STRATEGY TO ENHANCE INTERNATIONAL SUPPLY CHAIN SECURITY

JULY 2007

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
19 JUL 2007	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Strategy to Enhance International Supply Chain Security	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Homeland Security Washington, DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**130**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

FOREWORD

The "Security and Accountability for Every Port Act of 2006" (the SAFE Port Act, P.L. 109-347, 120 Stat. 1884, October 13, 2006) required that the Secretary of Homeland Security, in consultation with appropriate Federal, State, local, and tribal government agencies, the private sector, and the international community develop and implement a strategic plan to enhance the security of the international supply chain. An initial version of the strategy is required to be submitted to Congress by July 10, 2007, with a final version to be completed by October, 2009.

In signing the SAFE Port Act, President Bush stated:

"This bill makes clear that the federal government has the authority to clear waterways, identify cleanup equipment, and reestablish the flow of commerce following a terrorist attack. We'll do everything we can to prevent an attack, but if the terrorists succeed in launching an attack, we'll be ready to respond."

This strategy establishes the overarching framework for the secure flow of cargo through the supply chain and builds on existing national strategies, plans specific to individual segments of the supply chain or transportation system, and numerous programs and tactical plans developed and implemented by appropriate Department components and agencies. Specifically, it follows the flow of cargo throughout the chain, from point of origin to final destination. It provides the overall strategic structure in which United States cargo security programs and efforts operate and clarify how those programs harmonize with similar international programs, such as the World Customs Organization's "Framework of Standards to Secure and Facilitate Global Trade."

Additionally, the strategy specifically focuses on resumption of trade following an incident. It establishes protocols for the prioritization of vessels and cargo, identifies incident management practices specific to trade resumption, and describes guidance for the redeployment of resources and personnel. In doing so, the strategy recognizes that there exist many different types of incidents which might impact the supply chain, but that resumption itself is an "all hazards" requirement.

The DHS is the lead department for this strategy. However, its successful execution involves cooperation and coordination across a wide spectrum of organizations with different roles and responsibilities including Federal, State, local and tribal governments, the private sector, foreign governments, and international organizations. Many parts of the supply chain are outside the jurisdiction of the United States, and only through strong partnerships can supply chain security be achieved. Indeed, even within U.S. jurisdiction, the private sector owns and operates the vast majority of the supply chain. As such, the Department consulted extensively with stakeholders at all levels in developing this document, and looks forward to continuing the successful dialogue in developing the final strategy.

TABLE OF CONTENTS

FOREWORD i

TABLE OF CONTENTS ii

I. EXECUTIVE SUMMARY 5

II. PURPOSE 6

Strategic Strategy Objectives 6

Problem Definition 7

Risk Assessment 10

Goals 12

Strategic Objectives 12

III. SCOPE 16

Boundaries and Constraints 16

Relationship to Other Plans and Strategies 17

IV. GUIDING PRINCIPLES 27

Guiding Principles 27

The Role of Technology 28

Economic Impact 28

All-Hazards Planning 29

Concepts of Prevention, Response, and Recovery 31

Resources 33

V. CONSIDERATIONS AND ASSUMPTIONS 34

VI. STRATEGY DEVELOPMENT METHODOLOGY 36

VII. ROLES, RESPONSIBILITIES, AND AUTHORITIES 37

United States Federal Government Functional Responsibilities 38

State, local and tribal government 52

Private Sector 54

Authorities 56

Federalism 59

Existing Interagency Institutions 60

VIII. STRATEGIC ELEMENTS 64

Supply Chain Strategy Overview 64

Prevention Throughout the Supply Chain 64

Performance Measures 81
Incentives for Voluntary Private Sector Measures 81
International Standards 83
Implementation Schedule, Priorities, and Milestones 84
IX. RESPONSE AND RECOVERY 86
Recovery 94
Resumption of Trade 98
Information Sharing and Communications 103
X. TRAINING AND EXERCISE REQUIREMENTS 107
Appendix A: List of Acronyms 109
Appendix B: Terms 114
Appendix C: Additional Authorities 124

I. EXECUTIVE SUMMARY

This strategy was developed in response to Sections 201 and 202 of the SAFE Port Act (PL 109-347, 120 Stat. at 1901, 1903, October 13, 2006) which require the development of a strategic plan to enhance the security of the international supply chain, including protocols for the expeditious resumption of the flow of trade following a transportation disruption or transportation security incident.

The *Strategy to Enhance International Supply Chain Security* exists within a framework of other national strategies and plans including the National Security Strategy, the National Strategy for Homeland Security, the National Strategy for Maritime Security (and component plans), the National Response Plan, the National Infrastructure Protection Plan, the National Maritime Transportation Security Plan and other strategic plans. As a DHS Strategy, it does not replace these documents. Rather, this strategy seeks for the first time to harmonize their goals into a multi-layered, unified approach for further development by Department components.

The Department based its security programs on a layered, risk management approach. The individual elements, programs, and initiatives which compose this strategy are each built upon extensive risk analysis specific to the risk area they cover in the supply chain. Assessments are used to identify the highest risk areas and resources are directed at those areas. For instance, currently all cargo containers destined for the United States are screened through the Advanced Targeting System, and 100% of high-risk cargo is subject to additional scrutiny which may include physical inspection or scanning via non-intrusive sensor technologies.

This strategy identifies critical nodes where security efforts achieve the greatest impact across the breadth of the international supply chains. Action at these nodes (such as the Secure Freight Initiative), coupled with end-to-end programs (such as the Customs-Trade Partnership Against Terrorism), provides for truly layered security. The implementation of this strategy requires the combined efforts of DHS agencies, other government agencies and the development of partnerships with industry, foreign governments, and international organizations such as the World Customs Organization and the International Maritime Organization.

The international supply chain is owned by an amalgam of private sector interests and regulated by multiple international, national, state, and local government jurisdictions. This document delineates the supply chain security roles, responsibilities and authorities of government bodies within the United States.

Disruptions to the supply chain can quickly create serious economic consequences. As stipulated by the National Response Plan, this strategy explains the response activity necessary using a clear unified command to ensure recovery efforts are activated to secure and restore transportation capabilities, and resources are redeployed to support the flow of trade. Factors used in the prioritization of vessel and cargo movement during recovery operations are illustrated by a decision tree. Training and exercise programs are used to bring together government agencies and the private sector to test responses and foster the strong communications necessary to minimize the impact of any future disruption to the transportation system.

II. PURPOSE

STRATEGIC STRATEGY OBJECTIVES

As directed by Section 201 of the SAFE Port Act (P.L. 109-347, 120 Stat. 1901, October 13, 2006), the Department of Homeland Security (DHS) must develop, implement and update a strategy to improve the security of the international cargo supply chain. This strategy reflects work that has already been accomplished by the multiple agencies involved in international cargo supply chain security as well as describes how future actions mandated by the SAFE Port Act will be integrated to accomplish this objective.

There have been significant improvements in the security of the international cargo supply chain since September 11, 2001. These improvements include passage of the Maritime Transportation Security Act (MTSA, P.L. 107-295, 116 Stat. 2064, November 25, 2002), the development of the National Strategy for Maritime Security (NSPD-41/HSPD-13) and its eight supporting plans, and multiple individual agency initiatives such as the Customs - Trade Partnership Against Terrorism (C-TPAT), the Container Security Initiative (CSI), and the International Port Security (IPS) Program. Additional improvements have been achieved via cooperative agreements with the United States' trade partners, both governmental and in the private sector. In support of this, an objective of this strategy is discussion of how those plans and initiatives work together to strengthen supply chain security throughout the global span of the supply chain.

This document does not seek to replace the more detailed plans already in existence. It seeks to outline the strategic and tactical plans associated with the various initiatives and programs currently in process. By way of example, the National Response Plan (NRP) articulates in detail how the United States will respond to an incident, including addressing communications, specific roles and responsibilities, and logistics management (among other things). This strategy supports the NRP by articulating the strategic intent of the Department with respect to supply chain security and trade recovery.

The strategy describes the security efforts that begin at cargo origination (i.e., stuffing of a container at a foreign factory/consolidator), drayage to the foreign port, loading on a vessel or conveyance at the foreign port, movement to and arrival at a United States port of entry, release from the port of entry, and drayage to final destination. This focus on cargo movement from foreign point of origin to domestic destination arises out of recognition of sovereignty issues, specifically that our trading partners set their own regimes and requirements for cargo inbound to their ports. Efforts (such as the Secure Freight Initiative, SFI) which occur in the jurisdiction of foreign trade partners are accomplished via international or bilateral agreements.

Additionally, this strategy describes trade resumption efforts and provides a generalized decision tree for the prioritization of cargo and vessels in the event of a supply chain disruption. This decision tree is generalized in that unpredictable port level factors and operating conditions will of necessity inform actual decision-making processes.

PROBLEM DEFINITION

International cargo supply chain security is a global issue that cannot be successfully achieved unilaterally. From a United States perspective the most effective supply chain security measures are those that involve assessing risks and identifying threats presented by cargo shipments before they reach the United States. For international containerized cargo, this assessment and identification is most effective if it is conducted before a container is loaded onto a vessel destined for the United States. Yet this is only half of the necessary calculus. The global supply chain is bidirectional, requiring domestic efforts to ensure the integrity of both inbound and outbound cargo. Such an effective cargo security strategy requires a multi-layered, unified approach that must be international in scope.

THE INTERNATIONAL CARGO SUPPLY CHAIN

The Department studied the international supply chain extensively while developing "Operation Safe Commerce." Eighteen demonstration projects were conducted which identified the unique features of different supply chains. As analysis of the demonstration projects proceeded, it became apparent that supply chain similarities significantly outweighed supply chain dissimilarities. The review of the diverse supply chains resulted in the conclusion that a series of standard supply chain nodes could be defined to adequately describe all intermodal container trade. In addition, it was concluded that these supply chain nodes are functional in nature and could serve as standard security control points around which threats, vulnerabilities, consequences and security countermeasures could be identified, characterized, and analyzed or designed.

Similarly, the intermodal container flow can be seen as analogous with virtually all transportation modes, with the exception of pipelines.

Modifying the Operation Safe Commerce supply chain to accommodate non-containerized cargo results in 16 nodes, as shown in figure 1:

1. Origination of cargo (supplier or factory).
2. Origination of packaging.
3. Origination of container (if containerized cargo).
4. Mating of cargo and packaging.
5. Consolidating of cargo/sealing of container (if containerized cargo).
6. Storage awaiting transport.
7. Movement of cargo to Port of Origin.
8. Port of Origin (airport, marine terminal or facility, trucking company).
9. International transportation.
10. Port of Entry (airport, marine terminal or facility, border Port of Entry).
11. Movement to deconsolidation point.
12. Storage waiting for processing.

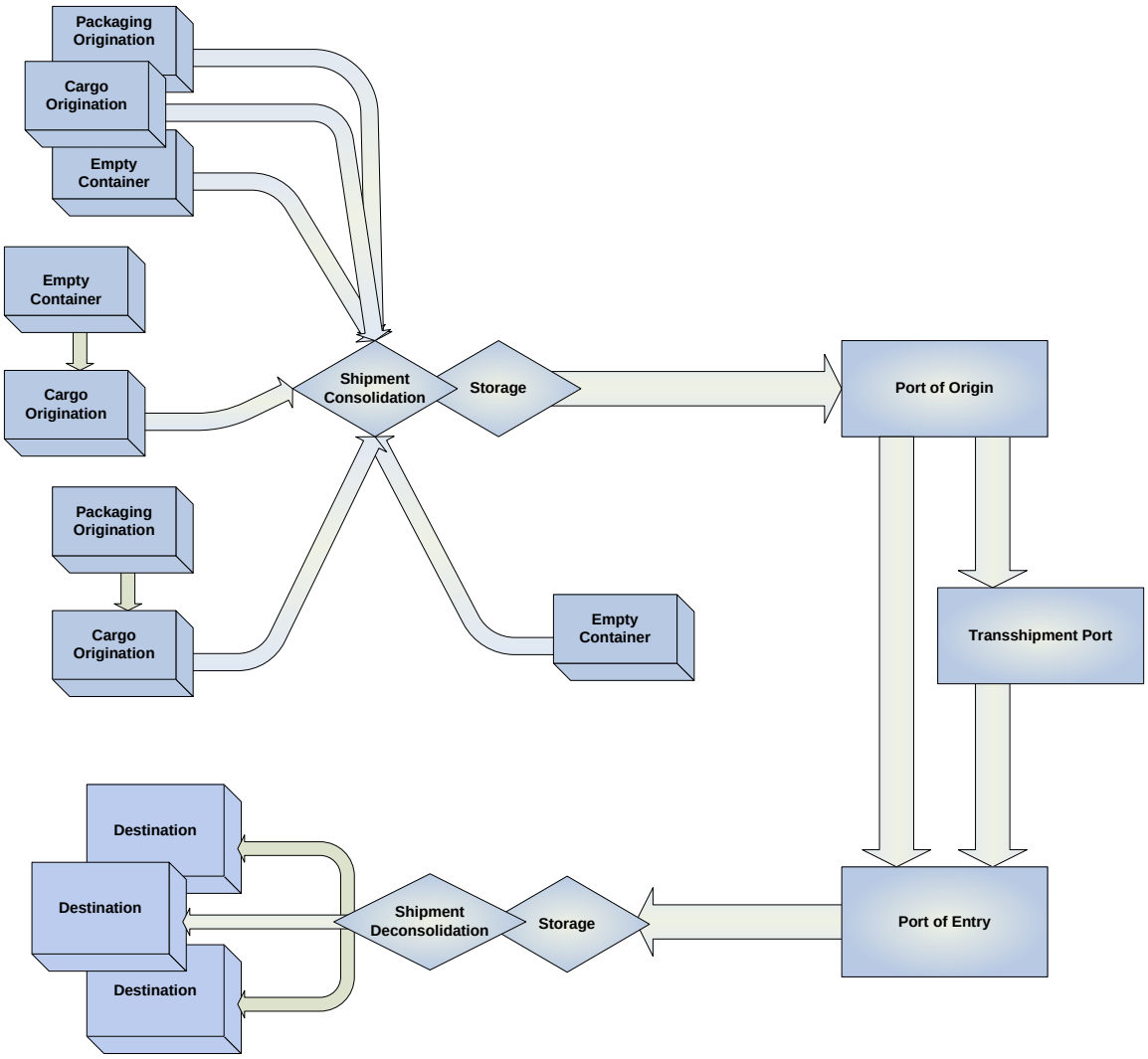


Figure 1: Generalized International Cargo Supply Chain

13. Deconsolidation.
14. Movement to destination.
15. Destination.
16. Information flow associated with cargo (end-to-end).

