be submitted electronically to Customs. Customs will promulgate final regulations under the act by October 1, 2003. It is expected that more foreign jurisdictions will require electronic submission of cargo manifest information in the future.

export cargo information; other ocean carriers provide that information today in paper (fax) form. The Advanced Passenger Information System, which has been used by airlines since 1986 to report airline passengers, has now become mandatory for other modes, under the Enhanced Border Security Act of 2002. It will soon require mandatory advance electronic crew member information from vessels. As with information technology in other applications, the use of systems and databases in public–private partnerships is subject to the cybersecurity implications previously mentioned in this chapter.

Information Flow Between Carriers and Customers

Estimates in the trade press suggest that about 75 percent of shippers' transactions with ocean carriers are handled by telephone or fax, 20 percent through individual carriers' websites, and 5 percent via the three Web-based portals (e.g., GT Nexus, Inttra, and CargoSmart) that provide access to multiple carriers at one site. In electronic transactions between ocean carriers and their customers, user registration and assignment of passwords is a common security measure. Encryption of data is primarily used in situations in which the parties are passing data related to title to goods, as, for example, with remote printing of bills of lading. Some companies in the liner shipping industry are moving to customer relationship management software, which allows them to more flexibly manage customer transactions through a simpler linking of all the company's individual business systems. Customers can obtain information on the status of particular cargo movements from the ocean carrier's customer service department or track the cargo's position in a secure section of the carrier's website using coded information from the bill of lading.

IT Trends and Emerging Technologies

A variety of approaches using new technologies may be linked to IT systems in the future. Some are intended to improve cybersecurity. Others would be implemented for efficiency reasons but may have secondary implications, positive or negative, for IT vulnerability. The topics discussed are still developmental, and there is no assurance that they will be (*a*) appropriate for freight transportation security or (*b*) available at an acceptable cost. The technologies discussed here are intended as examples of technology that the full study should consider. Determining which are likely to be widely implemented was beyond the scope of this study.

Electronic Supply Chain Manifest Demonstration

DOT, working with freight shippers, has tested a variety of ways to improve intermodal transfers of freight under the Intelligent Transportation Systems program. For example, at O'Hare International Airport, the Electronic Supply Chain Manifest system was tested in a 2-year demonstration that focused on the air–truck interface, but it is being considered for other modes as well.

Freight Information Real-Time System for Transport

The Freight Information Real-Time System for Transport (FIRST), being developed by the Port Authority of New York and New Jersey (https://www.firstnynj.com/), is an Internet-based system for trucking companies, railroads, terminal operators, ocean carriers, brokers/freight forwarders, and others to use in speeding the flow of cargo through the area (one of the busiest and most congested in the country). It allows cargo brokers, shipping agents, freight forwarders, and steamship companies, as well as trucking companies and railroads, to check the status of cargo and vessel arrivals, arrange pickups, and confirm deliveries. The FIRST website includes alerts of bridge and tunnel problems and traffic congestion (and Webcams of the busiest container terminals).

FIRST consolidates in one place on the Web various existing sources of critical cargo transfer and carrier information (including near real-time information on truck, ship, and train arrivals), real-time video feeds to monitor congestion at seaport entry gates and road conditions on arterial roads leading to the port, and enhanced intermodal connectivity by improving the in-transit visibility of cargo.

Interconnections of Systems Across Large Sectors

The interconnection of systems across the freight transportation sector, properly implemented, significantly increases the ability of participants to communicate effectively and efficiently by reducing mundane tasks and increasing accuracy. Various forces are currently driving the interconnection of information systems across the entire transportation sector. Economic forces, among other considerations, are causing large organizations in the transportation sector to interconnect their own systems to create enterprise-spanning systems. For example, all of the large overseas shippers now have interconnected systems that are used to control most aspects of the shipping process within their organizations. The systems have many of the same characteristics as those developed by FedEx to handle all of its various operations, including overnight, freight, and custom

deliveries. Furthermore, customers are being granted electronic access to those systems to gain "visibility" of shipments, which allows the customers to make their own operations more efficient.

As some large organizations develop interconnected systems for their own purposes, they also provide the resulting computer-assisted services to a larger number of smaller organizations who otherwise would not have their own systems. For example, the system used by Union Pacific to control its networkwide operations is also used by many short-line carriers to control local and regional operations. Such sharing of information systems helps large and small operators alike to increase efficiency, reduce overall costs, and amortize investments in IT.

Smaller operators also are interconnecting their existing systems to create "federated" or "cooperative" systems that allow them to compete more effectively with larger organizations. For example, four regional trucking carriers have formed the ExpressLink system to interconnect their own corporate-level systems. ExpressLink gives each carrier national coverage while allowing it to maintain a relatively small infrastructure.

In addition, policy and regulatory forces are driving the interconnection of governmental systems and the interconnection of commercial and governmental systems. The Bureau of Customs and Border Protection has several new IT systems (described in Appendix D) under development that—once they become operational—could serve more government agencies than originally envisaged as a result of homeland security initiatives and requirements. In many respects, the interconnection of government systems parallels the interconnection of commercial systems because regulatory agencies must streamline their operations to keep pace with increased efficiencies provided by commercial systems.

Regulatory forces are also driving the interconnection of commercial and government systems by requiring more information to be submitted electronically to the government by carriers, shippers, and manufacturers. For example, effective December 2002, Customs has been requiring the submission of sea cargo manifests 24 hours before loading of export cargoes destined for the United States (see Box 2-1). Customs, acting under statutory authority, is poised to propose that all sea cargo manifests be electronically submitted for both import and export cargo. Customs is likely to propose that similar electronic submission requirements for cargo descriptions be implemented for the other transportation modes.

Many of the economic, business, policy, and regulatory forces described above have existed for quite some time, although the pace of development in many of these areas has quickened as a result of homeland security initiatives.

Accordingly, pilot programs have been started or are being planned in various sectors to gain practical experience with various existing and emerging technological and procedural applications and processes before decisions are made on their adoption. Pilot programs (see Appendices B and C) such as Operation Safe Commerce, Sim-Tag, Cargo Handling Cooperative Program, and Smart and Secure Trade Lanes involve the testing of, and comparison between, different monitoring and identification systems of shipments as well as the handling of those shipments through the intermodal transportation chain. Each pilot program is intended to provide insights that may be relevant to determining future economic, policy, and regulatory priorities and requirements.

For all of the reasons stated above, the interconnection of information systems across large transportation sectors is likely to develop further. Transport carriers, shippers, and manufacturers will likely find economic value in increasing the efficiency of their operations by development and deployment of multifunctional and multifirm intelligent management systems. Similarly, government systems and the interconnection of commercial and government systems are likely to be used increasingly in satisfying complex policy and regulatory requirements. However, as the web of interconnected information systems increases to fulfill these requirements, it is likely to become more susceptible to unauthorized access, improper use, and denial-of-service attacks.[1] That is, the natural solution for the current set of economic and regulatory problems could become the cause of a host of cybersecurity problems if it is not implemented properly (CSTB 2002a).

Various architectural and technical mechanisms can be used to maintain security across interconnected systems, such as firewalls and different access control levels. However, regardless of the specific mechanism, they all essentially rely on authentication, the identification of every person or computer that accesses the system. The stronger the mechanism of identification, the stronger the overall security of the system. For example, most stand-alone and interconnected systems, including PCs, departmental servers, mainframes, and enterprise-spanning Web-based services, rely on a simple username and password combination to identify each person who should be allowed to access the system. Although many techniques have been developed to "increase the security" of the simple password

[1] This theme was reflected in "Continued Review of the Tax Systems Modernization of the Internal Revenue Service" (CSTB 1994) with the strong condemnation of the extremely weak security architecture, which had 55,000 members able to access a taxpayer's file over unsecured circuits using only a fixed password.

scheme (e.g., stamping additional numbers on the back of credit cards or requiring at least six characters in a password), most security experts agree that passwords are a weak authentication mechanism because it is relatively easy for an intruder to acquire such information. In an interconnected system, the potential problems caused by weak authentication mechanisms are amplified significantly because of the increased number of entry points into the system. Furthermore, access to one part of the system could lead to access to other parts of the system, if not to the entire system. As important as the authentication of individuals in an interconnected system is the authentication of every system that accesses another system.

The importance of credible authentication in interconnected systems has been well known for more than 20 years. Moreover, various competing theories and technologies have evolved over that time to address these concerns, primarily through the use of cryptographic techniques that rely on mathematical approaches to ensure that the authentication information cannot be stolen or forged (CSTB 1996). Credible authentication is based on a set of "digital certificates" (i.e., credentials) that have been "digitally signed" (i.e., authenticated) by a "trusted entity."[2]

The use of digital certificates and signatures went a long way toward solving the wide-scale software authentication problem. Support for digital certificates, which were first developed in a widespread manner in the mid-1990s with the Netscape Web browser, has since been added to most e-mail software for the authentication and encryption of e-mail, although it is not yet widely used. Digital certificates and signatures are often used in conjunction with hardware devices such as smart cards and smart tokens to further strengthen the authentication scheme used by a system.

Embedded Processors and Enabling Technologies

Historically, the primary interface between the real world and the cyberworld has been a human being: someone interprets real-world activities and enters data into the computer system, or someone is provided tasking by the computer and performs a real-world chore. Embedded processors transfer information directly between the real world and the cyberworld. They are already used in the transportation sector, primarily for the monitoring and identification of shipments, and

[2] Having a single "trusted entity" is only one approach. The study that is outlined should look at alternative approaches such as having multiple roots [e.g., SDSI/SPKI (simple distributed security infrastructure/simple public key infrastructure)] and other benefits of digital signatures such as the protection of certificate integrity.

that use could grow. Radio frequency identification (RFID) tags, e-sensors, and e-seals, together with their electronic readers at all relevant points, are examples of embedded processors.

RFID tags are used to provide an automated means of identifying an asset or its declared contents, or both. These tags can be either active or passive. Active RFID uses an internal power source (e.g., battery) within the tag to continuously power the tag and its RF communication circuitry, whereas passive RFID relies on RF energy transferred from the reader to the tag to power the tag. Passive RFID operation requires strong signals from the reader, and the signal strength returned from the tag is low because of the limited energy. As with any RFID system, one of the vulnerabilities to cyberattack occurs at the point where the tag communicates with the reader. The simplicity of passive RFID tags makes them relatively easy to "spoof." Active RFID systems, on the other hand, can include authentication and encryption techniques similar to those of any computer network. Some of their cybersecurity challenges are therefore similar to those of other IT systems, as discussed above.