Literally thousands (potentially, millions) of different source streams can feed from origination through packaging and consolidation. Even a single company shipping a product might use different companies to move product from their facility to a port or consolidator. Following entry into the United States, the cargo is again subject to thousands of differing delivery paths until it reaches its destination.

Parallel with the movement of cargo is an information chain. It is initiated prior to the origination when the destination communicates its order for the cargo and arranges for payment of the goods or commodities and transportation.

In the case of pipelines, the supply chain is composed of far fewer nodes. Liquid commodities flow from point of origin to a consolidation point, and then are pumped into the pipeline flowing to the United States

SECURING THE SUPPLY CHAIN

Securing the supply chain immediately raises issues involving the security of infrastructure, facilities, carriers, people, cargo and information. Strategic planning for supply chain security must proceed with an understanding of the plans and efforts in other areas that are complementary. As an example, controlling access to the secure areas of our seaports is an aspect of supply chain security. The Transportation Security Administration (TSA) and the United States Coast Guard (USCG) are working together on transportation worker credentialing and updating mariner credentialing. TSA is also addressing this issue at airports as part of the effort to secure air passenger travel.

The security assessment crew traveling by air, land or sea cannot be considered only a travel security issue. The assessment of a container ship's crew or of a driver moving a truck into the secure area of a port are also supply chain security issues. The Department created the Screening Coordination Office (SCO) to integrate terrorist and immigration-related screening efforts, creating unified screening standards and policies. This office will foster new and innovative approaches to how the Department detects and interdicts threats through its traveler screening and worker credentialing programs.

The strategy to secure the supply chain reflects the larger security strategy of the Department. DHS utilizes a risk-based management approach in assessing potential threats and vulnerabilities, focusing our resources on the highest risk areas and working in partnership with the private sector, other government agencies, foreign governments and international organizations to improve security across a wide spectrum of areas. The supply chain security strategy is a component of this larger strategy and benefits from a linkage to other Department security initiatives.

The focus currently centers on how to ensure the integrity of the millions of maritime cargo containers entering the United States annually while continuing to facilitate legitimate trade. Given that 95 percent of the cargo tonnage that comes to the United States comes by sea, and that more than 11 million loaded marine containers entered U.S. seaports in FY2005 (a number expected to grow annually), this current 'center of gravity' for security efforts makes sense. However, as greater security is built into the supply chain, additional areas of emphasis will receive attention, including break-bulk cargoes, small package cargoes, etc. A layered, risk-based approach to the supply chain as a whole will axiomatically ensure this.

Additionally, terrorist organizations utilize the global transportation system to both generate and move funds. An early hallmark of Al- Qaeda was the network of corporations set up by Osama bin Laden when he lived in Sudan, which generated finances for the organizations activities.[1] Similarly, funds are generated through illegal

[1] Greenberg, Wechsler, Wolosky, *Terrorist Financing: Report of an Independent Task Force Sponsored by the Council on Foreign Relations*, copyright 2002, Council on Foreign Relations, 58 East 68th Street, New York, NY 10021.

activities such as narcotics trafficking. Then, funds are moved via money laundering schemes, directly carried by witting or unwitting individuals, or otherwise moved as a form of 'cargo.'[2] Thus, a full spectrum supply chain security program requires that even at the point of origin trade partners must be known and trusted to be moving what is claimed and the financial flows similarly tracked. Implementation of the latter is performed under Public Law 108-458, 118 Stat. 3638, (December 17, 2004), the Intelligence Reform and Terrorism Prevention Act of 2004 and other laws, by multiple federal entities, including U.S. Immigration and Customs Enforcement (ICE), the Director of National Intelligence, the Federal Bureau of Investigation (FBI), and the United States Secret Service (USSS), and does not fall under the scope of intent for this strategy. Further, explicit discussion of such financial tracking is highly sensitive in nature, potentially revealing law enforcement sensitive or classified intelligence methods and information. It bears noting; however, such enforcement-related information is a component of the broader risk-management efforts inherent in securing the supply chain.

The supply chain is global, crossing national boundaries and using all modes of transportation. The DHS uses a multi-layered risk-based management approach creating systems with multiple opportunities to identify and mitigate threats across the supply chain. The broad security responsibilities of the Department, a major reason for its creation, allows for the coordination and integration of multiple programs that cross organizational lines to improve our national security.

RISK ASSESSMENT

The international supply chain could be used to transport a wide spectrum of threats. The threats include nuclear, chemical, biological, radiological, and high explosive weapons, weapon components, narcotics, currency, stowaways, and prohibited or restricted commodities. From a risk management perspective, the threat with the greatest consequences would be the delivery of a nuclear weapon. A nuclear terrorist attack would have a devastating impact. Depending on where the attack occurred, estimates of deaths range as high as a million people and economic damage would run in the hundreds of billions of dollars. Threats involving weapons of mass destruction, particularly the nuclear threat, must be considered the preeminent risk. This threat is not limited to containerized cargo, but includes bulk, break-bulk and roll-on, roll-off (RORO) cargo.

Despite the existence of key nodes within the international cargo supply chain, there is no "one size fits all" solution for supply chain security. This is due to the complex nature of the international supply chain and the fact that supply chains vary between industries and between companies within the same industry. In addition, not every country that exports cargo to the United States poses the same risk. Not every maritime cargo container poses the same threat and should not be treated as such. Because of this, the Department has followed the risk-based approach for strengthening the international supply chain. The focus remains risk-based, identifying high-risk maritime cargoes before they are even loaded abroad, vetting and targeting vessels and other conveyances, cargoes, or even

[2] For a detailed analysis of terrorist financing, see Martin A. Weiss, *Terrorist Financing: U.S. Agency Efforts and Inter-Agency Coordination*, August 3, 2005, Congressional Research Service, The Library of Congress.

crew members for additional action while they are in transit, and minimizing overall risk exposure through scanning and inspections activities at the key nodes of the transportation system.

Multiple risk assessment methods exist, both qualitative and quantitative, but one of the simplest forms of risk equation is that of:

Threat Risk = Likelihood x Vulnerability x Consequence

Or, put another way, the likelihood of an incident (manmade or natural) combined with the strength or weakness of the target and what would happen as a result of the incident represents the risk the threat poses. To quantify the equation, assessments are necessary for all three elements.[3]

Each of the programs implemented within this DHS Strategy has at its base an appropriate risk management model used for targeting the activity to the highest risks within its area of impact in order to drive down the associated probability, vulnerability, or consequence. The key nodes within the supply chain have provided logical arenas for programs, and taken as a whole the programs integrate to provide for an end-to-end supply chain security methodology.

The overall risk management process applied is that recommended by the GAO Risk Management Framework[4], an iterative repeatable process that integrates strategies (such as this document) with risk assessments, countermeasure evaluations, implementation and measurement, and ongoing review of strategic objectives and constraints. Figure 2 displays the framework graphically.

The Department has followed the path of this risk management framework in its identification of supply chain security strategies specific to the transportation nodes within the supply chain.

A detailed analysis of the specific risk management protocols for each program is beyond the scope of this strategy, due in large part to the security sensitive or classified nature of such risk assessment models. However, the programs are integrated in terms of the overall supply chain through their application of risk management processes at critical nodes within the supply chain (e.g., security activities taken at ports for cargo destined for the United States and at domestic ports).

[3] Decker, Raymond J., *Homeland Security Key Elements of a Risk Management Approach*, Testimony before the Subcommittee on National Security, Veterans Affairs, and International Relations, House Committee on Government Reform, Friday, October 12, 2001, GAO-02-150T.

[4] Walker, David M, *Strategic Budgeting Risk Management Principles Can Help DHS Allocate Resources to Highest Priorities*, Testimony before the Subcommittee on Management, Integrations, and Oversight, Committee on Homeland Security, House of Representatives, Wednesday, June 29, 2005, GAO-05-824T.

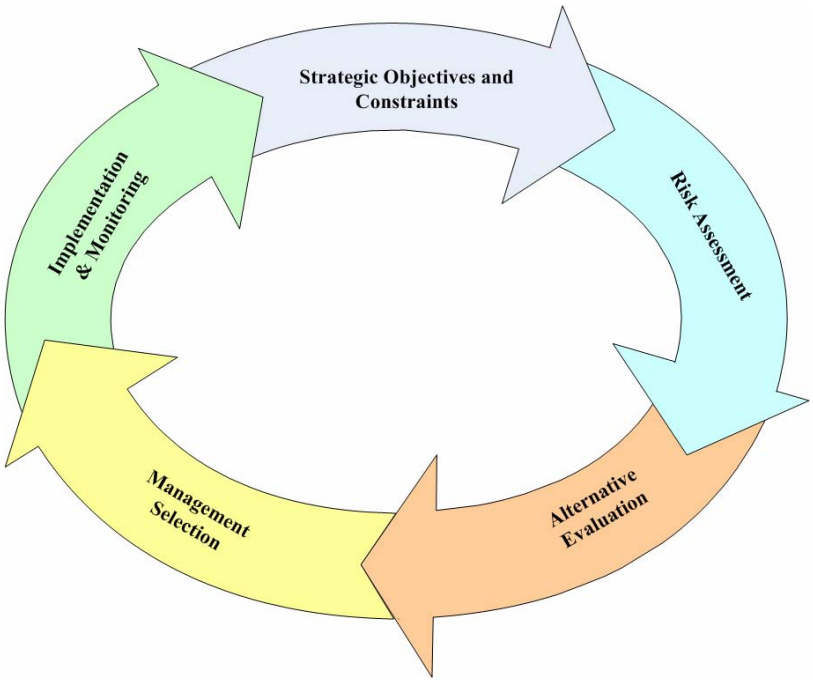


Figure 2: United States Government Accountability Office Risk Management Framework.

GOALS

The Department's Strategy has three primary goals:

GOAL 1: ENHANCE THE SAFETY AND SECURITY OF THE INTERNATIONAL CARGO SUPPLY CHAIN.

GOAL 2: FACILITATE GLOBAL COMMERCE WITHIN THE ENHANCED SECURITY FRAMEWORK.

GOAL 3: PROVIDE FOR THE RAPID RESUMPTION OF TRADE FOLLOWING AN INCIDENT WHICH DISRUPTS THE SUPPLY CHAIN.

To accomplish these goals, the Department has adopted a three-pronged approach. First, using end-to-end programs and initiatives, work with trading partners from cargo origin through final destination to foster global security. Second, target programs and initiatives toward natural security control points in the supply chain, such as ports of origination, transshipment, or entry in order to provide layers of detection and intervention. And, third, target programs and initiatives at conveyance modalities, such as vessels or containers, in order to increase the security of cargo while moving between cargo nodes.

STRATEGIC OBJECTIVES

Each of the three primary layers of the Department's approach to supply chain security is supported by a series of strategic objectives, implemented through programs, initiatives, and cooperative work in the international arena. Those strategic objectives are:

SO-1: Provide for end-to-end supply chain security by building trusted relationships and assisting trading partners and the trade community with enhancing their security systems.

SO-2: Provide incentives and benefits for supply chain partners who enhance their supply chain security, while recognizing that some benefits (e.g., increased security resulting in reduced cargo loss and/or reduced costs of doing business) are trade-driven issues.

SO-3: Advance security by promoting the development and implementation of international standards.

SO-4: Increase the availability and use of appropriate data in order to maintain complete awareness of the supply chain activities and target Department resources to the highest risk movements.

SO-5: Utilize provide WMD detection systems at ports of origin and entry, in order to provide for a defense in depth, layered system.[5]

SO-6: Expedite movement of low-risk shipments through the supply chain, while maintaining a level of detection such that even low-risk shipments are screened for high-consequence threats (e.g., WMD detection via RPMs).[5]

SO-7: Provide clear communications with the trade community and our international trading partners in order to facilitate recovery efforts.

SO-8: Ensure that data gathered during normal operations is also sufficient to allow for the management of resumption activities following a supply chain disruption.

SO-9: Promote technological development of detection systems which increase the probability of detection, decrease "false positive" detections, and expedite processing times in order to promote rapid trade movement.[5]

SO-10: Leverage key nodes in the supply chain to provide for specific scanning, screening, and inspections activities in order to detect and deter illicit use of the supply chain.[5]

SO-11: Develop systems which automate and expedite the use of Department resources.[5]

SO-12: Provide, or support development of, a robust cargo security system that will withstand a supply chain disruption, and rapidly resume pre-incident or near pre-incident status.

SO-13: Provide for a flexible, standardized response mechanism which includes processes to facilitate trade resumption in short and long term recovery operations.

SO-14: Promote development of modal-specific technologies and systems to ensure security of cargo while in transit.

SO-15: Leverage agreements with foreign partners to facilitate investigative activities related to the detection of illicit material in the supply chain.

[5] Specific technology development initiatives are driven by DHS Science and Technology (S&T) based upon an Implementation Planning Team (IPT) process in which S&T consults with customer bases and identifies targeted investment objectives. Specific information on IPT programs are protected information pending appropriate disclosure through appropriate contracting systems.

In order to achieve these objectives, the Department has implemented or is collaborating with other Federal Agencies on a number of initiatives, both domestically and in partnership with the international community. The programs and initiatives currently in place or being implemented are detailed in Section VIII, Strategic Elements, and are shown linked to each strategic objective in Table 1, below. (NOTE: The DOE Megaports Initiative is a DOE/NNSA program, not a DHS program)

Table 1: DHS Supply Chain Security Strategic Objectives and Implementing Programs

Strategic Objective:	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*Pg*
Customs-Trade Partnership Against Terrorism	■	■				■		■				■	■		■	64
Container Security Devices			■					■	■		■	■	■	■		66
24-Hour Rule				■		■		■			■	■	■			67
Container Security Initiative		■			■	■		■	■	■	■	■	■	■	■	68
Secure Freight Initiative		■		■	■	■	■	■	■	■	■	■	■		■	69
Automated Targeting Systems				■		■		■	■	■	■	■	■			70
DOE Megaports		■			■	■	■	■	■	■	■	■	■	■	■	71
Known Shipper Database	■			■		■		■		■	■	■	■			71
International Port Security Program	■		■	■			■			■		■	■	■		71
ISPS Code Implementation / Enforcement			■									■				72
Maritime Domain Awareness Program				■					■	■	■	■	■	■	■	72
Nationwide Automatic Identification System				■				■	■	■	■	■	■	■		72
Long Range Identification and Tracking of Vessels			■	■			■	■	■		■	■	■	■	■	73
Advance Notice of Arrival				■		■		■			■	■	■			74
Security and Response Operations					■				■	■	■	■	■		■	74
Domestic Maritime Security Regulations										■		■	■	■		75
Transportation Worker Identification Credentials									■	■		■	■	■		76

Strategic Objective:	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*Pg*
CBP Cargo Screening						■				■	■	■	■			76
Non-Intrusive Inspections and Radiation Scanning Technology				■	■	■		■	■	■	■	■	■	■	■	76
Certain Dangerous Cargo Tracking				■		■			■		■	■	■	■		77
Corporate Security Review (CSR)												■	■			78
HAZMAT Truck Tracking Program				■		■			■		■	■	■	■		78
Enhanced Security Measures for Highly Hazardous Materials												■	■	■		78
Federal Security Clearances for State Departments of Transportation												■				79
REAL ID Act									■			■				79
Hazmat Threat Assessment program						■						■	■			79
FLETC Training of Roadside Enforcement Officers												■	■			79
Freight Railroad Security Plans										■		■	■			80
Rail Protocols for Transportation of High-Risk Hazardous Materials										■		■	■	■		80
Air Cargo Security Programs						■			■	■	■	■	■	■	■	81
Strategy to Enhance International Supply Chain Security							■								■	N/A
Participation in International Forums (e.g, APEC Trade Recovery Workgroup)							■								■	N/A
ICE International Affairs & Trade Relations	■	■	■	■	■	■	■	■	■	■		■	■	■	■	N/A

III. SCOPE

This strategy addresses the security of cargo moving through the international supply chain from foreign point of origin to its arrival in the United States. The approach is based on the principal that supply chain security is best accomplished as an end-to-end process with specific checks and verifications at critical nodes. The focus of this strategy are shipments from a foreign origin to a United States destination out of a recognition of foreign sovereignty, with specific acknowledgement that our overseas trading partners set their own regimes and requirements for cargo inbound to their ports.

The strategy uses integral risk-based approaches to promote cooperation with our international trading partners in securing cargo and vessels destined for the United States and to secure our domestic ports. This strategy includes far-reaching initiatives to mitigate threats to our ports including the potential threats posed by vessels and international cargo arriving at these ports. In addition to protecting our ports and the supply chain, this strategy also includes protocols for the resumption of trade in the event of a transportation disruption or transportation security incident (TSI).

The DHS is the lead department for this strategy; however, its successful execution involves cooperation and coordination across a wide spectrum of organizations with different roles and responsibilities including Federal, State, and local governments, the private sector, foreign governments, and international organizations. This is necessary because of the multiple authorities having jurisdiction over domestic seaports and the global nature of the supply chain and marine transportation system.

This is a national strategy that works within and complements other national strategies and plans including, the National Security Strategy, the National Strategy for Homeland Security, the National Strategy for Transportation Security, the National Strategy for Maritime Security (and component plans), the NRP, the National Infrastructure Protection Plan, the Transportation Sector Specific Plan, and the National Maritime Transportation Security Plan. These national documents represent detailed guidance for specific segments of the supply chain and transportation infrastructure, and are neither superseded nor replaced by this strategy for their individual foci.

BOUNDARIES AND CONSTRAINTS

This strategy focuses specifically on the movement of cargo within the international supply chain. It does not address passenger movement, recreational vessels, or domestic port to domestic port commercial activity (e.g., commercial fishing).

This strategy does not provide, other than through broad-brush prioritization issues, for government coordination of the movement of individual containers for resumption of trade issues. Coordinating the movement of individual containers, and the cargo within them, is a business function. Where possible, coordination processes which provide for industry input to key decision makers managing response operations both in directly impacted areas and on regional/national scales are outlined so as to facilitate communications.

A significant constraint in the implementation of this strategy is the lack of direct control over a large portion of the supply chain. Specifically, supply chain security from the

cargo point of origin through drayage to a foreign port rests within the sovereignty of our trade partners. To address this, a number of the initiatives discussed in Section XIII, Strategic Elements are either voluntary programs developed to encourage enhanced security, bilateral agreements between the United States and specific trade partners, or formal international agreements such as the International Maritime Organization's (IMO) International Ship and Port Facility Security (ISPS) Code.

RELATIONSHIP TO OTHER PLANS AND STRATEGIES

Through multiple National Security Presidential Directives and Homeland Security Presidential Directives (NSPDs/HSPDs) tailored to the various transportation modes, the President underscored the importance of securing each segment of the transportation system. Each directive has resulted in the development of plans and strategies addressing different aspects of the system; they are mutually linked and reinforce each other.

Additionally, specific legislation has resulted in both strategies and tactical plans.

The overall inter-relationships of the multiple NSPD/HSPD and legislative plans are represented in figure 3. Their informational relationships to this strategy are delineated in Table 2, with specific details of each following in this section.

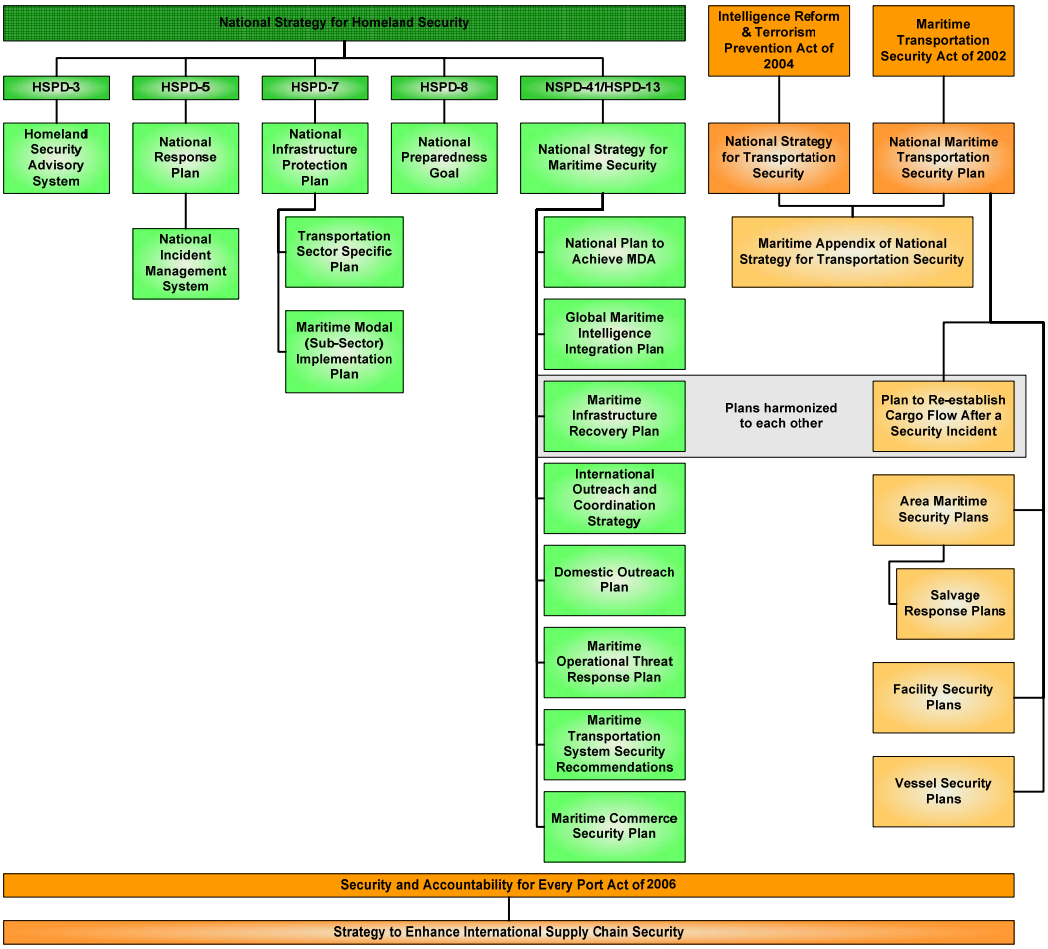


Figure 3: Relationships of National Security Strategies and Plans.

	NATIONAL STRATEGY FOR HOMELAND SECURITY (NSHS)									
	HSPD-3	HSPD-5		HSPD-7			HSPD-8	NSPD-41/HSPD-13		
	Homeland Security Advisory System	National Response Plan	National Incident Management System	National Infrastructure Protection Plan	Transportation Sector Specific Plan	Maritime Modal (Sub-Sector) Implementation Plan	National Preparedness Goal	National Strategy for Maritime Security	National Plan to Achieve MDA	Global Maritime Intelligence Integration Plan
Creates National Security Framework	■			■	■		■	■		
Provides Security Action Triggers	■									
Establishes Response Protocols		■	■			■	■			
Delineates Command and Control Roles		■	■	■	■	■				
Delineates Sector-specific Requirements		■				■				
Provides for Data and/or Intelligence Sharing		■	■	■	■				■	■
Provides Tactical Response Planning		■	■							
Provides Tactical Security Operations by Threat Condition										

Table 2: Principle Areas in which National Plans or Strategies Inform the Strategy to Enhance International Supply Chain Security

NSHS													
NSPD-41/HSPD-13						IRTPA '04	IRTPA '04/	MTSA '02					
Maritime Infrastructure Recovery Plan	International Outreach and Coordination Strategy	Domestic Outreach Plan	Maritime Operational Threat Response Plan	Maritime Transportation System Security Recommendations	Maritime Commerce Security Plan	National Strategy for Transportation Security	Maritime Appendix of National Strategy for Transportation Security	National Maritime Transportation Security Plan	Plan to Re-establish Cargo Flow after a Security Incident	Area Maritime Security Plans	Salvage Response Plans (Estimated for 2009 Completion)	Facility Security Plans	Vessel Security Plans

STRATEGIES

The President's **National Strategy for Homeland Security** (NSHS) clearly establishes that the United States will prevent our enemies from threatening us, our allies, and our friends with weapons of mass destruction (Section V). The strategy also clearly states that *"Promoting free and fair trade has long been a bedrock tenet of American foreign policy. Greater economic freedom is ultimately inseparable from political liberty. Economic freedom empowers individuals, and empowered individuals increasingly demand greater political freedom. Greater economic freedom also leads to greater economic opportunity and prosperity for everyone. History has judged the market economy as the single most effective economic system and the greatest antidote to poverty. To expand economic liberty and prosperity, the United States promotes free and fair trade, open markets, a stable financial system, the integration of the global economy, and secure, clean energy development."* These two goals form the bedrock of the Department's strategy for international supply chain security. We will ensure the facilitation of legitimate commerce while denying our enemies the use of the transportation infrastructure through a layered, risk-based effort.

The NSHS forms the umbrella under which all DHS homeland security efforts are conducted.

NATIONAL SECURITY PRESIDENTIAL DIRECTIVES/HOMELAND SECURITY PRESIDENTIAL DIRECTIVES

National Security Presidential Directives and Homeland Security Presidential Directives set national policies and executive mandates for specific programs and activities. The first was issued on October 29, 2001, shortly after the attacks on September 11, 2001, establishing the Homeland Security Advisory Council. It was followed by a series of directives regarding the full spectrum of actions required to "prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from incidents that do occur." A number of these are relevant to international supply chain security, and are discussed below in order of NSPD/HSPD number.

HSPD-3, Homeland Security Advisory System

Signed in March of 2002, HSPD-3 established the policy for the creation of the Homeland Security Advisory System (HSAS) to provide warnings to Federal, State, and local authorities, and to the American people in the form of a set of graduated Threat Conditions that escalate as the risk of threat increases. At each threat level, Federal departments and agencies are required to implement a corresponding set of protective measures to further reduce vulnerability or increase response capabilities during a period of heightened alert. The threat conditions also serve as guideposts for the implementation of tailored protective measures by State, local, tribal, and private sector security partners. The USCG employs Maritime Security (MARSEC) Levels to provide warnings to Federal, State and local authorities, the maritime industry, and the American public. MARSEC Level 1 aligns with HSAS Conditions Green, Blue, and Yellow. MARSEC Level 2 aligns with HSAS Condition Orange. MARSEC Level 3 aligns with HSAS Condition Red.

Many of the department and agency activities resulting from increases in the HSAS directly impact the international supply chain. As an example, an increase in inspections for in-bound cargo or vehicles at Ports of Entry may be triggered by an elevation in the Threat Condition.

HSPD-5, Management of Domestic Incidents

Signed in February of 2003, HSPD-5 required the Department to lead a coordinated national effort with other Federal departments and agencies; State, local, and tribal governments; and the private sector to develop and implement the National Incident Management System (NIMS) and the NRP.

The NIMS, implemented in March of 2004, provides for a nationwide template enabling Federal, State, local, and tribal governments; the private sector; and nongovernmental organizations to work together effectively and efficiently to prevent, prepare for, respond to, and recover from incidents regardless of cause, size, and complexity. The NIMS provides a uniform doctrine for command and management, including Incident Command, Multiagency Coordination, and Joint Information Systems; resource, communications, and information management; and application of supporting technologies.

The NRP, signed in December of 2004, was built on the NIMS template, signed by 29 Federal departments and agencies and 3 nongovernmental organizations, and fully implemented on April 14, 2005. It establishes a single, comprehensive framework for the management of domestic incidents (including threats) that require Department coordination and effective response by an appropriate combination of Federal, State, local and tribal governments; the private sector; and nongovernmental organizations.

The NRP provides for the framework for responses to international supply chain security incidents. Under the NRP, NIMS implementation in the event of a transportation disruption provides for the appropriate incident management framework for direct coordination of an effective response and recovery effort utilizing the protocols outlined in this strategy.

HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection

By signing Homeland Security Presidential Directive-7 (HSPD-7), the President established a national policy to identify and prioritize United States critical infrastructure and key resources and protect them from terrorist attacks. The definition of critical infrastructure as "*systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters*" clearly placed much of our port, transportation, and cargo infrastructure within the program, and resulted in the development of multiple plans:

- The **National Infrastructure Protection Plan (NIPP)** provides the unifying structure for the integration of Critical Infrastructure and Key Resources (CI/KR) protection into a single national program. The NIPP provides an overall framework for programs and activities that are currently underway in the various sectors, as well as new and developing CI/KR protection efforts.

The plan obligates each CI/KR sector to develop a Sector Specific Plan (SSP) to develop strategies that protect the nation's CI/KR under their purview, outline a coordinated approach to strengthen their security efforts, and determine appropriate programmatic funding levels.

The NIPP and its SSPs provide details regarding security of CI/KR which are integral to this strategy, as well as an extensive discussion of information sharing.

- The **Transportation SSP (TSSP)** and its supporting Modal Implementation plans and appendices establishes the Transportation Systems Sector's strategic approach based on the tenants outlined in NIPP and the principles of the Strengthening Surface Transportation Security Executive Order. This strategic approach describes the security framework that will enable sector stakeholders to make effective and appropriate risk-based security and resource allocation decisions.