E-sensors make use of embedded processors to detect and document environmental characteristics or changes to a shipment along its route. For example, temperature sensors can be used on refrigerated containers to detect whether the internal temperature was maintained within proper limits over the entire route. Certain types of sensors have been used for some time in various applications in the transportation sector but are now, to some degree, being integrated with embedded processors. For example, a temperature e-sensor can record the actual temperature of the shipment over the entire route, and the temperature data can be stored in a tamper-indicative manner by using a variety of hardware and software techniques. E-sensors also can be configured to document container intrusions.

Seals, whether electronic or mechanical, are placed on shipments or structures to detect an unauthorized entry (thereby alerting officials to the need for further inspections) or deter intrusions because of the fear of detection. They can be designed for different applications. For example, e-seals on a container door might store information about the container, the declaration of its contents, and its intended route through the system. E-seals can document when the seal was opened. In combination with digital certificates and signatures, an e-seal also could document whether the individuals sealing and unsealing the container were authorized.

While these technologies are intended to enable monitoring of shipments and physical security, they all use IT and are linked to IT systems. Thus the additional

connection points (e.g., electronic readers) may increase cybervulnerability. A full assessment of the potential cybersecurity vulnerabilities that would be created through the widespread adoption of these technologies in the freight transportation industry is needed (see Task 1 in Chapter 3), perhaps as part of the larger study that is the focus of this report.

In addition to the embedded devices described above, enabling technologies, including public-key cryptography, biometrics, and wireless communication tracking, are of potential use in the transportation sector's IT infrastructure and are relevant from a cybersecurity perspective.

Cryptography has been used across a range of application areas for more than 25 years to ensure that information is exchanged privately between two entities over a network. Cryptography is the basis for most "secure" Web-based activities and "secure" e-mail applications, and it is supported by all major software applications. The need for strong cryptographic techniques in electronic commerce has led to its widespread availability beyond traditional military applications.

Biometric devices are used to authenticate human beings on the basis of one or more physical attributes such as a retina or iris pattern, a fingerprint, digital face recognition, or voice pattern. As such, this limits access to a specific person, not just to someone who knows certain information (i.e., a password) or holds certain credentials (e.g., a digital certificate). Biometric devices can be used in conjunction with a smart card (or smart token) and a digital certificate to improve authentication. [The report *Who Goes There? Authentication Technologies and Their Privacy Implications* (CSTB 2003b) has a more in-depth discussion of biometrics as an authentication technology, commonsense rules for the uses of biometrics, and potential privacy and other social implications of their use.]

Wireless communication tracking systems are used in the domestic transportation sector to monitor the location of shipments along their route. In some cases, the shipment reports its location using wireless communication to a control system, while in other cases the shipment simply records its location along its route, and those data are gathered at a control point.

It will be important to closely monitor ongoing and planned pilot programs (e.g., Operation Safe Commerce and Smart and Secure Trade Lanes) intended to test these technologies to determine what role, if any, they might have in enhancing supply chain security. Standardization efforts of various national and international organizations and institutions (e.g., the Auto-ID Center at the

Massachusetts Institute of Technology and the International Organization for Standardization) and the degree to which such efforts would address recognized cybersecurity vulnerabilities of the technologies and their possible commercial deployment are also worth monitoring.

Electronic Data Interchange

Proper paperwork, including the bill of lading, work order, and letters of credit, is essential to the movement of shipments. The electronic exchange of documents required throughout the shipping process is becoming more and more common. Mature EDI standards exist for the transportation sector, and operational systems are already in use by large and small organizations within the sector.

The first electronic documents to be exchanged were those directly related to money, such as purchase orders, work orders, invoices, and payments. For example, 96 percent of all invoices generated by Union Pacific are exchanged electronically. The electronic exchange of other documents in the shipping process is increasing, to the extent that no paper document is ever generated in some cases. For example, 80 percent of all FedEx orders are placed electronically over the Internet, and corresponding electronic invoices and credit-card receipts are sent to the consumer.

Historically, the validity of a shipping document was verified by human beings along the route who physically examined the document itself and any attached seal. Some fraudulent or forged documents would routinely be detected, but some would not. In general, the system was designed to limit the number of improper documents to an acceptable level across the entire transportation sector. The steady move toward electronic documents, however, could significantly alter that delicate balance because electronic documents are easily reproduced, altered, or forged if they are not implemented properly. More important, it is practically impossible for a human being to detect such a forgery, let alone monitor the rapidly increasing number of documents being exchanged.

The use of a cryptographically generated signature on a sensitive document that is exchanged between two information systems helps ensure the authenticity of the document author and that it can be exchanged privately with another party. As discussed above, such technology has been used extensively in many application areas and is widely available. An effective digital signature would reduce the vulnerability of a document to tampering and fraudulent use.

The transportation sector in general and system developers in particular have not to any large degree incorporated digital signatures into emerging systems

and standards. To date, forgeries in the freight transportation industry have had few implications beyond finance. If weapons of mass destruction were to be smuggled, however, forgery might be an integral part of the deception. The study that is outlined here should analyze the use of digital signatures on electronic documents and determine whether steps could be taken to encourage more widespread use.

In many cases, the worst cybersecurity problems result from the first wave of productivity enhancements gained by computer-assisted systems. That is, when computerized systems are first deployed to increase productivity, they naturally cause a change in the business processes and procedures followed by human beings to do their job. If the consequences of those human-oriented changes are not considered by the system designers, a wrongdoer could take advantage of those changes and cause more difficult problems than were possible before (CSTB 2003a, 80–81). Similarly, equipping electronic documents with digital signatures based on strong cryptography might create an environment in which the electronic documents would replace paper-based documents, thus possibly altering normal business processes and procedures.

The productivity enhancements provided by electronic documents come at a price. Widespread use of electronic documents would require development of an electronic infrastructure to support the authentication of individuals and organizations, document standards across a range of transportation sectors, and a set of auditing processes to ensure that the system is working properly. Such infrastructure elements are being developed across a wide range of business sectors and are starting to evolve in the transportation sector. The study that is outlined here should consider the value of pilot programs to identify the various issues and challenges surrounding the creation of such an electronic infrastructure throughout the transportation sector.

As in the deployment of any technology, the deployment of EDI could result in new or additional vulnerabilities and consequences. They could result from alteration of existing business practices (e.g., the involvement of one less person in a check-and-validation process) and the development of infrastructure elements across various business sectors (e.g., two incompatible systems are "united" by a third "mediating" system), among other causes.

Increased Reliance on the Internet for Communication

Economic forces are pushing most systems toward Internet communications as the result of widespread, near-universal access. Consumer-oriented carriers handle a significant portion of their business over the Internet, keeping pace with

the general push toward online commerce in all sectors. Similarly, business-to-business carriers are also starting to use the Internet for a significant portion of their transactions.

With the increased use of the Internet has come an increased awareness of the need for secure communications and stronger authentication techniques in most information systems, especially those using the Internet. Hardware-based authentication tokens, which are issued to users who need to access a system over the Internet or by use of some other remote access technology, either replace or augment a conventional password system to strengthen the remote authentication process. For example, FedEx uses 20,000 tokens to provide system access at various levels to remote users. Virtual private network (VPN) technology has been developed to provide extra levels of security for remote user-to-system and system-to-system communication over the Internet. VPN technology creates a virtual network on top of the Internet that allows access only to a specified set of users and systems. The VPN technology has well-established hardware and software standards. VPN works for prearranged situations involving a small number of systems.

One of the challenges still facing Internet developers is that of availability. As the Internet is increasingly used as the primary communication method between transportation systems, the ability to transmit data reliably across the Internet becomes more critical. Internet availability is a double-edged sword. On one hand, the Internet is vast, with many redundant paths between all points—local and even regional breakdowns in one part of the Internet are healed relatively quickly by rerouting traffic around the problem areas (CSTB 2002b, 2). On the other hand, key resources on the Internet depend on standard software components that are under continuous attack from a variety of sources constantly looking for ways to make them fail. For example, attacks on the Domain Name Service and Sendmail servers have demonstrated the susceptibility of these widespread components.

As stated previously, the most difficult security aspect of any large networked system such as the Internet is that the attacks can come from virtually anywhere in a nearly anonymous manner (using current authentication methods). Denial-of-service attacks have been conducted for a long period of time by a wide range of people located around the world. More important, such attacks are inherently difficult to prevent, and it is difficult to track down the perpetrators. Owners of key transportation systems that use the Internet for communication purposes should be aware of the risk of such attacks. Protective measures are often used as a normal part of the business process.

Emergence of Decentralized Systems

Since the introduction of Web-based application techniques in the early 1990s, decentralized information systems have emerged as an alternative system architecture to the prevalent centralized systems. That is, instead of having a small number of servers that provide services to a large number of users (the centralized approach), systems are now designed with a larger number of servers that communicate directly with each other to provide services (the decentralized approach). Decentralized systems have an inherent ability to work around local and regional network outages, communicating whenever possible, but otherwise not preventing local users from continuing to work. Early applications such as Napster allowed music files to be exchanged between peer systems, while mainstream software applications such as Groove allow peer-to-peer processing of typical business documents. The security implications of decentralized systems include the lack of a centralized "authority" to authenticate that all the users and computers in the system are who they purport to be.

References

Abbreviation

CSTB Computer Science and Telecommunications Board

Air Transport Association. 2002. *Annual Report*. Washington, D.C.

Association of American Railroads. 2003. *Facts About Railroads*. Policy and Economics Department, Jan. 10. www.aar.org/PubCommon/Documents/AboutTheIndustry/Statistics.pdf.

Chopra, S., and P. Meindl. 2001. *Supply Chain Management: Strategy Planning and Operation*. Prentice Hall, Upper Saddle River, N.J.

CSTB. 1994. Continued Review of the Tax Systems Modernization of the Internal Revenue Service. National Research Council, Washington, D.C. www.cstb.org/pub_irscontinuedreview.html.

CSTB. 1996. *Cryptography's Role in Securing the Information Society*. National Academies Press, Washington, D.C.

CSTB. 2002a. *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*. National Academies Press, Washington, D.C.

CSTB. 2002b. *The Internet Under Crisis Conditions: Learning from September 11*. National Academies Press, Washington, D.C.

CSTB. 2003a. *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities*. National Academies Press, Washington, D.C.

CSTB. 2003b. *Who Goes There? Authentication Technologies and Their Privacy Implications*. National Academies Press, Washington, D.C.

Kiely, D. 1999. XML: More Than Just a Quick Fix, Extensible Markup Language Is Seen as a Universal Object Model That Will Enhance Web Development and Simplify Application Integration. *Information Week,* Feb. 8.

McDougall, P. 2003. Nissan's I.T. Road Map: Integration and Security Top Automaker's Project List. *Information Week,* Feb. 10.