HSPD-8, National Preparedness Goal

Signed in December, 2003, HSDP-8 mandates the development of a National Preparedness Goal aimed at helping entities at all levels of government build and maintain the capabilities to prevent, protect against, respond to, and recover from major events "to minimize the impact on lives, property, and the economy." This DHS Strategy, and especially its section on recovery, is a component of achieving the National Preparedness Goal

NSPD-41/HSPD-13, Maritime Security Policy

National Security Presidential Directive-41/Homeland Security Presidential Directive-13 (NSPD-41/HSPD-13) underscores the importance of securing the Maritime Domain, defined *as "All areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyance."* NSPD-41/HSPD-13 established a Maritime Security Policy Coordinating Committee – the first coordinating committee specifically tasked to address this issue – to oversee the development of a National Strategy for Maritime Security and eight supporting implementation plans:

- The **National Plan to Achieve Maritime Domain Awareness** (MDA) lays the foundation for an effective understanding of anything associated with the Maritime Domain and identifying threats as early and as distant from our shores as possible. Activities taken toward implementing the MDA plan have a direct correlation on supply chain security by providing information for strategic element risk assessment and the development of an overall common operating picture for management of the maritime domain.
- The **Global Maritime Intelligence Integration Plan** uses existing capabilities to integrate all available intelligence regarding potential threats to United States interests in the Maritime Domain. This integrated intelligence directly informs decision making under this strategy, including during strategic element risk management and during response/recovery operations.

- The **Maritime Operations Threat Response Plan** (MOTR) aims for coordinated United States government response to threats against the United States and its interests in the Maritime Domain by establishing roles and responsibilities, which enable the government to respond quickly and decisively. The MOTR-delineated roles and responsibilities are primarily focused on responding to threats; however, in the aftermath of an incident they will also inform national security activities affecting the international supply chain both at impacted and non-impacted ports and waterways.
- The **International Outreach and Coordination Strategy** provides a framework to coordinate all maritime security initiatives undertaken with foreign governments and international organizations, and solicits international support for enhanced maritime security.
- The **Maritime Infrastructure Recovery Plan** (MIRP) recommends procedures for the recovery of maritime transportation systems. These procedures form a part of the framework which this strategy recovery section operations within, though the NRP remains the overriding plan for implementation.
- The **Maritime Transportation System Security Recommendations** provides strategic recommendations to holistically improve the security of the marine transportation system.
- The **Maritime Commerce Security Plan** establishes a comprehensive plan to secure the maritime supply chain.
- The **Domestic Outreach Plan** engages non-federal input to assist with the development and implementation of maritime security policies resulting from NSPD-41/HSPD-13.

The National Strategy for Maritime Security (NSMS) and its supporting plans clearly articulate protective strategies and plans for the elements of the international supply chain stretching from ports and port facilities (including in many cases storage and deconsolidation nodes). Additionally, the NSMS provides for the extension of United States' efforts into the international sphere through such elements as domestic and global intelligence integration, development of Maritime Domain Awareness, and international outreach/coordination.

NATIONAL STRATEGY FOR TRANSPORTATION SECURITY

The Intelligence Reform and Terrorism Prevention Act of 2004 resulted in the development of the **National Strategy for Transportation Security (NSTS)**. Delivered to Congress on September 9, 2005, and called for by the 9-11 Commission, the NSTS is a classified document, and therefore its details cannot be discussed in a public forum. In general, it outlines the Federal government's approach, in partnership with State, local and tribal governments and private industry, to secure the United States' transportation system from terrorist threats and attacks, and prepare the Nation by increasing our capacity to respond if either occurs. It describes the policies the Federal government will apply to manage transportation risk and discusses how the government will organize its resources to secure the transportation system from terrorist attacks.

The NSTS applied a threat-based, risk-managed approach, using the factors of threat, vulnerability, and consequence, to evaluate asset categories in the six transportation modes: aviation; freight rail; highway; maritime; pipeline; transit, commuter and long-distance passenger rail. This evaluation identified asset categories at greatest risk for each mode, for which corresponding risk-based priorities were developed. The document also discusses the roles and missions of Federal, State, regional, local, and tribal authorities and the private sector, response and recovery responsibilities, and research and development requirements.

The **Maritime Appendix of the NSTS** is also known as the **National Maritime Transportation Security Plan (NMTSP)**, and was additionally required by the MTSA of 2002. The NMTSP is a Sensitive Security Information (SSI) document, and discussed in general below.

NATIONAL MARITIME TRANSPORTATION SECURITY PLAN, AREA MARITIME SECURITY PLANS, AND VESSEL/FACILITY SECURITY PLANS

The MTSA of 2002 mandated the development of the **National Maritime Transportation Security Plan (NMTSP)**. The NMTSP provides for efficient, coordinated and effective action to deter and minimize damage from a TSI involving maritime assets and infrastructure. This is accomplished through a three-tier maritime security planning regime, with the 'capstone' tier being the NMTSP itself. The second tier is comprised of **Area Maritime Security Plans (AMSPs)** developed by the local USCG Sector Commander acting as Federal Maritime Security Coordinator (FMSC) in cooperation with Area Maritime Security Committees (AMSCs) comprised of local stakeholders and government officials. The third tier is comprised of **Vessel** and **Facility Security Plans (VSPs and FSPs)** developed by facility and vessel owners and operators.

Specific to the international cargo supply chain, the NMTSP includes a Plan to Re-establish Cargo Flow after a Security Incident and, at all three tiers, provides for both preventative security and incident responses in the maritime domain.

At each level of the three-tier structure, the plans are based upon security risk assessments. VSPs and FSPs are based on private sector assessments which are required to be conducted as part of a five-year plan review and approval cycle. AMSPs are based upon an initial risk assessments conducted by the USCG, and a continuous risk assessment process (also conducted by the USCG). These risk assessment results are used to update the AMSPs as necessary, but at a minimum each AMSP is reviewed annually. On the national level, the continuous risk assessment results from each AMS process are merged and analyzed to develop a National Maritime Risk Assessment, with appropriate risk reduction measures developed to inform the security planning process.

Actual operations and responses are conducted under applicable organizational, community-based, and incident-specific operating, contingency, and response plans. These plans are folded under the NRP structures as supporting elements for the management of significant incidents.

The requirements of the MTSA were implemented through:

- 33 Code of Federal Regulations Part 101 - Maritime Security: General.

- 33 Code of Federal Regulations Part 103 - Maritime Security: Area Maritime Security.
- 33 Code of Federal Regulations Part 104 – Maritime Security: Vessels.
- 33 Code of Federal Regulations Part 105 – Maritime Security: Facilities.
- 33 Code of Federal Regulations Part 106 – Maritime Security: Outer Continental Shelf (OCS) Facilities.

In the international arena, the Safety of Life at Sea (SOLAS) Convention was amended on 12 December, 2002, to create the ISPS Code. The ISPS Code, through its Part A (mandatory) and Part B (recommended) sections, requires security standards and plans similar in scope to the MTSA requirements for the maritime facilities and vessels of signatory Nations.

RELATIONSHIP OF PLANS AND STRATEGIES TO THE INTERNATIONAL SUPPLY CHAIN

The overall relationships with this strategy of the various level plans and strategies discussed above and the international cargo supply chain are displayed graphically in figure 4, National Planning Structure as Related to the International Cargo Supply Chain.

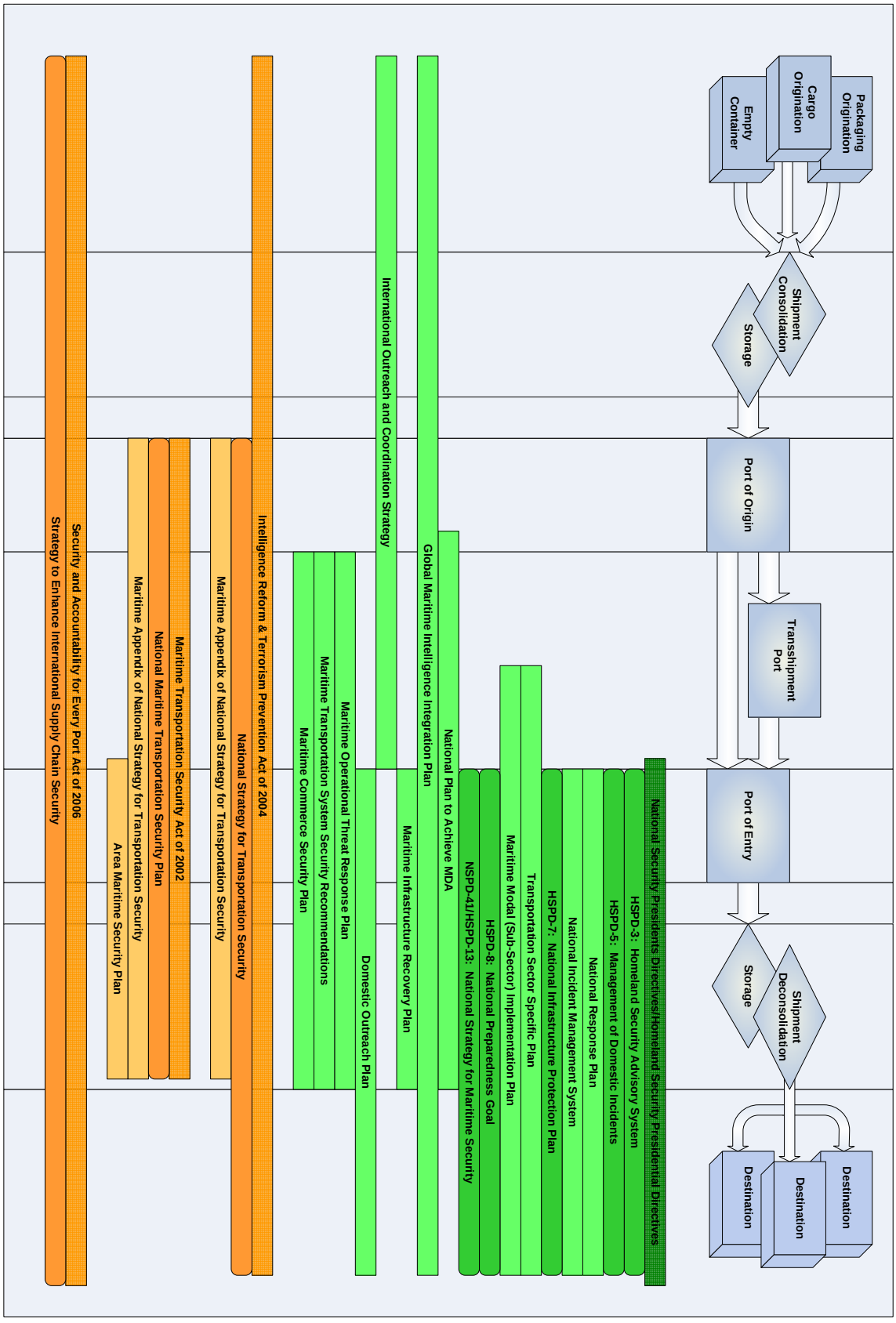


Figure 4: National Planning Structure as Related to the International Cargo Supply Chain.

IV. GUIDING PRINCIPLES

GUIDING PRINCIPLES

In its simplest form, international supply chain security requires that the cargo is secure from the point of origin, and that it remains secure during transit until the point of deconsolidation and domestic distribution. The framework to achieve this objective is best described in terms of four parts: (1) accurate data and information sharing, (2) secure cargo, (3) secure transit, and (4) international standards and compatible regulations.

(1) Accurate data in the form of advance electronic information is necessary to support the risk assessment of the cargo. This information is needed early in the process to identify high-risk cargo before it approaches the United States. In the case of containers, the information is needed before vessel loading in a foreign port. Information must also come from reliable sources with, wherever possible, first-hand knowledge.

(2) Information must be appropriately shared amongst United States government agencies and our trading partners, while simultaneously being safeguarded from improper disclosure.

(3) Secure cargo requires a procedure to ensure that the cargo conforms to the cargo information electronically transmitted to the authorities. This process connects first-hand knowledge of the cargo with the validation of the cargo information. This process also ensures that safeguards are in place to prevent unlawful materials (or persons) from being combined with the legitimate cargo. As an example, this process would involve security procedures to prevent unauthorized cargo and persons from being added to a container while it is being stuffed at a factory. This part also includes a risk management process that includes the scanning and/or inspection of cargo identified as high risk prior to loading at foreign ports and, in some cases, after arrival at the United States port.

(4) Secure transit is a procedure designed to ensure that cargo remains secure as it enters and moves through the supply chain. Successful implementation requires a method of detecting if security has been compromised during transit and a response protocol to be enacted in the event of such a compromise. Securing the conveyances and transportation facilities used in the movement of commerce is critical to maintaining the security of the cargo while it is in transit.

(5) Improvements to security within the first three parts of the framework must be addressed in a way that will ensure consistency and substantive improvements across the supply chain. This can only be achieved via engagement with the appropriate international organizations, e.g. the World Customs Organization (WCO) and the IMO and international trade partners in the development of standards. Standards are the only meaningful way that the government will be able to ensure that a high level of security across the supply chain can be expected and achieved.

THE ROLE OF TECHNOLOGY

Security technology is continuously evolving, not only in terms of capability but also in terms of compatibility, standardization, and integration with information systems. It is important to note that there is no single technology solution to improving supply chain security. As technology matures, it must be evaluated and adjustments to operational plans must be made. Priority should be given to effective security solutions that complement and improve the business processes already in place, and which build a foundation for 21st century global trade. A more secure supply chain also can be a more efficient supply chain.

Layered security with multiple opportunities to mitigate threats is better than a single point of defense. The ability to identify threats earlier in the supply chain is desirable; as such identification minimizes the need for 'end zone' response operations.

Technology plays a particularly important role in providing for screening of cargo at the critical nodes of the supply chain through data acquisition, delivery, and analysis (e.g., the secure transmission of cargo manifests). It also provides for certainty, through scanning and imaging of cargo at those nodes where multiple cargo flows join, (e.g., at ports of departure and entry). Such information built into normal business process as a preventative measure also leverages recovery capabilities by providing necessary information to key decision makers on the safety, security and prioritization of cargo.

ECONOMIC IMPACT

There is some debate about calculating the economic impact of even a brief closure of a major port. Some estimates run into the millions of dollars. Other estimates suggest that the economic cost would be in the billions. Nevertheless, there is agreement that any sustained closure of U.S. major ports will have a significant and rapidly expanding impact on the economy.[6] Since the United States represents nearly 20% of global maritime trade activity, any disruption in the United States would have repercussions affecting economic growth throughout the world.

The United States' response to a terrorist incident will not be an automatic shutdown of the nation's ports. Instead, a prudent and measured response will be taken based on an assessment, including available intelligence, of the specific incident. In all modalities, elevated security activities triggered by the HSAS or by modality specific threat conditions (e.g., MARSEC Levels in the maritime domain, or an increase in the HSAS for a transportation segment such as aviation) will be used to achieve an appropriate level of security such as is required to safeguard United States interests. International supply chain security must balance security requirements with the need to maintain the flow of international commerce. The response to an incident must not unreasonably hinder the free flow of goods.

The cost of securing the supply chain should not be so great that the transportation process becomes a barrier to free trade. Security requirements should be flexible enough

[6] By many estimates, the 11-day 2002 West Coast port lockout has been estimated at costing the U.S. economy close to $1 billion per day, and required roughly 6 months for full recovery.

to contain viable options that maintain maritime transportation security while connecting with emerging markets.

There are many obstacles in the path to ensuring the security of the international supply chain. The ability of terrorists and criminals to use any type of vulnerability to their advantage, combined with the need to keep international commerce flowing, makes supply chain security a difficult task. The sheer magnitude of the global supply chain constrains our ability as a Nation to prescribe and enforce security standards across its full breadth. The technologies to secure cargo during transit and detect threats hidden within cargo are still evolving. In spite of these challenges, significant progress has already been made. Still, there is much more to be done.

We all share a common interest in keeping destructive forces out of the supply chain. Through partnerships and international cooperation, the global supply chain will become secure and transparent. The more security gets integrated into common business practices and modern information systems, the better likelihood of sustaining increased levels of security.

ALL-HAZARDS PLANNING

Many types of incidents or threats may have a significant impact on the ability of vessels, vehicles, aircraft and cargo to move throughout the United States' transportation system. Such events may include transportation disruptions such as TISs[7], natural disasters, or even incidents such as vessels grounded in channels.

Incidents impacting the international supply chain may also not be centered in the United States, but still may require action to recover cargo flow. As an example, a tsunami could sever critical communications lines, impacting the ability of ports to assess the security of cargo or transmit the data associated with such assessments. Redundancy of systems and a unified approach to managing the supply chain will help minimize the impacts from such events.

A common, all-hazard compatible approach will be used by all United States agencies for the incident management of transportation disruptions. Where boundaries delineated under enabling authorities may be narrowly construed towards specific hazards (e.g., hazardous materials and the Comprehensive Environmental Response, Compensation, and Liability Act, P.L. 96-510, 94 Stat. 2767, December 11, 1980), all-hazard compatibility is intended to encourage and promote a core approach for response and recovery. This allows responders to optimize and harmonize plans, coordination, procedures, and resources across hazard categories, in keeping with the central philosophy of the NRP.

SCALABILITY

The character of incident management measures for prevention, response and recovery to enable the resumption of trade following an incident will vary according to the character, scale and scope of the threat, incident, or incidents.

[7] Defined in 46 U.S.C. 70101(6) as "…a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area."

Incident scale may range from a local transportation disruption that is capable of being managed through steady-state coordination and communication with resources on hand to wide-area catastrophic events that necessitate full-scale national level engagement with extensive infrastructure and trade recovery periods.

NATIONAL INCIDENT MANAGEMENT SYSTEM (NIMS)

Incident command actions associated with response or recovery to domestic incidents which impact the ability of cargo and transportation through the supply chain will be carried out in accordance with NIMS principles. NIMS was mandated in HSPD-5 to provide for interoperability and compatibility among Federal, State, and local capabilities, and includes a core set of concepts such as the Incident Command System (ICS), Unified Command Structure (UCS), incident information reporting, etc. The NMTSP and the MIRP describe how recovery management is carried out at the various levels, and reflects the organizational constructs detailed in the NRP, as well as the use of ICS and UCS procedures.

In accordance with NIMS, incidents are generally handled at the lowest jurisdictional level possible. In instances regarding marine transportation infrastructure, a Federal agency may act as a first responder and may provide direction or assistance specific to its statutory authorities and responsibilities.

At the local level, the incident command and management organization is located at the Incident Command Post (ICP) once implemented. Designated incident management officials and responders from Federal, State, local, and tribal agencies, as well as private sector and nongovernmental organizations, are typically on site at the ICP. When multiple command authorities are involved in a response or recovery effort, the ICP may be led by a Unified Command, which is comprised of officials who have jurisdictional authority or functional responsibility for the incident under appropriate law, ordinance, or agreement.

For significant events, elements of the NRP may be activated to provide support to the incident command organization on scene. If designated, the Principal Federal Official (PFO) and/or the Federal Coordinating Officer (FCO) represent the Secretary of Homeland Security and are responsible for overall coordination of support to the incident through the Joint Field Office (JFO).

At the national level, overall incident information sharing, operational planning, recovery, and deployment of federal resources are coordinated by the National Operations Center (NOC) and its component elements. Agencies with primary responsibility for movement of vessels and cargo (i.e. the USCG and U.S. Customs and Border Protection, CBP) will form the core of a specific national level interagency coordinating body specifically to monitor the status of the marine transportation system and provide direction to field commanders to expedite MTS recovery and resumption of trade.

CONCEPTS OF PREVENTION, RESPONSE, AND RECOVERY

PREVENTION

Prevention, or the actions taken to avoid incidents or to intervene to stop incidents from occurring, is a primary goal of the Department of Homeland Security. The Department merges beneath one roof the capability to anticipate, preempt and deter threats to the homeland whenever possible, and the ability to respond quickly when such threats do materialize. Prevention involves actions taken to protect lives and property as well as to secure cargo and trade.

Effective prevention strategies require the coordination of all involved parties, at all levels of government and the private sector, in all nations. This is especially true in the international cargo supply chain, where cargo, most often owned and transported by the private sector, originates under the sovereignty of one nation, moves through international space (air and sea), and then enters the sovereignty of another nation. Effective, end-to-end security must be as cooperative in nature as the actual cargo movement itself.

RESPONSE

Response for the purposes of resumption of trade consists of measures, operations and activities in incident areas that are needed to set the stage for the recovery activities described in the following section. Response includes the determination and assessment of infrastructure impacts and transportation disruptions to support assessment of the primary and secondary effects of an incident, including supply chain interdependencies.

Prevention activities will continue during response in incident and non-incident areas to the extent necessary as a supporting security activity consistent with prevailing HSAS or MARSEC Levels and threats as resources permit.

Recovery planning and operations will be conducted concurrently with response activities and will be initiated as soon as practicable following an incident.

Sector-Specific Agency (SSA) CI/KR responsibilities under the NIPP and the NRP CI/KR Annex relative to response will normally be conducted through the NRP and NIMS structures within incident areas and, to the extent necessary in non-incident areas, through steady-state coordination and communications or as otherwise prescribed by national policy or directives.

RECOVERY

Recovery consists of measures, programs, and other activities that are planned and applied across CI/KR Sectors consistent with the NRP CI/KR Support Annex to facilitate and support the resumption of trade within incident areas (those areas directly impacted by the effects of the incident) and non-incident areas (those areas indirectly affected by the consequences of the incident). Recovery also consists of measures and actions needed to resume trade at normal levels following the threat of an incident which necessitates heightened security and possible transportation restrictions affecting cargo flow.

Recovery measures are characterized as those that are needed to provide initial recovery and to provide the basis to facilitate and support long-term recovery and mitigation activities where required, as characterized below. For incident areas, a primary focus will be on restoring infrastructure sufficiently to enable restoration of transportation and trade/cargo flow. In non-incident areas, a primary focus will be on offsetting loss of functionality and capacity resulting from the incident(s) and mitigation of the associated disruption of transportation and trade.

Initial recovery

Differing from response, initial recovery is that period where impacted infrastructure and supporting activities within the incident area have been returned to service and are capable of operations or service at some level. Initial activities, policies or mitigation strategies aimed at recovery are considered to be achievable in 90 days or less.

Outside the incident area, measures and supporting activities, including prevention, may have been redirected, reallocated or supplemented to support response and recovery operations in incident areas. This may result in increased operations and service tempos outside the incident area, to accommodate the near-term indirect effects of the incident.

Long-term Recovery

Long-term recovery is defined as that period in which infrastructure and supporting activities have been returned to pre-incident conditions or service or have the capacity or capability to operate or provide service at pre-incident levels. Activities, policies or mitigation strategies aimed at long-term recovery may take longer than 90 days. Long-term recovery as used here parallels long-term recovery measures associated with NRP Emergency Support Function (ESF) #14.

Outside the incident area, measures and supporting activities, including prevention, may have been redirected, reallocated or supplemented to support long-term recovery operations in incident areas. This may result in increased operations and service tempos outside the incident area, to accommodate long-term indirect and permanent effects of the incident.

Restoration

The extent to which infrastructure has individually or collectively recovered or the extent to which trade has recovered is characterized as the level of restoration. It is expressed as a percentage or other suitable metric of pre-incident conditions or service, or as the capacity to operate or provide service at pre-incident levels, as appropriate. This characterization recognizes that an incident or incidents can potentially have profound effects on trade patterns and business interests and that a return to pre-incident condition or service does not necessarily mean that there will be a corresponding return to pre-incident trade patterns and conditions, although facilitation of the latter is a goal of this strategy.

Recovery Division of Responsibility

Each Department, agency, and organization is responsible for the recovery of its own infrastructure and for the recovery of infrastructure that it directly administers, operates or maintains.

The Federal, State, local, and tribal governments will provide recovery services and assistance in support of affected communities and stakeholders in accordance with NRP constructs and applicable laws, regulations and policies.

Private Sector owners and operators have the primary responsibility for recovery of infrastructure that these parties own and operate and for trade conducted by these parties.

RESOURCES

It is presumed that individual agencies are budgeted and staffed in accordance with their required duties, including those associated with response and recovery activities. Agency resources will be assigned and allocated during steady-state (normal operations or long-term recovery) activities according to standing practices and polices.

Resources will be assigned and allocated during events as per the NRP, and in accordance with individual agency policies.

National and international level engagement with stakeholders will be conducted as necessary to identify and prioritize resource needs and allocations and to adjudicate and resolve competing interests and disputes.

V. CONSIDERATIONS AND ASSUMPTIONS

In developing this strategy, the following broad-based assumptions were considered:

- Agencies are currently appropriately resourced for their responsibilities, including limited surge capabilities. Such surge capabilities will likely result in reprioritization of duties and resources from normal operating conditions.
- Agencies have internal plans for surge operations which include the movement of personnel and resources to theaters of operations impacted by incidents or threats and to areas not impacted in order to address increased operational tempos resulting from incidents or threats.
- The international cargo supply chain is, by its very nature, a bi-directional system. Cargo carriers, across the modes, arriving in a country and delivering cargo will also carry outbound cargo.
- Trade will continue to expand in the coming years. As an example, current estimates for West Coast trade show a doubling of container traffic within the next decade.
- Expansion of trade will result in expansion of infrastructure to accommodate the cargo flow. Expansion of infrastructure affords the opportunity to embed security systems and procedures into the expanded business practices and infrastructures. If done properly, such expansion with embedded security systems can represent increases in both security and efficacy.
- Enhanced delivery of security data (e.g., imaging and scanning data) will enable more informed targeting of cargo. However, such data must in itself be protected in order to ensure proprietary information is not inappropriately disseminated.
- On any given day, roughly 370,000 containers of cargo are on board vessels destined for the United States. This means that approximately one third of all the vessel capacity serving U.S. international containerized commerce is already loaded and en route. In order to address this in-transit cargo, data used for supply chain security management and risk assessment (e.g., "10+2" data) must be sufficient for trade continuity and resumption efforts.
- Improvements to radiation/nuclear scanning capabilities at critical nodes will afford greater assurances toward international nonproliferation goals. Such increases in capabilities will require technological maturation.
- Increased container security will have the greatest immediate impact on cargo security as a whole, but such security must include not only the container itself, but also the data associated with the container and the infrastructure that handles the container.
- The promotion of established relationships with trusted members of the supply chain (e.g., WCO Framework of Standards Authorized Economic Operators and CBP C-TPAT participants) will continue to develop and serve as a means of enhancing the security of cargo and validity of cargo information. This approach enhances overall security while facilitating legitimate trade.

- Security systems and procedures must balance the facilitation of legitimate trade with the need for security.
- Domestic incident prevention, response and recovery planning must be addressed both from the perspective of the directly threatened or impacted (or attacked) site(s) or region(s) as well as the areas that are not directly impacted by the incident, but may be affected in terms of adjustments in security measures, operational restrictions, or trade flow to meet the national strategic purpose. Domestic incidents may disrupt the United States supply chain including the flow of commerce to and through United States ports (and beyond) in several ways.
    - An incident affecting the labor force, such as a Chemical/Biological/ Radiological/Nuclear/Explosive (CBRNE) event, may adversely impact labor availability at key nodes or across broad areas, disrupting the supply chain.
    - An incident may cause damage to CI/KR within the supply chain, such as transportation system infrastructure and rolling stock, which must be repaired, otherwise rendered operable, or replaced in order to move goods.
    - Operational restrictions or security measures may be enacted in order to stabilize and mitigate the effects of an incident, and to prevent further incidents.
    - Such operational restrictions or security measure may directly impact the ability of the transportation system to handle cargo. For instance, MARSEC Level 3 will result in container port facilities being able to operate only at an extremely limited basis, being ineffective at handling normally scheduled operations, and unlikely to handle any significant additional operations which may be diverted to them.
- Prevention, response and recovery actions will take place at the national, regional, and local levels, depending upon the character and scale of the incident, and other pertinent factors.
- In order to facilitate trade and commerce while still providing appropriate security measures and managing response and restoration activities, it is the policy of the DHS and its component agencies to take measured and deliberate steps toward increases in security resulting from incidents or threats. It is not the Department policy, for instance, to close all ports automatically as a result of an incident involving a single port or multiple ports. However, this does not preclude such closures, or increases in across-the-board security requirements, in situations warranting such.

VI. STRATEGY DEVELOPMENT METHODOLOGY

This strategy was developed using a multi-tiered approach.

The Department brought together subject matter experts from component agencies and divisions including the USCG, CBP, TSA, DHS Policy, Science and Technology, Domestic Nuclear Detection Office, Grants and Training, and Preparedness to create an initial draft of the strategy.