Radding, A. 2000. A New Approach to Integration: E-Commerce Requires Companies to Integrate Processes at Many Levels with Multiple Partners. *Information Week,* Aug. 28.

Planning a Full Study

As discussed in previous chapters, the freight transportation industry's information systems may be vulnerable to cyberattacks. The consequences of a cyberattack could be serious, both economically and physically. Further study is needed to identify specific vulnerabilities and risks and develop possible strategies to address those vulnerabilities while minimizing the costs of doing so. Such studies are warranted for the following reasons:

- Information technology (IT) is becoming increasingly central to freight transportation.
- With all IT come cybersecurity issues that should be carefully considered, in particular in the post–September 11 environment.
- Addressing cybersecurity issues presents the same conundrum as other security issues: a trade-off between risk reduction and the costs of implementation.
- No mechanism exists for determining analytically how far to go in reducing vulnerability or which steps should have the highest priorities.
- Not enough is yet known about cybersecurity as related to freight IT or the impact of potential measures to enhance security.

Therefore, the committee concludes that a need exists for a comprehensive study to assess the current challenges in cybersecurity in freight transportation information systems and to identify possible strategies to mitigate identified vulnerabilities. Such strategies must account for the company composition and structure in each mode, the operations the companies perform, and the information systems they use. They must be based on an analysis of security gaps, the

advantages and disadvantages of current and emerging technology and processes that could be implemented to enhance cybersecurity, and the ability of transport companies to implement them. The analysis that would permit such strategies to be developed has not been conducted. The committee discusses some elements of the required analysis below.

Assessing Security Issues

It is generally understood that achieving cybersecurity requires a two-step risk assessment. First, an analysis must be performed to identify overall system vulnerabilities, the threats that might exploit those vulnerabilities, and the consequences if the threats were indeed carried out. Figure 3-1 illustrates the interrelationship of these factors. Second, a risk management analysis must be conducted to evaluate possible measures to enhance cybersecurity, their costs, and their benefits. As discussed in Chapter 2, the nature of the coordinated information system that serves the nation's freight transportation system makes this risk analysis extraordinarily difficult compared with other computer security assessments. Nonetheless, this analysis of the overall interconnected system, as well as the individual subsystems, could be an important factor in reducing vulnerability to terrorist attacks.

Actions to mitigate threats should depend on the specific threats considered plausible, the natures of the systems involved, and their owners. For example, a broad denial-of-service attack on the Bureau of Customs and Border Protection's Automated Manifest System could shut down this necessary interaction point for all international shipments into the United States (see Appendix D).

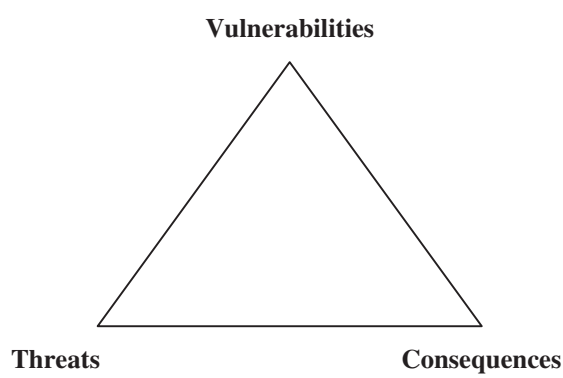


FIGURE 3-1 Factors involved in cybersecurity assessments.

Without this system, international transportation activities could grind to a halt, with significant economic consequences for U.S. manufacturers and businesses and, ultimately, the U.S. economy. The U.S. government is responsible for countering such threats. Alternatively, a disabling attack on the dispatch system of a large carrier could bring that operation to a halt (and, correspondingly, all transportation activities linked to it). When potential targets are individually owned and operated systems, the design and implementation of the solution move to the companies that own these systems.

Diversity characterizes the freight transportation sector. Achieving information system security demands a certain continuity of system design, implementation, and security procedures that does not readily permit the flexibility that might be desirable in accommodating such a diverse range of participants. As a result, careful identification of possible measures is required.

The choice of measures to counter cyberterrorism must consider economic as well as security issues. Ignoring cost could have serious economic consequences, handing terrorists one of their stated objectives. It is difficult to estimate economic impacts across a broad sector such as freight transportation. Nonetheless, it must be recognized that this sector operates on tight profit margins. Implementation of cybersecurity measures is unlikely to be optimal unless economic benefits accompany the security solutions. Figure 3-2 provides a visualization of the overlap between measures to improve security and measures to improve economic performance; some security initiatives may improve economic performance, and others may not. Prioritization of possible measures for a diverse consortium of participants must be sensitive to this point as a specific aspect of the risk management analysis. Another example of the tension between the diversity of the community and the continuity required for cybersecurity concerns evaluation of cybersecurity capabilities. Important questions must be addressed, including who would perform the monitoring role, how it would be accomplished (for example, whether penetration tests would be conducted), how frequently evaluations would occur, and how they would be reported.

In view of these points, the process of evaluating possible measures and eventually selecting some for implementation must be an integrated effort that is based on a risk prioritization methodology and a cost–benefit methodology that are shared and understood by all affected members of the freight transportation community. The prioritization methodology should account for the consequences of potential attacks; the availability, efficacy, and cost of possible measures; their side benefits; and the distribution of costs and benefits to community members and the nation as a whole. At present, no such methodology is in use or under

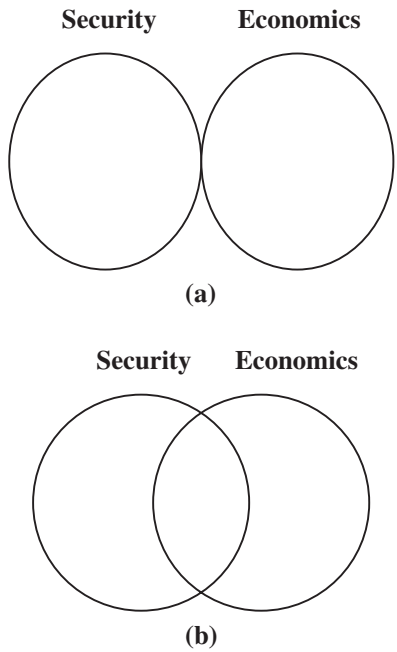


FIGURE 3-2 Relationship between security and economic benefits: (*a*) little or no economic benefit to security enhancements; (*b*) significant economic benefit to security enhancements.

development. In addition, no single organization has a mandate to develop and manage the use of such a methodology. This report provides a set of recommendations that, if followed, would be the start of a process for selecting, implementing, and managing measures for countering potential terrorist cyberattacks.

The study suggested here is intended to provide a strategy for approaching these issues. It might be necessary to involve several entities in the conduct of the study. The National Academies could do some of the work, but this is not a proposal for an Academies study. Industry consultants might collect data. One or more federally funded research and development centers could do the detailed analysis. Various academic research programs also could be involved.

In all these tasks, it will be necessary to impose strict conditions on the information collected and on the way it is processed. Not only is company confidentiality a major concern, but so is the possibility that the information might

be compromised by the terrorists that the study is intended to combat. Also, for all these tasks, it will be important to study not only private freight information systems, but also those government information systems that interface with the freight transportation sector (e.g., the various information systems operated by Customs and Border Protection).

Study Plan

Task 1. Determine the chief vulnerabilities of freight transportation information systems. No complete system description exists of the use of IT in the transportation sector. The first step of this task is to identify at least the major components that can affect cybersecurity and their interconnections. Part of this task would be to understand the role that these IT components play in normal operations so that the consequences of their loss to cyberattacks can be understood. Information on backup systems should also be sought.

This information might be obtained with a survey (if consistent with current administration requirements) and then a series of interviews. A variety of companies in each mode must cooperate to ensure adequate coverage and mask company-specific data. In many cases, the information will be already available. It will not be necessary to have great detail as to which company uses which technology. Rather, information concerning the general prevalence of different types of systems in each mode and their interconnections is desired.

Then the systems—and the intermodal, interconnected system—can be examined for vulnerabilities and the potential consequences if those vulnerabilities should be exploited. Much of this work would reflect generic IT vulnerability studies, but the specific use of the technologies in the freight industry would have to be reviewed. A variety of plausible attack scenarios would then be tested on the different modes to assess the systems as they exist now and as they are evolving in order to understand the likelihood of success and the extent of the consequences. The purpose would be to develop a preliminary list of the vulnerabilities that should be considered in the tasks below. As shown in Figure 3-1, priority should be a function of the plausibility of the type of threat that could exploit the vulnerability, the ease of exploiting the vulnerability, and the consequences. Of particular interest would be the ease of shutting down large parts of the system and the possibility of malicious use of the system.

This task might identify or develop a methodology to determine the prioritization analytically on the basis of these factors. The great diversity of transportation modes and company characteristics suggests that a large

number of cases must be considered and that potential remedial measures could differ widely. However prioritization is determined, it will be important to maintain a system-level perspective to identify, assess, and compare the security issues at the level of components, subsystems, and the overall system.

Task 2. Review current industry and government practices addressing IT security. Security practices will be difficult to obtain in detail. Most companies will be understandably reluctant to discuss their practices and protective hardware and software because of concern that any revelations could compromise security. It may be possible, as in Task 1, to obtain this information by interviews conducted under stringent departmental assurances of nondisclosure. As in Task 1, an exhaustive list of which companies use which measures is not necessary, just a general sense of the level of security in each mode.

Representative companies and government agencies might be presented with a menu of security options and asked what they use. This information could then be compiled without identifying the source.

One concern, however, is that the effectiveness of these options often lies in the stringency with which they are implemented. For example, if an employee forgets his smart token but can log on anyway through a back door, security will be compromised to some degree. That information will be even more difficult to procure and may even be unknown to most company officials. Interviewers must be well versed in the technology and its use and prepared to probe for details. Another possibility might be for the government to fund a series of pilot studies of various technologies and processes to see how well they work in specific contexts.

Task 3. Determine the potential for IT-related security enhancements in the sector. This task is, in part, a follow-up to Tasks 1 and 2 and could lead to a prioritization of possible measures to reduce vulnerability. The purpose would not be to identify which measures specific companies should take, but to provide a general sense of the important identified cybervulnerabilities that could be addressed and the approximate costs of doing so.

Possible measures to address the vulnerabilities identified in Tasks 1 and 2 should be identified for each mode and for the overall freight transportation system, because of its pervasive intermodal nature, as well as for technologies and processes as they are now and as they may evolve. Analyses should be made of the expected costs (including potential interference with normal operations) in countering these vulnerabilities.