This draft was then subjected to an extensive review process involving internal staff across the Department, interagency reviews with non-DHS agencies, consultation with the private sector through advisory committees, including: the National Maritime Security Advisory Committee and the Commercial Operations Advisory Committee, and consultation with international trade partners, principally selected by volume of trade with the United States (e.g., APEC).

After a final round of corrections, taking into account the recommendations and requests of the reviewers and consultants, the strategy was subject to a formal review by DHS components and submitted for formal Department review.

Figure 5: Plan Development/Review Process.

Upon approval of the strategy by the Department, it was submitted for a final round of interagency clearance and Office of Management and Budget Review.

Recognizing that the SAFE Port Act requires this strategy to be submitted as an initial report 270 days after enactment and calls upon the Department to submit a final report not later than 3 years after the date of initial submission, further development and consultation is anticipated. Multiple technologies, programs and pilot projects, including some required by the SAFE Port Act itself, are expected to be developed or mature during this period and the results will be used to inform the final strategy. (These programs, projects, and technologies are discussed in detail in Section VIII, Strategic Elements.) Following initial release, further consultation in developing the final strategy is anticipated with:

- The private sector through formal trade organizations (e.g., the World Shipping Council and Port Authorities, including coastal and inland ports).
- State and local stakeholders.
- International organizations, including the IMO, the WCO, the International Labor Organization, and the International Organization for Standardization.

VII. ROLES, RESPONSIBILITIES, AND AUTHORITIES

The international cargo supply chain, when viewed from origin to destination, is a constant series of transitions from national and intranational agency jurisdictions to international spaces (water and air) to national and intranational agency jurisdictions. In many cases, these jurisdictions overlap as well, with differing spheres of influence converging on supply chain nodes. For instance, both the USCG and CBP have specific jurisdictions within a port. Further complicating this maze of jurisdictions are cases where the cargo is transshipped, moving into and out of yet another nation's controls. And every nation addresses its commerce, transportation, customs, and maritime systems differently.

As an example, following a fictitious container shipment from a foreign nation to the United States, the container will most likely:

- Be subject to the commerce and transportation laws and regulations of the originating nation as it is manufactured, containerized, and transported to a port.
- Move into jurisdiction of that nation's customs organization.
- Move from Customs jurisdiction to that of the Nation's maritime administration.
- Depart the nation's maritime jurisdiction and enter international waters, where it would be subject to multiple international agreements and where the vessel could conceivably be under the control of a second nation serving as the vessel's Flag State.
- Move into the jurisdiction of the USCG.
- Arrive at the port and transfer into the jurisdiction of CBP.
- Be released by CBP for further transport, subject to the jurisdiction of the Department of Transportation and the TSA.

And finally upon release by CBP, the cargo becomes subject to State and local jurisdictions.

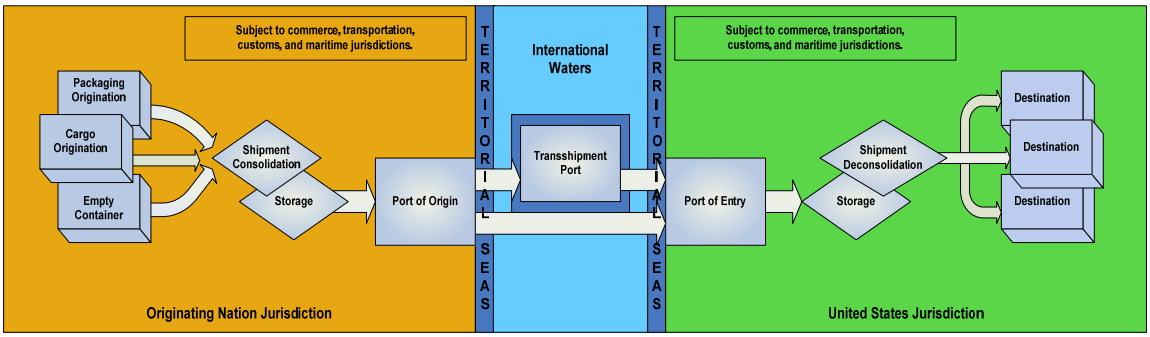


Figure 6: Possible international jurisdictions impacting supply chains.

Due to the complexities of the supply chain, and the differences in jurisdictional assignments made by our trade partners, it has been Department policy to negotiate necessary agreements bilaterally, nation by nation, or where appropriate to work with international organizations. An example of the former is the customs CSI agreement negotiated between CBP and Singapore. An example of the latter is the ISPS Code, created in partnership with the IMO and its signatory nations.

From a strictly United States perspective, below are descriptions of the primary functional responsibilities of United States entities with responsibilities involving cargo, trade, customs, and security, including restoration activities in the event of a transportation disruption. Coordination of involved agencies in a disaster response scenario will be in accordance with the NRP.

The general jurisdictions of Federal agencies are displayed graphically in figure 7, Primary Supply Chain Federal Agency Jurisdictions.

UNITED STATES FEDERAL GOVERNMENT FUNCTIONAL RESPONSIBILITIES

DEPARTMENT OF HOMELAND SECURITY (DHS)

The United States DHS is a Cabinet level department of the Federal government of the United States with the responsibility of protecting the territory of the United States from terrorist attacks and responding to natural disasters.

The Department works to protect the United States within, at, and outside its borders. Its goal is to prepare for, prevent, and respond to domestic emergencies, particularly terrorism.

In addition to its 17 component branches and directorates, the Department includes:

- TSA.
- CBP.
- United States Citizenship and Immigration Services.
- United States Immigration and Customs Enforcement (ICE).
- The USSS.
- The Federal Emergency Management Agency (FEMA).
- The USCG.

In responding to supply chain disruptions, the Department:

- Acts as the PFO for domestic incident management.
- Coordinates Federal maritime infrastructure recovery operations within the United States.
- Coordinates Federal government resources.

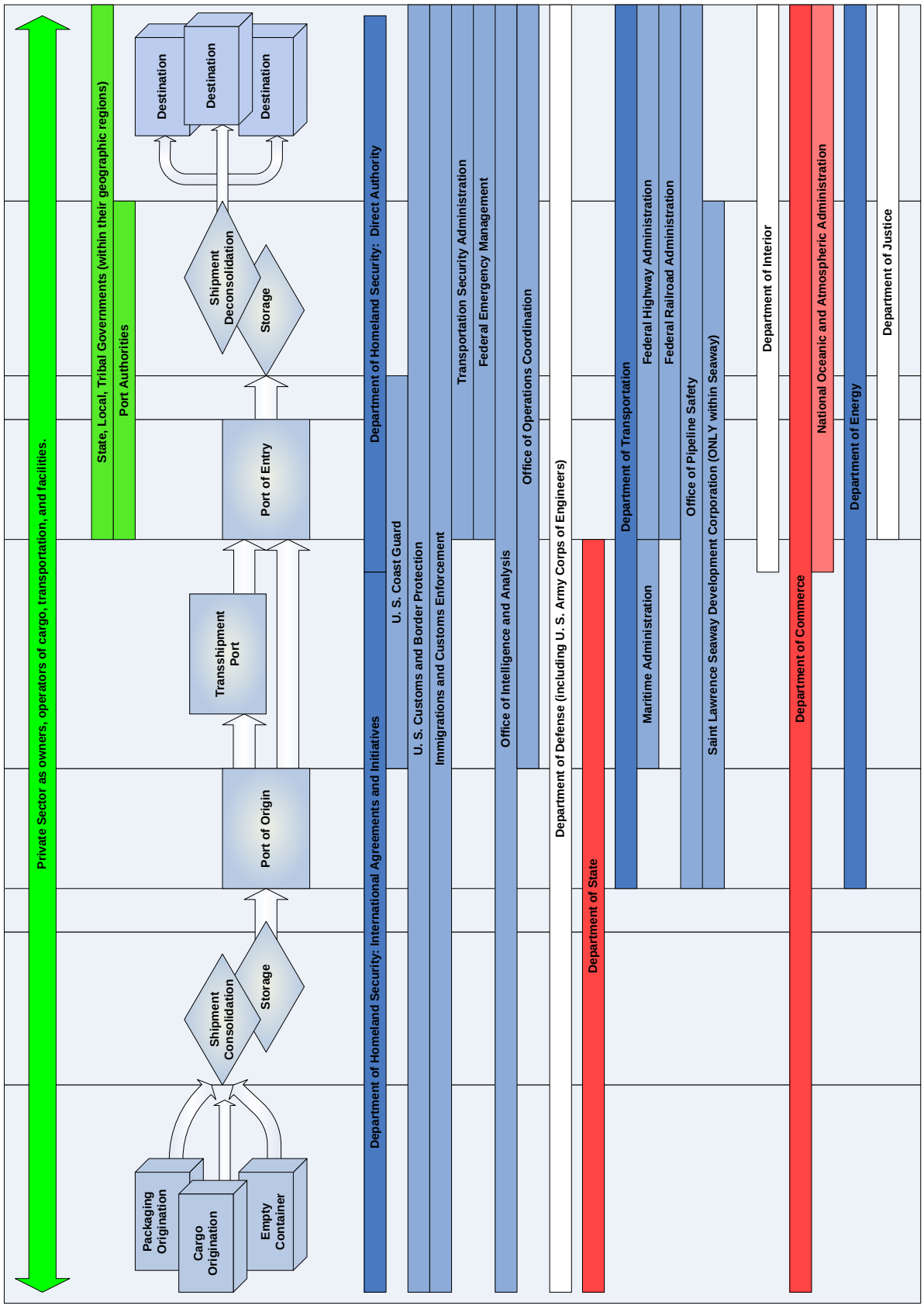


Figure 7: Primary Supply Chain Federal Agency Jurisdictions.

UNITED STATES COAST GUARD (USCG)

The USCG is a multimission, maritime service within the Department and one of the five services of the Nation's armed forces. Its core roles are to protect the public, the environment, and United States economic and security interests in any maritime region in which those interests may be at risk, including international waters and America's coasts, ports, and inland waterways.

The USCG provides unique benefits to the Nation because of its distinctive blend of military, humanitarian, and civilian law-enforcement capabilities. To serve the public, the USCG has five fundamental roles:

- **Maritime Safety:** Eliminate deaths, injuries, and property damage associated with maritime transportation, fishing, and recreational boating.
- **Maritime Security:** Protect the U.S. maritime domain and the Marine Transportation System, and deny their use and exploitation by terrorists as a means for attacks on U.S. territory, populations, vessels, and critical infrastructure. Uphold U.S. maritime sovereignty and enforce U.S. law, international conventions, and treaties. Defend U.S. national interests in the maritime domain against hostile acts through military action.
- **Maritime Mobility:** Facilitate maritime commerce and eliminate interruptions and impediments to the efficient and economical movement of goods and people, while maximizing recreational access to and enjoyment of the water.
- **National Defense:** Defend the Nation as one of the five United States armed services. Enhance regional stability in support of the National Security Strategy, utilizing the USCG's unique and relevant maritime capabilities.
- **Protection of Natural Resources:** Eliminate environmental damage and the degradation of natural resources associated with maritime transportation, fishing, and recreational boating.

The routinely inspects and assesses the security of United States ports in accordance with the MTSA of 2002, the Ports and Waterways Safety Act, and other pertinent legislation. Every regulated United States port facility is required to establish and implement a comprehensive security plan that outlines procedures for controlling access to the facility, verifying credentials of port workers, implementing the Transportation Worker Identification Credential (TWIC), inspecting cargo for tampering, designating security responsibilities, training, and reporting of all breaches of security or suspicious activity, among other security measures. Working closely with local port authorities and law enforcement agencies, the USCG regularly reviews, approves, assesses and inspects these plans and facilities to ensure compliance. In addition, also as required by the MTSA, the USCG assesses the effectiveness of anti-terrorism measures in foreign ports.

In responding to supply chain disruptions, the USCG:

- Acts as the Principle Federal Official when directed by the Secretary of DHS or as the Senior Federal Official (SFO).

- Participates in recovery planning by developing AMSPs and collaborating with maritime stakeholders, especially AMSCs and other local groups such as Area Committees and local harbor safety committees.
- Through its Captains of the Port (COTP):
    - As FMSC, develops and maintains AMSPs.
    - Controls vessel traffic, movement and anchorage.
    - Establishes and enforces safety and security zones.
    - Controls access to the operations of facilities under, in, or adjacent to waters subject to the jurisdiction of the United States.
    - Actively manages risks to ports by directing the movement of vessels, as necessary.
    - Furnishes available personnel, equipment or other resource support as requested, consistent with overriding mission responsibilities and within the capabilities of assigned resources.
    - Provides port security measures to reduce potential threats and to ensure integrity of the existing infrastructure system, including boarding of certain high-risk vessels prior to port entry.
    - Tracks Notice of Arrival (NOA) information from ships entering U.S. waters and ensures changes to NOAs are provided to the appropriate USCG and CBP officials at alternate ports of entry.
    - As part of AMSPs, in coordination with appropriate stakeholders and other government agencies, monitors maximum vessel, cargo and inter-modal throughput within the respective area of responsibility.
    - Considers temporary easements for the enforcement of regulations to facilitate re-routing of cargo, including NOA lead times.
    - Supports CBP in the screening and evaluating of cargo movement into and out of the United States.
    - Collects, integrates, and analyzes maritime intelligence concerning threats to vessels, ports and maritime infrastructure.
    - In support of ESF #3 of the NRP, coordinates with the U.S. Army Corps of Engineers (USACE) for marking and removal of obstructions declared to be hazards to navigation.
    - Ensures the safety of navigation and security of an Area of Responsibility (AOR) prior to reopening of any waterway.
    - Coordinates post-incident assessments and the reporting of maritime Critical Infrastructure/Key Asset status and intermodal linkages.
    - Assists in debris and contaminated debris management activities.

- Acting as FMSC, the COTPs will develop salvage response plans for inclusion in the AMSPs, and be responsible for their implementation when completed.
- Provides support as outlined in ESFs #1, #3, #4, #9, #10, #11, #13 of the NRP and any other tasking as directed by the Secretary of DHS.

UNITED STATES CUSTOMS AND BORDER PROTECTION (CBP)

CBP's mission is to prevent terrorists and terrorist weapons from entering the United States by eliminating potential threats before they arrive at our borders and ports. CBP uses a multi-layered risk-based approach to ensure the integrity of the supply chain. This includes the use of advanced information under the 24-Hour Rule, use of the Advanced Targeting System to identify high-risk cargo before it is loaded onto vessels destined for the United States, the C-TPAT program, the CSI and the use of Non-Intrusive Inspection (NII) technology and mandatory exams for all high-risk shipments, either at the foreign port or upon arrival into the United States.

In responding to supply chain disruptions, CBP:

- Provides on-scene resources.
- In coordination with appropriate stakeholders and other government agencies, monitors maximum available vessel, cargo and inter-modal throughput within the respective area of responsibility.
- Screens and evaluates cargo, crew, and passenger movements into and out of the United States.
- Conducts hands-on physical boardings of vessels with highest-risk cargo.
- Inspects and searches vessels, conveyances, persons, and cargo within the Customs territory of the United States.
- Detains and seizes vessels, cargo, and contraband.
- Authorizes lading and unlading of cargo.
- Determines the admissibility of persons arriving in the United States.
- Collects, integrates and analyzes maritime intelligence concerning cargo and inter-modal shipments.
- Identifies and mitigates security risks within the supply chain through the C-TPAT program.
- Authorizes the redirection of conveyances to other ports.
- Monitors NOA changes provided by the USCG.
- Ensures changes to the Trade Act of 2002 cargo manifests and Advance Passenger Information System (APIS) manifests for passengers and crewmembers are provided to the appropriate USCG and CBP officials at alternate ports of entry.

- In coordination with the Department of State, works with the governments of Canada, Mexico, and Panama to make arrangements for the diversion of United States bound cargoes and passengers.
- Detects and identifies chemical, biological, radiological, and nuclear materials through the employment of detection technology and coordination with CBP Weapons of Mass Destruction Teleforensics Center.
- Reviews cargo information and inspects cargo containers in advance of loading in foreign ports, through the CSI.
- When requested, in accordance with agency authority and the availability of resources, redeploys appropriate personnel, equipment, air and marine assets and other resources in support.
- Participates in the recovery activities of AMSCs.
- Supports the USCG so as to ensure compatibility, as appropriate, between the C-TPAT and requirements promulgated by the USCG.
- Supports the USCG in planning transportation disruption recovery, as appropriate.
- Provides support as outlined in ESFs #1, #8, and #13 of the NRP and any other tasking as directed by the Secretary of DHS.

Immigration and Customs Enforcement (ICE)

The mission of ICE is to protect America and uphold public safety by identifying criminal activities and eliminating vulnerabilities that pose a threat to the U.S. borders, as well as enforcing economic, transportation and infrastructure security. By protecting national and border security, ICE seeks to eliminate the potential threat of terrorist acts against the United States. ICE hosts the largest international investigative component in DHS, interacting with the international community on behalf of multiple agencies through investigations of immigration and customs violations, representation with international organizations, conducting international training and guiding repatriation efforts.

ICE Attachés work within U.S. Embassies to implement and support multiple maritime security initiatives (i.e. CSI/C-TPAT/SFI) in foreign countries.

In responding to supply chain disruptions, ICE:

- Provides essential resources in domestic recovery operations. ICE provides personnel and communications capabilities in coordination with Federal, State and local law enforcement agencies to affected areas through ESF #13, Public Safety and Security, under the NRP.
- Utilizing the sustainable framework of the NRP, NIMS and ICS, ICE's National Incident Response Unit (NIRU) coordinates and oversees ICE operations which support the prevention, preparedness, response and recovery plans for critical and significant incidents, such as natural disasters, man-made or accidental disasters, or other national emergencies or incidents of national significance.

- Cooperates with foreign governments in the coordination of DHS foreign investigations, and provides homeland security intelligence to the DHS Office of Intelligence and Analysis, other government entities, and our State, local, and private sector partners.
- Works with foreign counterparts to combat transnational crimes involving national security by conducting investigations of entities that pose a potential risk of terrorism and/or criminal activities before they arrive at U.S. ports of entry.
- Participates in Border Enforcement Security Task Forces (BESTs) and Integrated Border Enforcement Teams (IBETS), with foreign government counterparts to increase capability to detect and interdict harmful goods and materials.
- Serves as a point of contact for the import/export community and is involved in several DHS trade security programs such as the CSI and the C-TPAT.
- Serves as a point of contact in Canada and Mexico in the Security and Prosperity Partnership (SPP) and the Secure Border Initiative (SBI).

TRANSPORTATION SECURITY ADMINISTRATION (TSA)

TSA provides oversight of the security for the highways, pipelines, mass transit systems, ports and the 450 United States airports.

Along with the USCG, TSA has the responsibility for the implementation and enforcement of the TWIC program. The TWIC, as required by 46 U.S.C. § 70105, will be issued to all U.S. merchant mariners, all individuals who require unescorted access to the secure areas of facilities and vessels, as well as other individuals specified in the law who meet the security screening requirements for issuance. It will give facility and vessel security personnel reasonable assurance that individuals holding a TWIC are who they say they are, and that they have successfully completed a background check. The TWIC program will reduce the risk of unauthorized persons gaining access to secure areas of port facilities or vessels where cargo operations occur.

In responding to supply chain disruptions, TSA:

- Develops policies on the identification of critical assets and infrastructure for air and surface transportation modes and provides support for the maritime sector.
- Coordinates with USCG, CBP, DOT, and private industry to facilitate redirection of conveyances to other ports.
- Following a TSI, in coordination with other appropriate stakeholders and government agencies, monitors maximum available vessel, cargo and inter-modal capacity, to take steps to ensure the continuity of cargo flow.
- Monitors the investigation of TSIs to obtain lessons learned to improve risk mitigation plans and programs.
- Supports the USCG in maritime security planning.
- Supports the USCG and participates as a member of the AMSCs.

- Coordinates intelligence functions with other entities of the DHS through the Transportation Security Operations Center (TSOC).
- Provides support as outlined in NRP and accompanying ESFs.

FEDERAL EMERGENCY MANAGEMENT AGENCY

The FEMA's mission is to coordinate the response to a disaster which has occurred in the United States and which overwhelms the resources of State and local authorities. The governor of the State in which the disaster occurred must declare a state of emergency and formally request from the President that the Federal government respond to the disaster. The only exception is when an emergency or disaster occurs on federal property or to a federal asset, for example the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma in 1995.

While on-the-ground support of disaster recovery efforts is a major part of the organization's charter, the agency provides State and local governments with experts in specialized fields and funding for rebuilding efforts and relief funds for individual citizens and infrastructure, in conjunction with the Small Business Administration (SBA). The FEMA also assists individuals and businesses with low interest loans and provides funds for the training of response personnel throughout the United States and its territories as part of its preparedness efforts.

The FEMA is responsible for the issuance and maintenance of the NRP and the implementation of the NIMS.

In responding to supply chain disruptions, the FEMA provides disaster relief resources in accordance with the NRP.

OFFICE OF INTELLIGENCE AND ANALYSIS (I&A)

I&A identifies and assesses a broad range of intelligence information concerning current and future threats against the United States. The office is responsible for issuing timely warnings and advisories for the full spectrum of terrorist threats against the homeland, including physical and cyber events. In responding to supply chain disruptions, I&A will review threats to the Maritime Transportation System and marine CI/KR, and provide intelligence to key decision makers within the Department.

OFFICE OF OPERATIONS COORDINATION

The Office of Operations Coordination conducts joint operations across all organizational elements, coordinating activities related to incident management. It employs all Department resources to translate intelligence and policy into action and oversees the NOC which collects and fuses information from more than 35 Federal, State, territorial, tribal, local, and private sector agencies.

DEPARTMENT OF DEFENSE (DOD)

The Department of Defense is responsible for defending the United States while helping to promote American interests globally.

During a supply chain disruption, DOD may, at the direction of the President or the Secretary of Defense, provide Defense Support of Civil Authorities (DSCA), in accordance with the NRP and consistent with the law, to Federal, State, and local response and recovery activities while simultaneously defending the United States directly and globally. In addition, local military commanders and responsible officials of other DOD components are authorized to take necessary action to response to requests of civil authorities to save lives, prevent human suffering, or mitigate great property damage. All such necessary action is referred to as "immediate response

UNITED STATES ARMY CORPS OF ENGINEERS (USACE)

The Corps' mission is to provide engineering services to the United States, including:

Planning, designing, building and operating dams and other civil engineering projects, designing and managing the construction of military facilities for the Army and Air Force, and providing design and construction management support for other Defense and Federal agencies.

During a supply chain disruption, the USACE may:

- Provide rapid dredging capability through contracting or from the Federal Dredging Fleet.
- Conduct high-tech channel surveys.
- Conduct pre- and post-incident assessments of public works and infrastructure.
- Provide technical assistance to include engineering expertise, construction management and contracting, and real estate services.
- Provide emergency repair of damaged public critical infrastructure and facilities.
- Remove and dispose of contaminated and uncontaminated debris from public property.
- Provide appropriate representation to the IIMG and/or NOC when requested by Office of Assistant Secretary of Defense for Homeland Defense.
- Assist with the restoration and operation of inland waterways, ports and harbors to include assisting in restoring the transportation infrastructure.
- Obtain heavy equipment and/or demolition services.
- Support mass care operations by providing ice, water and temporary housing.
- Provide for the temporary restoration of damaged public utilities by providing equipment, supplies and technical assistance.
- Provide recovery assistance to radiological and nuclear incidents to include radiological surveys, gross decontamination, site characterization, contaminated water management and site remediation.
- Assist with incident environmental impact assessments by providing technical environmental expertise.

- Deploy emergency power teams for power-system restoration.
- Provide long-term community recovery through community planning, civil engineering and hazard risk assessment expertise.
- Support the development of national strategies and plans for the restoration of public facilities and infrastructure.
- Provide operational support for mobilization centers (including mobile command centers), staging areas, and distribution sites for all infrastructure and engineering service commodities.
- Support the USCG and participate as an advisory member of the AMSCs.

DEPARTMENT OF STATE (DOS)

Within the Executive Branch, the Department of State is the lead United States foreign affairs agency, and its head, the Secretary of State, is the President's principal foreign policy advisor. The Department advances United States objectives and interests in the world through its primary role in developing and implementing the President's foreign policy. The Department also supports the foreign affairs activities of other U.S. government entities including the Department of Homeland Security. It also provides an array of important services to U.S. citizens and foreign nationals seeking to visit or immigrate to the United States

As stated by the Department of State, its purposes include:

- Protecting and assisting United States citizens living or traveling abroad.
- Assisting U.S. businesses in the international marketplace.
- Coordinating and providing support for international activities of other United States agencies (local, State, or Federal government), official visits overseas and at home, and other diplomatic efforts.
- Keeping the public informed about U.S. foreign policy and relations with other countries and providing feedback from the public to administration officials.

In the event of a supply chain disruption, DOS:

- Coordinates requests for, and offers of, transportation assistance from foreign governments.
- Provides support to the various ESFs, when activated, as outlined in the NRP.
- Notifies foreign governments as appropriate of impacts on commerce.
- In coordination with CBP, works with the governments of Canada, Mexico, and Panama to make arrangements for diversion and facilitation of U.S. bound cargo and passengers.
- Provides support to DHS Maritime and Cargo Security Programs.
- Provides awareness and monitoring of cargo subject to export control.

DEPARTMENT OF TRANSPORTATION (DOT)

The mission of the DOT is to serve the United States by ensuring a fast, safe, efficient, accessible and convenient transportation system that meets our vital national interests and enhances the quality of life of the American people, today and into the future.

During a supply chain disruption, DOT may be called upon to:

- Prioritize and/or allocate civil transportation capacity.
- Manage hazardous material containment response and movement.
- Assess damage to the Nation's rail, pipeline and highway systems.
- Provide technical expertise and assistance for repair and restoration of transportation infrastructure.
- Provide advice and assistance on the transportation of contaminated materials.
- Provide engineering personnel and support to assist in damage and structural assessments, structural inspections and debris.
- Provide support to the various ESFs, when activated, as outlined in the NRP.

MARITIME ADMINISTRATION (MARAD)

MARAD administers financial programs to develop, promote, and operate the U.S. Merchant Marine; conducts research and development activities in the maritime field; regulates the transfer of U.S. documented vessels to foreign registries; maintains equipment, shipyard facilities, and reserve fleets of Government-owned ships essential for national defense; operates the U.S. Merchant Marine Academy; and administers a Grant-In-Aid Program for State-operated maritime academies.

During a supply chain disruption, MARAD may be called upon to:

- Provide transport of critical supplies, bulk goods, or heavy equipment/supplies to ports adjacent to disaster areas through the use of the National Defense Reserve Fleet.
- Obtain priority use and allocation of port facilities and services, shipping services, containers and chassis under the Defense Production Act.
- Maintain personnel readiness services needed to operate active and reserve vessels.
- Assist the USCG in the development of recovery assessments and plans.
- Participate in the activities of the AMSCs.

FEDERAL HIGHWAY ADMINISTRATION (FHWA)

The Federal Highway Administration (FHWA) is a division of the U.S. Department of Transportation that specializes in highway transportation. The agency's major activities are grouped into two programs: the Federal-aid Highway Program and the Federal Lands Highway Program.

FHWA's role in the **Federal-aid Highway Program** is to oversee federal funds used for constructing and maintaining the National Highway System. Under the **Federal Lands Highway Program**, FHWA provides highway design and construction services for various federal land-management agencies.

In addition to these programs, FHWA performs research in the areas of automobile safety, congestion, highway materials and construction methods.

In the event of a transportation system disruption, the FHWA will provide highway management expertise and emergency funds or loans for the repair or reconstruction of highways.

FEDERAL RAILROAD ADMINISTRATION (FRA)

The Federal Railroad Administration promulgates and enforces rail safety regulations; administers railroad assistance programs; conducts research and development in support of improved railroad safety and national rail transportation policies; provides for the rehabilitation of Northeast Corridor rail passenger service; and consolidates government support of rail transportation activities.

In response to a transportation system disruption, the FRA will provide railway system expertise as well as direct loans and guarantees to rehabilitate inter-modal or rail equipment or facilities.

ST. LAWRENCE SEAWAY DEVELOPMENT CORPORATION (SLSDC)

The Saint Lawrence Seaway Development Corporation (SLSDC) is a wholly owned government corporation created by statute in 1954, to construct, operate and maintain that part of the St. Lawrence Seaway between the Port of Montreal and Lake Erie, within the territorial limits of the United States. Trade development functions of the SLSDC aim to enhance Great Lakes/St. Lawrence Seaway System utilization without respect to territorial or geographic limits.

In response to a transportation system disruption, the SLSDC may establish, operate, and maintain vessel traffic services; and control or supervise vessel traffic.

OFFICE OF PIPELINE SAFETY (OPS)

The Office of Pipeline Safety (OPS) is the federal safety authority for the Nation's 2.3 million miles of natural gas and hazardous liquid pipelines. The OPS has the mission to ensure the safe, reliable, and environmentally sound operation of the pipeline transportation system.