Then an additional factor can be added to the prioritization of Task 1: the costs of reducing vulnerability. This refinement may change the list of priorities. For example, a vulnerability that might result in only a moderate-consequence incident could rise on the list if the cost of remedying it were small and could actually involve significant improvements in operational efficiency. Alternatively, a vulnerability subject to a high-consequence attack that can only be addressed with very expensive fixes might drop in priority.

In connection with this task, emerging technologies and practices should be examined to determine what role, if any, they could play in addressing identified cybersecurity gaps and deficiencies. Integral to such an assessment should be both an analysis of various modes of the industry and an analysis of the overall, intermodal freight transportation system, along with an assessment of how realistic and attractive these technologies and practices would appear to decision makers—that is, their economic and operational incentives and disincentives. Companies must believe that the benefits of their investments are commensurate with the costs. If a measure improves both security and efficiency at a reasonable cost, it may be implemented as a matter of course (although these measures must compete for a place above the cutoff point on the list of potential investments that all companies consider). Other concepts might require government support because the benefits to the company are insufficient. In addition, IT may decline in cost with increasing scale of deployment. This pattern may or may not apply to cybersecurity technology. Therefore, this task should examine potential cost changes and the possibility that targeted deployment strategies might make prioritized cybersecurity measures more attractive. What might now be impractical could become cost-effective within a few years.

In addition, there should be study of "upstream" scientific and technological developments that may result in new opportunities for IT application in the future.

Task 4. Analyze policies to reduce cybervulnerability. The U.S. government could play a useful role in disseminating information on new security options and best practices. For example, the pilot studies listed in Appendix B may identify promising measures to enhance cybersecurity, but unless they are recognized by companies that can use them, they will not be implemented. The study could identify likely means, such as an annual symposium to discuss innovations or a series of training sessions.

The study also might identify follow-up studies to determine the extent to which these options were being implemented. For example, it might suggest

government–industry cooperation in performing cybersecurity validations, perhaps including "red teaming" to test security. It should apply the same tests to government's connections to the private-sector IT systems.

Finally, this task might develop a set of cybersecurity guidelines and recommendations, or at least suggest a methodology to determine how much security is enough. It could analyze how to promote the use of such guidelines most effectively.

Task 5. Assess the economic impacts of cost increases in the freight transportation industry. Some cybersecurity measures may bring with them corresponding economic benefits. For example, the use of digital signatures might reduce costs related to errors and fraud detection and management. The resulting improved service could also increase customer confidence. However, certain measures might protect against low-likelihood but very high-consequence events, such as those that may help enable the transport of weapons of mass destruction. Such measures are less likely to have ancillary benefits but could result in significant additional costs. The public might benefit from a reduction in the risk of a catastrophe, but the companies making the investment may not. Even cost-effective measures may be problematical for companies that are making no profit. The costs of increased cybersecurity could ultimately affect all companies that rely on the transport industry. This task should deal with the following issues:

1. At what levels and distribution of costs for security does the economic impact become a concern, for the freight industry itself, its users, and the U.S. economy?
2. On the basis of existing models for relating economic inputs and outputs, what changes in economic outputs might result from varying levels of investment in security?
3. Given the tight margins associated with the freight industry, is there a significant possibility of economic damage to the companies that constitute this industry?
4. For investments that may be needed for national security purposes but that provide little or no advantage to the company implementing the measures, what form of government participation (e.g., tax credits) would be most effective?

Results should be quantitative and be developed for a wide set of assumptions in order to permit consideration of a significant range of possible outputs.

Appendix A

Information Management Systems in the International Liner Shipping Industry

A detailed description of information systems in one sector of the freight transportation industry is provided in this appendix. It is included for illustrative purposes only and is not intended to suggest that the information systems of the liner shipping industry are particularly vulnerable to cyberattacks or are more lacking in protection against such attacks than the information systems in other transportation sectors.

In general, liner shipping companies manage their information and business processes with an array of technologies, including mainframe computer systems, electronic data interchange (EDI), Web tools connected to mainframe systems, customer relationship management software, fax, and e-mail. Individual lines' information management or communication systems vary. They include mainframe computer systems that allow worldwide access to a common central database and information management processes, as well as regional databases.

International liner shipping is not a concentrated industry. For example, the market share for *the major lines* serving the U.S. trade (imports and exports combined) for the first 8 months of 2002 is shown in Table A-1.

Each liner shipping company owns and operates its own information systems, which are in different locations. This reduces the potential for cyberterrorists to target all liner shipping companies' information systems at the same time in one coordinated attack. Furthermore, because shipping is a global business, a company's computer systems generally have backup and redundant capacity and operational centers in order to facilitate 24 × 7 business operations.

These features of the industry suggest that a cyberattack directed against an individual liner company's information systems is unlikely to disrupt the ocean transportation system as such.

TABLE A-1 Market Share of Major Lines Serving U.S. Trade (January–August 2002)

Line	Market Share (%)
Maersk-Sealand	13.1
Evergreen	7.1
APL	6.7
Hanjin	6.0
Cosco	5.1
P&O Nedlloyd	4.4
OOCL	4.1
Hyundai	4.0
K-Line	3.8
NYK Line	3.7
MSC	3.7
Yang Ming	3.7
Hapag Lloyd	3.5
MOL	2.5

Source: *Journal of Commerce*, Dec. 9–15, 2002, pp. 28–34 (from the top 50 lines serving the U.S. trade).

On the other hand, a more significant disruption and greater economic damage to the U.S. freight transportation system could result if a centralized government information management system used by all U.S.-bound carriers, importers, brokers, and so forth were to be targeted [e.g., the Bureau of Customs and Border Protection's (Customs') Automated Manifest System (AMS)].[1]

Another example of a centralized government information management system is the Coast Guard's National Vessel Movement Center, which receives notices of arrival (NOAs) from all vessels originating from outside the United States 96 hours prior to arrival at the first U.S. port of call. The information in the NOAs is used for U.S. government agencies' monitoring of vessel movements. Similarly, Customs' Advanced Passenger Information System (APIS) receives and screens information on persons coming to the United States, and effective later this year it will receive electronic crew manifests from vessels 96 hours prior to arrival in a U.S. port. Both Customs and the Immigration and Naturalization Service use the

[1] See "Information Flow Between Carriers and Governments" on page 51.

information in APIS to screen visitors to the United States; it is expected that eventually the Coast Guard will also use APIS for its prescreening purposes.

Business Data Systems

The heart of a liner company's information and communication processes is usually a legacy mainframe computer system that provides the critical "behind the scenes" processing and storage of data for various aspects of the business. By linking Web-based technologies to its mainframe computer, an ocean carrier can create a near real-time information-sharing system that is accessible by all its geographically diverse offices. Thus, for example, information could be input using a Web tool, put into a large relational database, and fed into the company mainframe—giving the various specialty business functions in offices across the globe (sales, customer service, operations, etc.) access to common data sets, standard report formats, and activity records.

The databases thus made available typically would include *financial databases*, such as those for invoicing, billing, and trade lane pricing; *terminal operations databases*, which are key to vessel management; *container yard inventories;* and *customer support data* used in taking bookings, creating bills of lading, tracing cargo, changing "trip plans" (from, say, rail to truck), and distributing, diverting, or consolidating cargo.

There are, of course, different levels of security for, and access to, such centralized mainframe systems. That is also the case with liner companies' public websites, which typically combine (*a*) a "general site" that can be accessed by anyone using the Internet and (*b*) a "business transaction site" that requires would-be users (mainly customers) to provide identification and be cleared for specific levels of access. A general site might include general background information about the line, company news, descriptions of available services, a company history, hiring information, contact information for offices worldwide, and links to other sites. The business transaction site requires customer registration and would provide specific access for activities such as making bookings, submitting bills of lading, tracking shipments, creating customer reports, and viewing accounts. The business transaction feature will typically involve "special privileges" (customized access) depending on the nature of the customer's business and available carrier services.

In addition to public Internet sites, many global carriers have company intranet systems for internal communications. However, because liner companies often have overseas offices in countries with communications infrastructure of variable

quality, Internet connections may be less than reliable at some locations. In those cases, intracompany communications may depend more on e-mail. In general, however, Web-based systems are preferred.

Central Dispatch/Redirection

In liner shipping, vessels operate on fixed schedules in specific trade lanes—and, except in the case of serious unforeseen circumstances, those schedules are revised as part of a broader company planning process. So the most common dispatching/redirection activities in the industry are those for containers and chassis.

When a container or group of containers is booked with a carrier, arrangements are made as to the size and type of containers needed, the container pickup date (from the company's container yard), and which vessel is scheduled to carry the containers. This can be done by the shipper either by (*a*) directly contacting the line's booking agent or (*b*) inputting the required information (origin, destination, port of loading, commodity description, shipper's name, type of container, etc.) using the appropriate business transaction section of the line's website.

Under either approach, that information goes into the company's mainframe system and becomes available to, for example, the equipment dispatcher, who must determine whether the container yard has the necessary inventory and make arrangements to have the containers available for use; and the marine terminal and vessel operators, who ensure that appropriate preparations are made and that needed equipment (e.g., reefer plugs for refrigerated containers) is available.

The ocean carrier takes control of the cargo either (*a*) at the terminal gate, in cases where the shipper handles the drayage of the container (known as "merchant haulage") from its facility to the port of loading; or (*b*) at the customer's premises, called a "store door" move, when the ocean carrier provides for the trucking service (known as "carrier haulage") using a "house" trucking firm that operates under an agreement with the ocean carrier. Carrier haulage is common in the United States and Europe but limited in Asia and Latin America, where merchant haulage is more common.

In the port of departure, the terminal operator will typically have access, via the line's mainframe system, to reports on arriving containers and the booking information needed to arrange loading by stevedores and plan the arrangement ("stowage") of containers in the vessel. That information would include, in addition to the identity of the vessel against which the cargo was booked (and therefore the sailing date), details about the type of cargo, special storage requirements, and destination port.

Once the vessel has completed its voyage and arrived at the destination port, the terminal operations staff at that port typically will be working from another report containing the relevant information for off-loading the containers and handing them off for the next leg of their journey. If the next leg is by truck, the move could again be merchant haulage or carrier haulage. If a rail move is involved (say for cargo arriving at the Port of New York and New Jersey and scheduled for a rail move to Chicago), the terminal operator will contact the rail partner by EDI with details about which containers need to be moved and when. For example, if 10 boxes need to be moved by rail to Chicago, the terminal operator will know that its rail partner has five trains running to Chicago in the next 3 days and will inform the rail planning staff which of the 10 boxes have the highest priority (i.e., need to go on the earliest of the trains), or which may require special handling (e.g., hazmat cargo).

Information Flow Among Collaborators

Because multiline alliances and other vessel-sharing arrangements are such a central part of liner shipping today, a given vessel operating in the U.S. trade may be carrying the cargo of different container lines. Consequently, a significant amount of information must be exchanged among alliance members. Most of this information exchange is handled via EDI, which in turn requires that each alliance partner's information system be programmed to accept data from the other alliance partners' systems.

Carriers' dealings with house truckers are generally handled via EDI or Web tools, if available (and bigger lines generally require such capabilities from their house truckers). Otherwise, trucking arrangements are handled by fax or e-mail. Arrangements for freight movement by rail are also generally made via EDI.

Information Flow Between Carriers and Governments

Customs' AMS represents a vital link in the flow of information about imported goods. With Customs' recent promulgation of the so-called "24-hour rule," which requires that advance cargo (CF 1302) declarations be submitted 24 hours before loading of U.S.-destined cargoes in foreign ports, AMS—in combination with Customs' Automated Targeting System (ATS)—is becoming the preeminent centralized government data management system for security prescreening of import cargoes to the United States.

Many shipping lines provide cargo manifest information electronically via AMS.[2] In addition, a number of ocean carriers and most shippers are participating in Customs' Automated Export System for the electronic submission of export cargo information; other ocean carriers provide that information today in paper (fax) form.[3]

Inbound cargo manifest data are sent to Customs' AMS through one of two data formats: (*a*) ANSI X12 or (*b*) CAMIR (Customs Automated Interface Requirements). Each ocean carrier is limited to using only one of those two systems, with ANSI X12 being predominant. Each ocean carrier is also limited to a single source with an electronic interface with AMS. So, for example, ABC Line's Rotterdam office first will provide cargo manifest information for containers scheduled to be loaded in Rotterdam for a voyage to the United States internally to the ABC Line's designated single point of contact with AMS (perhaps an office in New Jersey) to be forwarded to AMS. Thus, all cargo manifest information for cargo to be loaded at any port in Asia, Latin America, Europe, onto a vessel bound for, or calling at, a U.S. port must first go to each shipping line's single AMS contact entity.

When the line's central source for inbound manifest information contacts AMS, a return receipt is automatically generated confirming the number of bills of lading that were received and accepted and the number of bills of lading that were received and rejected because of incomplete data. The lines then know that further information is required on the rejected bills of lading.

Security prescreening checks are done by using AMS and ATS. An assessment of risk factors results in point scores that allow Customs to determine whether a container should be subject to a so-called security "hold" pending further investigation at the foreign port and whether the container should be physically inspected. Containers for which no hold messages have been communicated by Customs can be loaded, but not until 24 hours after submission of the advance cargo manifest information.

Ocean carriers also produce inbound cargo manifests to foreign governments. However, such manifests are usually paper reports, not electronic filings. Some foreign jurisdictions also request filing of export cargo manifests.

---

[2] The 24-hour rule does not formally require that the CF 1302 cargo declarations be submitted electronically via AMS, but electronic submission is strongly encouraged.

[3] It should be noted that Section 343 of the recently enacted Trade Act of 2002 (P.L. 107-210) requires, *for all modes*, that "not later than 1 year after the date of the enactment of this Act, the Secretary [of the Treasury] shall promulgate regulations providing for the transmission to the Customs Service, *through an electronic data interchange system*, of information pertaining to cargo destined for *importation* into the United States or *exportation* from the United States, prior to such importation or exportation" (emphasis added).

It is expected that more foreign jurisdictions will require electronic submission of cargo manifest information in the future. There are already indications that governments that have signed Container Security Initiative agreements with Customs for prescreening of containerized shipments bound for the United States may be in the process of implementing electronic (export) cargo manifest requirements. Also, the World Customs Organization is developing an international Customs Data Model that assumes the electronic submission of data elements to—and exchange of data elements between—exporting and importing Customs administrations.

Information Flow Between Carriers and Customers

Estimates in the trade press suggest that about 75 percent of shipper transactions with ocean carriers are handled by telephone or fax, 20 percent through individual carriers' websites, and 5 percent via the three Web-based portals (GT Nexus, Inttra, and CargoSmart) that provide access to multiple carriers at one site. The portal systems are designed to allow customers (usually larger shippers) easy access to multiple carriers when they make rate requests or book cargo.

In business transactions between ocean carriers and their customers, user registration and assignment of passwords is a common security measure, but actual encryption of data tends to be limited to situations in which the parties are passing data related to title to goods, as, for example, with remote printing of bills of lading.

Carriers communicate with customers, whether cargo owners, consolidators, or logistics management companies, in a similar fashion. As mentioned in an earlier section ("Central Dispatch/Redirection"), ocean carriers typically have "business transaction" functions as part of their public websites. When customers use the business transaction portion of a carrier's site, the information input into the system typically goes through an EDI transformation and is forwarded to the (global or regional) mainframe system.

Some companies in the liner shipping industry are moving to customer relationship management (CRM) software, which allows them to more flexibly manage customer transactions through a simpler interlinking of all the company's individual business systems. For example, CRM software can, by allowing all the separate systems to "talk to each other," permit a line's sales representatives, customer service representatives, and various operational staff to access a given customer's complete transactions history and account information. When a sales

representative signs a service contract, for example, the detailed information (e.g., the number of containers to be moved in each trade lane) would go into the CRM system in a way that facilitates the creation of sales management reports; allows customer service representatives access to the sales representative's detailed notes on the contract discussions; and indicates to system users factors such as the relevant vessel booking, loading date, and when the trucker is to be contacted. CRM also facilitates contract management activities and simplifies contract compliance reviews.

When customers want to check on the status of particular cargo movements, they can contact the line's customer service department or use the line's website. On the website, in a secure section, the customer can track the cargo's position by using coded information from the relevant bill of lading.

Appendix B

Security Initiatives and Programs with Cybersecurity Relevance

The following programs and initiatives are connected with improving freight security and use or affect a range of technologies, systems, and technology protocols.

Note: Customs = Bureau of Customs and Border Protection (formerly U.S. Customs Service); DHS = U.S. Department of Homeland Security; DOT = U.S. Department of Transportation; FAA = Federal Aviation Administration; FHWA = Federal Highway Administration; GIS = geographic information system; NHS = National Highway System; TSA = Transportation Security Administration; WMD = weapons of mass destruction.

Project:	**Electronic Supply Chain Manifest (ESCM) Operational Test**
Description:	Intermodal research project that uses biometric fingerprint readers, smart cards, and encrypted Internet transactions to enhance the security and efficiency of freight supply chain activities. The project, which initially focused on air cargo transactions, is being incorporated into other freight modal tests
Stakeholders:	Trucking, manufacturing, air cargo industries, DOT, TSA/DHS
Technology implications:	Full integration of personnel, cargo, and tracking data using a range of cutting-edge technology systems

Project:	**Transportation Worker Identification Card**
Description:	Proposed government initiative to develop and test a technology-based secure identification system for transportation workers
Stakeholders:	TSA/DHS
Technology implications:	May use two or more biometrics on a smart-card platform
Project:	**Surface Transportation Information Sharing and Analysis Center (Rail/Waterways ST-ISAC)** **Commercial Vehicle Operations ISAC**
Description:	Public–private system for sharing/transferring security-sensitive information between safety and security agencies and modal interests
Stakeholders:	Railroads, trucking companies, domestic waterway carriers, U.S. intelligence agencies, public safety agencies, law enforcement agencies
Technology implications:	Multijurisdictional data-transfer systems. Data formatting and encryption issues
Project:	**TSA Airport Biometric Research Solicitation**
Description:	TSA and FAA are developing and releasing a solicitation to develop and install aviation personnel identification systems throughout the United States (20+ airports). The focus is on access and perimeter control using existing and emerging technologies
Stakeholders:	Aviation personnel (possibly including air cargo personnel), TSA/FAA, law enforcement agencies
Technology implications:	Large-scale systems integration using personnel data and government information. Biometric data and readers integrated with personnel management applications

Project:	**Cargo Handling Cooperative Program**
Description:	Public–private consortium to pursue industry-driven enhancements to cargo handling that support a sustainable and seamless transportation system
Stakeholders:	Ocean carriers, railroads, port authorities, terminal operators/stevedores, trucking companies, government organizations
Technology implications:	Currently performing assessments of electronic seal technologies in support of the Operation Safe Commerce initiative
Project:	**Freight Performance Measures (Satellite-Based Vehicle Tracking)**
Description:	Research project that uses satellite tracking systems to develop real-time freight performance measures for the NHS (e.g., travel speeds, travel times)
Stakeholders:	FHWA, state departments of transportation, metropolitan planning agencies, NHS users
Technology implications:	New applications for vehicle tracking and analysis
Project:	**American Transportation Research Institute Data Privacy Study (Data Sharing Protocols and Strategies)**
Description:	ATRI will begin a study to analyze data privacy issues, data-sharing opportunities, and tools for protecting data
Stakeholders:	DOT, freight industries/business communities, Department of Justice
Technology implications:	The study will likely identify industry data that exist in electronic form and offer data protection strategies

Project:	**Port Security Grants Program**
Description:	Congressionally mandated and funded port security program that provides funding for proposals that test technologies and programs for improving port security. The program is focused on the largest U.S. ocean ports and strategic ports
Stakeholders:	Ocean carriers, trucking companies, port authorities, railroads, shippers, Customs, DOT, TSA
Technology implications:	Enhanced security infrastructures. Major systems integration between port systems, carrier systems, and public agencies. Likely to use new and emerging technologies and integration software applications. May require the development and collection of new data sets
Project:	**Trucking Industry Anti-Terrorism Operations Center**
Description:	The expanded Highway Watch Program has four elements: (*a*) a nationwide antiterrorism training program to maintain a 3 million–person cadre as "America's Trucking Army"; (*b*) a Call Center to take, route, and record security and safety reports from the industry; (*c*) an Operations Center to perform analysis, planning, and communications functions for the industry on a comprehensive, integrated platform; and (*d*) an Information Sharing and Analysis Center to serve as the intelligence bridge between industry and government. Scope is directly linked to the level of federal financial support for this effort
Stakeholders:	The program is open to the entire trucking industry and is coordinated by the Trucking Security and Anti-Terrorism Working Group, which consists of 19 national trade and professional organizations

Technology implications:	The Call Center will utilize a national-capability contractor to conduct this activity. The Operations Center will use a technology platform to integrate industry data, GIS simulation, and open source data
Project:	**National Hazmat Tracking and Security Test**
Description:	DOT-sponsored research program to install and test a suite of existing and emerging technologies that may improve the security and efficiency of hazmat shipments in the United States
Stakeholders:	Hazmat carriers, DOT safety and highway agencies, law enforcement, safety regulatory agencies
Technology implications:	Uses existing and emerging wireless technologies including satellite tracking and communications, new biometric authentication systems, and electronic cargo data systems
Project:	**Operation Safe Commerce**
Description:	Coordinated research and testing of supply chain security systems using existing and emerging technologies, systems, and processes through the ports of Seattle/Tacoma, Los Angeles/Long Beach, and New York/New Jersey
Stakeholders:	Coordinated by Customs, DOT, and TSA; all research and testing via partnerships among the ports and the supply chains that use those points of entry
Technology implications:	Existing and new technologies and systems in tracking, management, information interchange, physical security, and risk assessment
Project:	**Washington E-Seal Program**
Description:	Track commercial inbound containers to determine whether container integrity has been compromised and facilitate border-clearance activities

Stakeholders:	Customs, Washington State Department of Transportation, Washington State Trucking Association, ports of Seattle and Tacoma
Technology implications:	Test technology to enhance security while improving efficiency of inspection and clearances
Project:	**Safe and Secure Trade Lanes**
Description:	Industry-funded initiative to demonstrate and deploy automated tracking and security technology for containers entering U.S. ports
Stakeholders:	Hutchison Whampoa, Ltd., PSA Corporation, P&O Ports, Port of Seattle, Port of Tacoma, Port of Los Angeles/Long Beach, Qualcomm, Savi Technology, SAIC, PB Ports & Marine, many others
Technology implications:	Testing technology and concepts developed for the U.S. Department of Defense in monitoring and tracking containers
Project:	**West Coast Tracking Initiative**
Description:	Industry-funded expansion of the ESCM project that will install and test biometric smart cards for container access and tracking purposes. Will likely tie into Port of Los Angeles/Long Beach for expanded functionality
Stakeholders:	Trucking industry, shippers/manufacturers, port authorities, container stakeholders
Technology implications:	Driver authentication through biometrics; facility access control and event notification via smart card (and prox card) systems
Project:	**Customs Trade Partnership Against Terrorism (C-TPAT)**
Description:	Customs initiative to certify companies who agree to conduct a comprehensive self-assessment

	of supply chain security on the basis of guidelines developed by Customs and the trade community
Stakeholders:	Shippers, port authorities, importers/exporters
Technology implications:	Will vary depending on specific C-TPAT agreement
Project:	**Container Security Initiative**
Description:	Customs initiative to prescreen cargo at designated foreign "megaports" before export to the United States
Stakeholders:	Foreign ports, shippers, importers, and ocean carriers
Technology implications:	Use of the information provided on the Automated Manifest System to target "high-risk" shipments for further screening via X-ray, gamma ray, WMD detection technologies
Project:	**Chicago Intermodal Data Transfer Initiative**
Description:	FHWA-sponsored research to identify data-sharing opportunities among maritime shipping, rail, and trucking—with an emphasis on container movements to and from ports. The study will propose a technology system for expediting the flow of data between the modes
Stakeholders:	Freight industries, shippers/manufacturers, DOT
Project:	**Port Authority of New York and New Jersey's FIRST System**
Description:	Internet-based port community system that consolidates cargo data and integrates vessel, highway, and rail data
Stakeholders:	Port community participants (terminals, truckers, freight forwarders, brokers, ocean carriers, etc.)

Technology implications:	Potential use as a nationwide platform for consolidated cargo data
Project:	**Cargo*Mate Project**
Description:	Multitechnology, multiphased system for tracking container chassis across the United States. Recently expanded to connect system to tractor/container tracking
Stakeholders:	PAR Logistics Management Systems, maritime shipping industry, trucking industry, Customs, DOT
Technology implications:	Real-time satellite/cellular tracking of chassis to provide end-to-end cargo visibility
Project:	**Free and Secure Trade (FAST) Initiative**
Description:	A joint program between the United States and Canada, the FAST initiative is now operational at Detroit, Michigan/Windsor, Ontario; Port Huron, Michigan/Sarnia, Ontario; and Buffalo, New York/Fort Erie, Ontario. In early 2003, the FAST lane program will be extended farther west along the border to Blaine, Washington/Douglas, British Columbia, and to the east, at Champlain, New York/Lacolle, Quebec
Stakeholders:	Customs, trucking companies, DOT
Technology implications:	Electronic data sharing/transfer between public- and private-sector entities using several technologies

Appendix C

Protecting International Trade Corridors: The Operation Safe Commerce Initiative[1]

Operation Safe Commerce (OSC) is an innovative public–private partnership dedicated to enhancing security throughout international and domestic supply chains while facilitating the efficient cross-border movement of legitimate commerce. The object is to prevent terrorists or their weapons from gaining access to the United States to cause catastrophic harm, while sustaining the viability of the global transportation lifelines that support international commerce. The way to accomplish this is to move away from primary reliance on a system of control at the borders that lie within U.S. jurisdiction and toward point-of-origin controls. Point-of-origin controls are to be supported by controls developed within international supply chains and accompanied by a concentric series of checks built into the system at points of transshipment and at points of arrival. In return, the nation's world trade partners rightfully expect reciprocity and controls on U.S. exports to aid the security of their imports.

Effective international trade corridor security must rest on a foundation of credible risk management—that is, a regime that can reliably identify the people, goods, and conveyances that are legitimate, so their movements can be facilitated. This would allow shippers, importers, regulators, and inspectors to focus on the smaller number of entities about which they know little or have specific concerns. Achieving this goal requires a layered public–private approach.

OSC will validate security at the point of origin and will demonstrate what is needed to ensure that parties associated with commercial shipping exert reasonable care and due diligence in packing, securing, and manifesting the contents of

[1] The material in this appendix is based on government-supplied information not independently verified by the committee.

a shipment of goods in a container. In addition, OSC will demonstrate various methods to ensure that the information and documentation associated with these shipments are complete, accurate, and secure from unauthorized access. The project will ultimately gauge the security of the supply chain with these new procedures in order to determine their viability.

OSC will provide validated recommendations and workable solutions to legislators, regulatory agencies, the International Maritime Organization, and the World Customs Organization on how best to address the critical issue of cargo security.

The following are some of the major objectives of OSC:

- Ensure the integrity of the supply chain by encompassing the entire transaction between an importer and a supplier. This includes validating security at the point of origin, ensuring the contents of containers, and tracking the container in transit with the intent of identifying methods and evidence of possible tampering.

- Pilot the use of off-the-shelf technologies and conduct proof-of-concept projects to demonstrate other technologies to monitor the movement of legitimate cargo in transit before it reaches the U.S. border and all the way to its final destination.

- Provide a tangible prototype that can inform post–September 11 efforts—by federal and international authorities—that aim to enhance the security associated with all types of cargo, conveyances, and people moving across borders and within international trade corridors, by proving the feasibility of various industry and government proposals for layered cargo security strategies.

To achieve these objectives, OSC proposes the following:

1. Apply a common set of standard security practices to govern the loading and movement of cargo throughout the supply chain. The goal is to ensure that an authorized packer of a container knows what is in that container and can report those contents accurately.

2. Ensure that the container's electronic documentation is complete, accurate, and secure against computer hackers and is provided to law enforcement agencies in a timely manner.

3. Reduce the risk of a container being intercepted and compromised in transit.

OSC will work initially with three major ports: Seattle/Tacoma, New York/New Jersey, and Los Angeles/Long Beach. Seventy percent of the container movement in the United States originates or terminates with these entities. To achieve these objectives, the three load centers will use several methods that may include all or some of the following:

- Validating and assessing the entire delivery system through examination of the discrete stages of the product flow (supply chain):
  1. Product origination (the factory and subcontract manufacturing),
  2. Product shipping to export facility (transportation company),
  3. Export stage repackaging and shipping (export broker),
  4. International transport (freight company),
  5. Export arrival and storage (transportation company, warehouses, customs facilities, port, ocean carrier),
  6. Vessel voyage (ocean carrier),
  7. Import arrival and storage (port, transportation company, warehouses, customs facilities),
  8. Cargo conveyance (rail, truck),
  9. Cargo breakup into multiproduct facilities (drop centers, distribution warehouses), and
  10. Product arrival and storage at the buyer's facility.

- Complying with Business Anti-Smuggling Security Coalition or similar procedures and standards.

- Requiring secure packing procedures for loading intermodal containers along the lines of ISO9000 quality assurance rules.

- Maintaining secure loading docks at manufacturing plants or at shipping facilities that restrict access to authorized individuals and that use cameras to monitor the loading process. Loading docks would be subject to periodic, random, independent inspections to ensure compliance.

- Using third-party verifiers to augment the capability of government enforcement authorities to audit, certify, and validate shipments and supply chain service providers.

- Providing and checking proper import vouchers before loading cargo on vessels.

- Using technology to secure and monitor containers and their movement through the intermodal supply chain.

- Outfitting containers with theft-resistant mechanical and electronic seals.

- Installing light, temperature, or other sensors in the interior of the container, which would be programmed to set off an alarm if the container is opened illegally at some point of transit.

- Conducting background checks of truck drivers who deliver goods to the port and outfitting them with biometrically based identity cards.

- Attaching an electronic transponder (such as those used for the "E-ZPass" toll payment system in the northeastern United States) and Global Positioning System devices to the truck cab and chassis or rail car carrying containers and using intelligent transportation system technologies to monitor in-transit movements to and within the port terminal.

- Maintaining the means to communicate with operators from their pickup to their off-load destinations.

- Providing tracking information to the appropriate regulatory or enforcement authorities within the jurisdictions through which the cargo will be transported.

- Leveraging the Port of New York and New Jersey's Freight Information Real-Time System for Transport vessel and cargo information system, or other similar information portals, by requiring all participants in the supply chain cycle to provide advance notice of the details about their shipments, operators, and conveyances in accordance with agreed-upon protocols. This early notice would give government inspectors the time to assess the validity of the data and check the data against any watch lists they may be maintaining, and would provide timely support to a field inspector deciding what should be targeted for examination.

The following may be among the major project tasks:

1. Forming regional task forces that will include the law enforcement community and other regulatory authorities, as well as appropriate academic and technical experts.

2. Enlisting private business-sector partners involved with all stages of product flow in the construction of a process flow map for the physical movement of each container/supply chain that has been identified. The chain of custody as well as the information flow will also be mapped out to identify security gaps and how they can be redressed.

3. Tasking the regional task force members to examine the following for security gaps: (*a*) the entire design-to-delivery product flow; (*b*) the means of conveyance—maritime, rail, truck, and air; and (*c*) the "who and how" connected with the operators who move the products.

4. Conducting field visits to witness the actual supply chain process.

5. Having the regional task force prepare recommendations they believe might redress the gaps they identify. A recommendation should fall under one of three groupings: (*a*) off-the-shelf technologies for securing and tracking shipments, (*b*) improvements to existing data collection and sharing arrangements, and (*c*) process changes that would close opportunities for compromise at the point of origin or in transit.

6. Enlisting a support group made up of academic and private-sector partners to develop technological applications for testing as the regional task force identifies gaps. An outreach effort will be made to other government-sponsored R&D programs that are field-testing tracking and sensor technologies that support a demonstration of how secure in-transit visibility and accountability can be achieved.

7. Conducting trials of new technologies, data arrangements, or process changes using volunteer manufacturers, importers, surface shippers, freight forwarders, maritime shipping lines, and terminal operators.

8. Testing the integrity of systems with "red-team" exercises.

9. Preparing reports to capture and quickly relate lessons learned from the security gap analyses and the testing and refinement of technological applications. The reports will aim to provide guidance for a layered, multitiered approach for replication and standardization of policy approaches to securing trade corridors. The audience includes legislators and policy makers involved in the U.S.–Canada "Smart Border" Agreement and participants in counterterrorism initiatives under consideration by the International Maritime Organization, the World Customs Organization, the International Standards Organization, and other relevant multilateral and international bodies.

APPENDIX D

U.S. BUREAU OF CUSTOMS AND BORDER PROTECTION USE OF INFORMATION TECHNOLOGY[1]

The U.S. Bureau of Customs and Border Protection (Customs) has developed an extensive array of information systems that support the collection, processing, and analysis of data on goods, people, and conveyances entering and exiting the United States. These systems were developed over the past three decades with the involvement of many government agencies and the international business and transportation communities. The following statistics are intended to provide a brief picture of the magnitude of two of these systems:

- The Automated Commercial System (ACS) currently processes more than 99 percent of the $1.8 trillion in imports and exports in all modes of transportation.

- The ACS database has 4 terabytes of electronic storage and 6.2 billion records accessed 578 million times daily.

- The Treasury Enforcement Communications System (TECS) currently processes more than 475 million travelers entering the United States by air, land, and sea.

- The TECS database has 3 terabytes of DASD and a database of 5.3 billion records accessed 766 million times daily.

[1] The material in this appendix is based on government-supplied information not independently verified by the committee.

- ACS and TECS support or have interfaces with more than 100 U.S. government agencies and foreign countries, nearly all international transportation carriers, and thousands of international businesses and service providers.

In August 2001, Customs embarked on a Modernization Program, a 15-year initiative to modernize and integrate its information technology infrastructure to support the government's oversight of import and export trade compliance, border enforcement, and international passenger processing. Modernization will enable Customs and all participating government agencies to collect, analyze, collaborate on, and disseminate the right international trade and traveler information to internal and outside users in advance or in real time—to the right people, at the right time, and in the right place. Furthermore, the program will enable border-related government agencies and the international trade and travel private sector to transform the way they do business by implementing new processes that support future trade growth and changing business requirements.

Baseline Description of Existing Systems

Today, Customs has information systems in place at the 300 U.S. ports of entry to process all inbound and outbound cargo and passengers. Although these systems are antiquated, they still provide the platform for air and sea carriers to transmit cargo and passenger manifests in advance of arrival and enable importers to file their entries electronically. Customs interfaces with virtually every entity in the international supply chain process—importers, exporters, carriers, and a multitude of intermediaries and service providers.

Currently, Customs uses multiple systems that process international trade and travel and support a multitude of agencies and commercial businesses. The following are examples:

- ACS tracks and monitors all imports of goods entering the United States.

- The Automated Broker Interface is the central government system for the filing of commercial declarations on imported cargo.

- The Automated Manifest System is a multimodular international cargo inventory control and release notification system for sea, air, and rail carriers.

- The Automated Export System is the central point through which export shipment data required by multiple agencies is filed electronically for all methods of transportation.

- The Advance Targeting System assembles and screens commercial, transportation, and passenger data to identify high-risk imported cargo and arriving international passengers.

- TECS is a megadatabase of law enforcement information shared by the Federal Bureau of Investigation, the Immigration and Naturalization Service, and Customs. It is used to screen all persons entering the United States.

- The Interagency Border Information System meets the data-sharing, analytical, and processing needs of a multiagency (State, Treasury, Justice, Agriculture) border effort for international passengers and conveyances.

- The Advance Passenger Information System receives and analyzes biographical data on international air passengers before their arrival in the United States. It covers about 85 percent of the 67 million passengers arriving.

The communications backbone is the Treasury Communications System Wide Area Network (Frame Relay) with multiple levels of protection and multiple remote access methods and controls.

Current and Planned Developments

The Customs Modernization Program will integrate all Customs information systems that encompass imports and exports, conveyance and shipment tracking, passenger enforcement, investigative and intelligence support, human resources, and financial management.

The first components currently under development are the Automated Commercial Environment (ACE) and the International Trade Data System (ITDS) programs, which focus on cargo import and export operations. ACE and ITDS form a coordinated system that provides a "single window" allowing the international business community to interact with Customs and all government agencies on import/export requirements.

ACE will lay the technology foundation for all Modernization programs and deliver enhanced "cradle-to-grave" support of the cargo control and enforce-

ment process. All related functions in field operations and enforcement will be supported from a single common user interface, a single window for officers to perform their work. ACE will process both imports and exports and will be linked seamlessly to enforcement, revenue management, and mission support systems to enable integrated field operations and nationwide collaborative teaming among officers. Delivery of ACE functions will begin in the field in January 2004 and will continue in phases extending through April 2006.

The following are the major business functions of ACE that directly link to the freight transportation sector:

- *Portal*—a universal, secure Internet "window" for all authorized system users (Customs, other government agencies, and the international transportation community) to transmit, analyze, and collaborate on supply chain data. Projected for spring 2003.

- *Account Management*—provides a single comprehensive, nationwide account-based picture of all reported activity and relationships for an importer, an exporter, an international carrier, or a logistics/service provider. Projected beginning spring 2003 through 2005.

- *e-Release*—provides for advance receipt of transportation data via transponders/electronic seal transmissions resulting in inspection or release information at the earliest point in the supply chain. Projected for truck transportation in 2004 and all other modes beginning in 2005.

- *Multimodal Manifest*—provides for advance transportation data at the earliest point in the supply chain. Projected for truck transportation in 2004 and all other modes beginning in 2005; will track cargo across modes in 2007.

- *Cargo and Conveyance Tracking*—provides for tracking shipments (including in-bond) and conveyances, and provides release or status of shipment subject to government agency control.

ITDS supports 101 agencies with information and actual operational interaction on shipments, crew, and conveyances crossing the border.

As stated by the ITDS multiagency Board of Directors:

> ITDS is a federal government information technology (IT) initiative to implement a secure, integrated, government-wide system for the electronic collection,

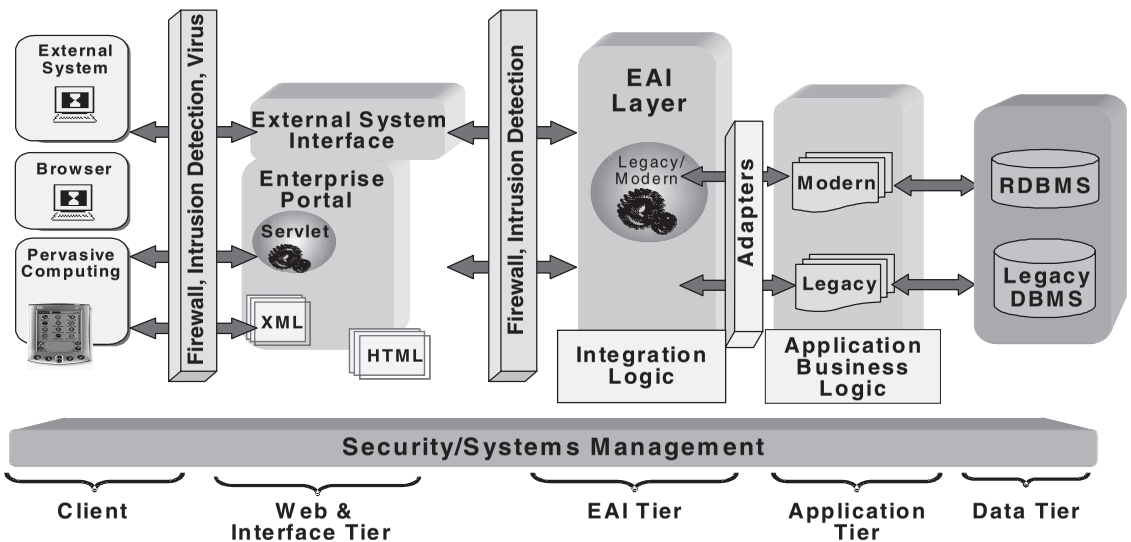


FIGURE D-1 ACE architecture: conceptual view.

> use and dissemination of international trade and transportation data . . . The ITDS Board of Directors has oversight responsibility and serves as a forum for harmonization of requirements and dispute resolution among federal agencies. The Board insures that ITDS goals and functionality are integrated with the needs of the public, the participating agencies and Customs modernization plans.

Customs Information Technology Systems Security

Customs' new Enterprise Architecture (EA) for ACE and the Modernization is established to support all field activities and align information technology with the strategic objectives of Customs and all agencies. The EA provides for a multi-layer security management system. The information Customs has made public is represented in Figure D-1.

Potential Vulnerabilities

The Customs Modernization and ACE programs will be state of the art but are subject to cyberattacks, as are all information systems. The reality of connectivity with the international trade and transportation community and the electronic exchange of massive amounts of data and database queries add to the potential vulnerability.

Study Committee Biographical Information

Robert E. Gallamore, *Chair,* is Director of the Transportation Center and Professor of Managerial Economics and Decision Sciences in the Kellogg School of Management at Northwestern University, Evanston, Illinois. Before joining Northwestern University, he was Assistant Vice President, Communications Technologies, and General Manager of the North American Joint Positive Train Control Program at the Transportation Technology Center, Inc., while on executive loan from the Union Pacific Railroad. Before this assignment, he was General Director, Strategic Analysis, for the Union Pacific Railroad in Omaha and an executive with UP Corporation in New York City. Dr. Gallamore has also served as Deputy Federal Railroad Administrator, Associate Administrator for Planning with the Urban Mass Transportation Administration, and System Plan Coordinator with the United States Railway Association. He received an A.B. from Wesleyan University and an M.A. in public administration and a Ph.D. in political economy and government from Harvard University.

A. Ray Chamberlain, *Vice Chair,* is Vice President of Parsons Brinckerhoff. He has previously held positions as Vice President, Freight Policy, and Acting Managing Director of the American Trucking Associations Foundation; Chief Executive Officer of the Colorado Department of Transportation; and President of Colorado State University. He has served as President of the American Association of State Highway and Transportation Officials (AASHTO), as Chair, TRB Executive Committee, and as Chairman, Board of Directors, National Association of State University and Land Grant Colleges. Dr. Chamberlain received a B.S. in engineering from Michigan State University, an M.S. in engineering from Washington State University, and a Ph.D. in engineering from Colorado State University.

Frank J. Anstett is Manager, Infrastructure Security, at Raytheon Company. Mr. Anstett's experience includes management of diverse functional groups,

including U.S. Department of Transportation security and infrastructure teams; information technology (IT) evaluation and implementation; performance of risk assessments; and the development of International Organization for Standardization–compliant procedures. As Engineering and Installation Manager, he was the primary interface between Raytheon and the Federal Aviation Administration (FAA) in support of the Transportation Security Administration's installation of explosive detection equipment. He led a diverse team in the evaluation and improvement of Raytheon/FAA management information systems (MIS). He then led a team in testing and implementing the new MIS tools, including the development of new functional policies and procedures. Mr. Anstett has successfully managed numerous FAA infrastructure upgrade projects across the United States. They include vulnerability and risk assessment requirements so that improvements do not interfere with the safety or effectiveness of FAA's air traffic control system.

Samuel H. Banks is Senior Vice President of the U.S. Customs Modernization Project and resident at Sandler and Travis Trade Advisory Services, specialists in international trade. His experience in customs and international trade includes more than 28 years at the U.S. Customs Service. Mr. Banks began his career at Customs as a uniformed inspector in San Francisco and rose to become the highest-ranking career official in the agency, Deputy Commissioner, for 4 years. He also served as the Acting Commissioner of Customs for 1 year. Throughout his tenure with U.S. Customs, Mr. Banks worked on a number of major initiatives, including the Customs Modernization Act, the landmark legislation that significantly altered the rules governing the entry of imported merchandise into the United States. He represented the United States at international forums and negotiated numerous international agreements, including significant portions of the North American Free Trade Agreement. Mr. Banks received many awards during his career at the Customs Service, including the Distinguished Government Executive Award—the highest award given to career public servants—granted to him by President Bush and the Excellence in Government Award from the Joint Industry Group. In the private sector, Mr. Banks worked as a consultant for various international trade businesses including the Air Transport Association, United Parcel Service, and Lockheed Martin. Most recently, Mr. Banks served as a corporate officer for an international trade information technology firm.

Richard A. Holmes, Jr., is the General Director of Security and Quality Assurance for Union Pacific Railroad and is responsible for information security,

disaster recovery, change management, development methodologies, and quality assurance functions at the company. He has been involved in information assurance activities for more than 16 years at Union Pacific. Currently he is a board member of the Partnership for Critical Infrastructure Security. He is past President of the Nebraska chapter of InfraGard. Most recently he led the Information Sharing and Analysis working group of the Association of American Railroads and participated in the development of the rail industry's risk analysis and security management plan. Mr. Holmes teaches information assurance courses for the Institute of Internal Auditors and is a Senior Technical Associate for the Nebraska University Consortium on Information Assurance. Before transferring to the Information Technologies Department, he performed financial, operational, and information systems audits of Union Pacific Corporation's railroad, trucking, oil and gas, mining, hazardous waste, and logistics companies. He earned an MBA from Creighton University and a bachelor's degree in management information systems from Iowa State University.

Barry Horowitz (NAE) is Professor of Systems Engineering at the University of Virginia. Formerly he was Chairman and founder of Concept Five Technologies, an e-business solutions provider specializing in applying enterprise application integration and security technologies to B2B systems. He served as President and CEO of The MITRE Corporation and President and CEO of Mitretek Systems. He received the highest civilian award of the U.S. Air Force for his contributions to the Gulf War related to locating, tracking, and destroying SCUD missiles. Dr. Horowitz is a member of the National Academy of Engineering. He holds a BSEE from City College of New York and an MSEE and Ph.D. in electrical engineering from New York University.

John L. King is Professor and Dean of the School of Information at the University of Michigan. His research is in the development of large-scale information systems in complex organizational and institutional problem domains, including logistics. He is a member of the Advisory Committee of the National Science Foundation's Directorate for Computer and Information Science and Engineering and the Board of Directors of the Computing Research Association. He previously served in faculty and administrative roles in the University of California at Irvine and as Marvin Bower Fellow at the Harvard Business School. From 1993 to 1998 he was editor-in-chief of the INFORMS journal *Information Systems Research*. He has been coeditor or editorial board member of many other journals, including *Information Infrastructure and Policy*, *ACM Computing Surveys*,

the *Journal of Organizational Computing and Electronic Commerce*, and the *Journal of the Association for Information Systems*. He holds M.S. and Ph.D. degrees in administration from the University of California at Irvine.

Lars Kjaer is Vice President of the World Shipping Council. He has been working closely with industry leaders and government agencies to enhance the security of containerized cargo at all points of the intermodal supply chain. His previous position was Washington Representative for the Council of European and Japanese Shipowners Associations from 1999 to 2000. Before that, Mr. Kjaer was counselor at the Royal Danish Embassy in Washington, D.C., from 1993 to 1998. During that tenure he was also chairman of the Cotton Club of foreign transportation counselors in Washington. At the Royal Danish Embassy, Mr. Kjaer was responsible for transportation matters, in particular shipping policy, and for bilateral and regional trade issues, including the GATS (services) negotiations in the World Trade Organization. He joined the Danish Ministry of Foreign Affairs in 1983. While with the Foreign Service of Denmark, his positions included principal head of section in the Middle East Political Department and chair of various working groups of the European Union's Foreign Policy Cooperation. His foreign postings included a 4-year term as First Secretary at the Danish delegation to the North Atlantic Treaty Organization in Brussels.

Art Kosatka is CEO of TranSecure LLC, an aviation consulting firm formed after his retirement as a Senior Civil Aviation Security Specialist with FAA and the Airport Security Policy and Planning Division of the Transportation Security Administration. Mr. Kosatka was responsible for writing the security regulations under which airports operate and for the definitive manual of policy interpretations used nationwide by federal security directors at all commercial airports. He came to FAA from a career in airport consulting in which he managed various security projects at 32 airports, including 13 of the Transportation Security Administration's 22 high-risk Category X airports. He has been Director of Public Safety and Security for the Airports Council International, representing the industry's security concerns nationwide, and he has served on both U.S. Senate and House of Representatives staffs handling transportation issues. He was three-term Chairman of the Airport Consultant Council's Security Committee and is an instrument- and multiengine-rated pilot.

Stephen J. Lambright is Vice President of Marketing, Savi Technology. He works with customers, global partners, and government agencies to identify and define

solutions for global supply chain security and asset management. With a focus on improving, hardening, and expanding the global supply chain IT infrastructure, Mr. Lambright has more than 12 years of international experience in enterprise IT solution design, development, and deployment. Mr. Lambright is a member of the Technology Board of the Auto-ID Center at the Massachusetts Institute of Technology, Council for Logistics Management, and the Society of Logistics Engineers. He is also currently acting as Executive Director of the Strategic Council on Security Technology. Mr. Lambright holds a bachelor of science from Northwestern University and a master's in business administration from the University of California at Berkeley.

Daniel Murray is Director of Research for the American Transportation Research Institute (ATRI; formerly the ATA Foundation). ATRI, the autonomous research arm of the American Trucking Associations (ATA), conducts comprehensive research on a variety of issues to improve trucking and transportation safety, security, and productivity. His areas of expertise are in intelligent transportation systems (ITS) applications and freight mobility and transportation planning, and his current research focuses on the development of national ITS systems to enhance freight efficiency and security. Mr. Murray has managed several large-scale research projects including the O'Hare Airport Air Cargo Security Access System Project, the Multimodal Electronic Supply Chain Manifest field test, a study to develop real-time freight performance measures, and the Tacoma–Chicago Intermodal Data Transfer Study. He is current or former board member of the Minnesota Guidestar ITS Board, the Midwest Transportation Alliance, and the Minneapolis–St. Paul metropolitan planning organization. He received his M.S. from Northwestern University.

Frank Pittelli is cofounder and President of Navius Technologies, LLC. He has more than 20 years of experience spanning the breadth of the computer industry, including research, system design and development, academic and professional teaching, high-level analysis, consulting, and product development. In the area of computer security, Dr. Pittelli has participated in a number of advanced computer security studies, including the National Research Council's Committee on Computer System Security and the Committee for Review of the National Cryptographic Policy. Dr. Pittelli's practical experience includes the design and analysis of secure systems. He was the principal author of the concept of operations for the key escrow system for the Clipper chip, and he developed a complete curriculum of courses for a major secure product vendor. He

has conducted a number of enterprisewide security audits for clients that combined the analysis of system functionality and security in a relatively short period of time. Dr. Pittelli has been instrumental in the development of three successful entrepreneurial companies. He received his B.S. degree, summa cum laude, in computer science from Rensselaer Polytechnic Institute in 1981 and his M.A. and Ph.D. degrees in computer science from Princeton University in 1984 and 1986, respectively.

Alan F. Spear is President of MRC Investigations (USA), Inc. The company specializes in cargo crime investigation and prevention, counterhijacking and piracy, tracing stolen marine assets, vessel tracking, and asset tracing. Before this appointment he was Director, Loss Control, Operation Intercept, and Assistant Vice President, Claims, XL Specialty Insurance Company (Intercargo). He has contributed to the development of standards on cargo security and is an author of articles published on the subject. Mr. Spear received a bachelor's degree from Knox College and a master's degree in community mental health from Northern Illinois University.

Karen Ryan Tobia has held administrative and managerial positions with the Port Authority of New York and New Jersey in departments as diverse as Comptrollers, Office of the Executive Director, Economic Development, World Trade and Economic Development, Regional Development, and Port Commerce. In her current position as Manager, Technology Planning, in the Strategic Analysis and Industry Relations Division of the Port Commerce Department, she is responsible for the research, development, and implementation of new maritime- and port-related technologies at Port Authority marine facilities within the Port of New York and New Jersey. This includes the research of ITS technologies as they relate to the movement of intermodal freight and commercial vehicle operations, testing and implementation of new security-related technologies, and testing and implementation of port-related information and data management systems. She also acts as the Project Manager for the Port Authority's Freight Information Real-Time System for Transport, or FIRST, which features an interactive website for ocean container tracking and port information. She is Vice Chair of the Cargo Handling Cooperative Program and Cochair of the Intermodal Program Track of the I-95 Corridor Coalition. Ms. Tobia received a bachelor of science degree in management and communications from Adelphi University.