In the event of a transportation system disruption that impacts pipelines, OPS may:

- Provide emergency funds or loans for the repair or reconstruction of pipelines.
- Coordinate recovery operations at the federal level for cross-modal aspects of a TSI.
- Respond to requests for waivers of restrictions to meet emergency requirements for pipeline operation.

DEPARTMENT OF INTERIOR (DOI)

The Department of the Interior (DOI) is the Nation's principal conservation agency. Their mission is to protect America's treasures for future generations, provide access to our Nation's natural and cultural heritage, offer recreation opportunities, honor our trust responsibilities to American Indians and Alaska Natives and our responsibilities to island communities, conduct scientific research, provide wise stewardship of energy and mineral resources, foster sound use of land and water resources, and conserve and protect fish and wildlife.

During a response to a transportation disruption, DOI will serve as a lead trustee to protect natural resources and provide tribal nation liaisons per ESF #3 of the NRP.

DEPARTMENT OF COMMERCE (DOC)

The historic mission of the Department of Commerce is "to foster, promote, and develop the foreign and domestic commerce" of the United States. This has evolved, as a result of legislative and administrative additions, to encompass broadly the responsibility to foster, serve, and promote the Nation's economic development and technological advancement.

During a response to a transportation disruption, DOC can:

- Provide expertise in the management of cargo and trade issues.
- Provide economic impact data and analysis.
- Provide to appropriate government agencies awareness and monitoring of cargo subject to export controls.

NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION (NOAA)

The National Oceanic and Atmospheric Administration conducts research and gathers data to support its mission to understand and predict changes in the Earth's environment, and conserve and manage coastal and marine resources to meet our nation's economic, social and environmental needs.

NOAA warns of dangerous weather, creates and maintains charts of U.S. waters, guides the use and protection of ocean and coastal resources, and conducts research to improve understanding and stewardship of the marine environment.

A Commerce Department agency, NOAA provides these services through five major organizations: the National Weather Service, the National Ocean Service, the National Marine Fisheries Service, the National Environmental Satellite, Data, and Information Service, and the Office of Oceanic and Atmospheric Research; as well as numerous special program units. In addition, NOAA research and operational activities are supported by the Nation's seventh uniformed service, the NOAA Corps, a commissioned officer corps of men and women who operate NOAA ships and aircraft, and serve in scientific and administrative posts.

In response to a transportation system disruption, NOAA may:

- Assess port and regional level maritime, seafloor, weather and infrastructure conditions.
- Provide scientific support coordination, as outlined in the National Contingency Plan (40 C.F.R. § 300).
- Provide awareness and monitoring information on maritime, seafloor weather and infrastructure conditions to appropriate incident management officials.

DEPARTMENT OF ENERGY (DOE)

The Department of Energy's overarching mission is to advance the national, economic, and energy security of the United States; to promote scientific and technological innovation in support of that mission; and to ensure the environmental cleanup of the national nuclear weapons complex. The Department's strategic goals to achieve the mission are designed to deliver results along five strategic themes:

- Energy Security: Promoting America's energy security through reliable, clean, and affordable energy.
- Nuclear Security: Ensuring America's nuclear security.
- Scientific Discovery and Innovation: Strengthening U.S. scientific discovery, economic competitiveness, and improving quality of life through innovations in science and technology.
- Environmental Responsibility: Protecting the environment by providing a responsible resolution to the environmental legacy of nuclear weapons production.
- Management Excellence: Enabling the mission through sound management.

The Department of Energy National Nuclear Security Administration (DOE/NNSA) developed and is implementing its Second Line of Defense Program, which includes the Megaports Initiative, and is a full partner in the SFI. Under the Megaports Initiative, DOE/NNSA works with other countries to enhance their ability to scan container cargo at major international seaports for nuclear and other radioactive materials. DOE/NNSA provides radiation detection equipment and associated communications systems to host nation authorities, provides training on the use of the equipment, and provides technical support to host nation officials and law enforcement officers. In return, the Department requires that data be shared on detections and seizures of nuclear or radiological material that resulted from the use of the equipment provided.

In the event of a transportation system disruption, the DOE may:

- Provide information and security assurances via Megaports and SFI.
- Assist in the economic assessment of damage to energy infrastructure.
- Consider the use of the Strategic Petroleum Reserve.

DEPARTMENT OF JUSTICE (DOJ)

It is the mission of the Department of Justice to enforce the law and defend the interests of the United States according to the law; to ensure public safety against threats foreign and domestic; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; and to ensure fair and impartial administration of justice for all Americans.

In the event of a transportation disruption related to or caused by a terrorist act or a terrorist threat, DOJ:

- Through the FBI, pursuant to statutory authority and Presidential directions, is the lead Federal agency for investigations of terrorist acts or terrorist threats by individuals or groups inside the United States, or directed at U.S. citizens or institutions abroad, where such acts are within the Federal criminal jurisdiction of the Unites States, and will conduct and coordinate all federal law enforcement and criminal investigation activities during a terrorist incident.
- Coordinates the activities of other members of the federal law enforcement community to detect, prevent, preempt, and disrupt terrorist attacks against the United States.
- Consults with other Federal agencies with regard to the temporary easement of enforcement regulations to facilitate the reconstruction of critical infrastructure and resumption of commerce.

STATE, LOCAL AND TRIBAL GOVERNMENT

State, local and tribal governments under NIMS principles have responsibility for incident management response and recovery efforts immediately after an incident. To manage their responsibilities, many of these government agencies currently have pre-established emergency response plans in place. However, recovery plans, especially for maritime infrastructure recovery and restoration of cargo flow, are not as prevalent. Many States engage individual task force groups to manage a myriad of disaster scenarios and response situations.

Due to the fact that the responsibilities, capabilities and organizational structures vary from agency to agency, it is difficult to establish specific functional responsibilities that each may be able to provide for recovery from a transportation disruption. However, to coordinate the Federal, State, local and tribal government relationships, the following generic list of functional responsibilities for recovery that State, local, and tribal governmental agencies may perform was developed for the Maritime Infrastructure Recovery Plan, and is applicable for those portions of the international cargo supply chain falling within State, local, and tribal government jurisdictions.

STATE GOVERNMENTS

- Coordinate State resources to address recovery.
- Make, amend, and rescind orders and regulations under certain emergency conditions in support of recovery efforts as appropriate.

- Communicate to the public recovery aspects of an emergency within State jurisdiction.
- Assist people, businesses, and organizations of the State cope with the consequences of recovery.
- Encourage participation in mutual aid and implement authorities for the State to enter into mutual aid agreements with other States, tribes, and territories to facilitate resource-sharing.
- Coordinate requests for federal assistance when it becomes clear that State or tribal capabilities will be insufficient or have been exceeded or exhausted.
- Engage in voluntary exchange of information with other Federal, State, local and tribal government agencies.
- Participate in various advisory committees and task forces regarding recovery management.
- Assist in the assessment of the economic impact created by a security incident.
- Assist in the identification of recovery resources and assets.
- Provide resources as requested and as appropriate.

LOCAL GOVERNMENTS

- Perform emergency first-responder activities as appropriate.
- Coordinate local resources to address recovery.
- Suspend local laws and ordinances, (dependent upon State and local law), under certain emergency conditions in support of recovery efforts as appropriate.
- Communicate to the public any type of declared emergency within local jurisdiction.
- Assist people, businesses, and organizations in the local area to cope with the consequences of any type of declared emergency and its recovery considerations.
- Negotiate and enter into mutual aid agreements with other jurisdictions to facilitate resource-sharing.
- Request State and, if necessary, Federal assistance through the governor of the State when the jurisdiction's capabilities have been exceeded or exhausted, or otherwise as appropriate.
- Engage in voluntary exchange of information with other Federal, State, local and tribal government agencies.
- Participate in various advisory committees and task forces regarding recovery management.
- Assist in the assessment of the economic impact created by a security incident.
- Assist in the identification of recovery resources and assets.

- Provide resources as requested and as appropriate.

TRIBAL GOVERNMENTS

- Coordinate local resources to address recovery.
- Suspend tribal laws and ordinances as appropriate.
- Communicate any type of declared emergency within tribal jurisdiction.
- Assist people, businesses, and organizations to cope with the consequences of any type of declared emergency.
- Negotiate and enter into mutual aid agreements with other tribes/jurisdictions to facilitate resource-sharing.
- Request State and Federal assistance through the governor of the State when the tribe's capabilities have been exceeded or exhausted.
- Deal directly with the federal government. (Although a State Governor must request a Presidential disaster declaration on behalf of a tribe under the Stafford Act, Federal agencies can work directly with tribes within existing authorities and resources.)
- Engage in voluntary exchange of information with Federal, State, local and other tribal government agencies.
- Participate in various advisory committees and task forces regarding recovery management.
- Assist in the assessment of the economic impact created by a national TSI.
- Assist in the identification of recovery resources and assets.
- Provide resources as requested and as appropriate.

PRIVATE SECTOR

As the owners and operators of the vast majority of the infrastructure, assets, commodities, etc., of the international cargo supply chain, the private sector plays the most important role in ensuring its overall security. During normal operations, while government entities legislate, regulate, validate and inspect, the private sector must operate the supply chain safely, securely, efficiently, and at a profit.

As a component of their business, private sector entities have responsibility for planning, operations, and advisory aspects relating to recovery of cargo movement and trade flow, and the restoration of passenger flow.

Following an incident that triggers implementation of this strategy, the Federal government will facilitate the restoration of commerce and recovery of the marine transportation in concert with private sector contingency planning. This will be accomplished in accordance with the plans already outlined in Section III, but most especially the NRP and the various infrastructure recovery plans.

To assist the private sector prepare for this role, the DHS advocates the following:

- Private sector owners and operators of vessels and facilities subject to United States government regulation are encouraged to expand their business continuity plans to include recovery operations as part of required planning pursuant to federal regulations, if such planning has not already been completed.
- Owners and operators of vessels and facilities not subject to United States government regulation are encouraged to establish recovery operations and business continuity plans, in coordination with appropriate trade partners.
- All private sector recovery operations plans should include (1) a plan for evacuation, (2) adequate communications capabilities, and (3) a plan for business continuity.
- All private sector recovery operations plans should consider the existing American National Standard on Disaster/Emergency Management and Business Continuity Programs (NFPA 1600), which contains minimum criteria for disaster management and guidance in the development of a program for effective disaster preparedness response and recovery.

To assist in the development of recovery operations plans and other contingency planning, the following *Business Roundtable* guidance documents are recommended for private sector continuity of operations plan development:

- Committed to Protecting America: A Private-Sector Crisis Preparedness Guide, March 2005.
- Committed to Protecting America: CEO Guide to Security Challenges, February 2005.

It is anticipated that the private sector will implement business continuity plans/recovery operations plans on their own accord, based on incident information provided by the Federal government. Information that may influence the decision to implement contingency plans and divert or redirect cargo and/or the conveyances include: national priorities; military requirements; MTS restrictions; and the expected duration of those restrictions.

To facilitate restoration of the flow of commerce, the following list of functional responsibilities that the private sector may perform was developed as part of the Maritime Infrastructure Recovery Plan, and is applicable within the overall cargo supply chain:

- Engage in voluntary exchange of information about recovery operations plans with other potentially affected private sector entities and the Federal government to mitigate potential congestion at non-incident site ports following the diversion of vessel traffic.
- Participate in various maritime industry stakeholder professional organizations and advisory committees such as the AMSCs regarding recovery management and contingency planning.
- Assist in the assessment of economic impact.
- Assist in the identification of recovery resources and assets.

- Provide resources to assist in recovery, as appropriate.
- When requested by the National Maritime Security Advisory Committee (NMSAC) during planning for recovery or the Sector Specific Agency (SSA) during actual recovery management operations, provide experts for advising on recovery management, especially regarding maritime salvage capability.
- Participate in pilot programs to test the effectiveness of the Federal government to communicate recovery activities to the private sector.
- Using existing information-sharing mechanisms such as the National Infrastructure Coordinating Center (NICC), AMSCs, Transportation Sector Coordinating Councils and Information Sharing and Analysis Centers (ISAC), communicate situational and operational information as well as physical asset capabilities for mitigation management.

AUTHORITIES

The international supply chain, given its complex set of interlocking jurisdictions and authorities, is subject to a vast collection of laws and regulations at the Federal, State, and local levels. Similarly, response efforts involved with supply chain disruptions fall under the provisions of further authorities. Below are some of the primary laws which provide the Federal government and its agencies with authority to regulate supply chain security and response to disruptions. Additional, secondary authorities are found in Appendix C.

HOMELAND SECURITY ACT OF 2002[8]

This Act established a cabinet-level department headed by a Secretary of Homeland Security with the mandate and legal authority to protect the American people from the continuing threat of terrorism. Congress assigned DHS the primary missions to:

- Prevent terrorist attacks within the United States.
- Reduce the vulnerability of the United States to terrorism at home.
- Minimize the damage and assist in the recovery from terrorist attacks that occur.
- Ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland.

CRITICAL INFRASTRUCTURE INFORMATION ACT OF 2002[9]

Enacted as part of the Homeland Security Act, this Act creates a framework that enables members of the private sector and others to voluntarily submit sensitive information regarding the Nation's Critical Infrastructure/Key Resources to DHS with the assurance that the information, if it satisfies certain requirements, will be protected from public disclosure.

[8] Public Law 107-296, November 25, 2002, 116 Stat. 2135. It is codified mainly at 6 U.S.C. 101 et seq.
[9] The CII Act is presented as Subtitle B of Title II of the Homeland Security Act (sections 211-215) and is codified at 6 U.S.C. 131 et seq.

AVIATION AND TRANSPORTATION SECURITY ACT OF 2001[10] (ATSA)

ATSA provides broad Federal authority for security in all modes of transportation. The authorities of ATSA are delegated by the Secretary of Homeland Security to the Administrator of the TSA. The Administrator "shall be responsible for security in all modes of transportation" including civil aviation security and all "security responsibilities over other modes of transportation that are exercised by the Department of Transportation." The Administrator is given an array of specific authorities which carry out this broad responsibility. Specific enumerated responsibilities and authorities include:

- Ensuring the adequacy of security measures for the transportation of cargo.
- Requiring background checks for transportation security personnel.
- Overseeing the implementation, and ensuring the adequacy, of security measures at transportation facilities.
- Receiving, assessing, and distributing intelligence information related to transportation security.
- Assessing threats to transportation.
- Developing policies, strategies, and plans for dealing with threats to transportation.
- Making other plans related to transportation security, including coordinating countermeasures with appropriate departments, agencies, and instrumentalities of the United States.
- Enforcing security related regulations and requirements.
- Issuing, rescinding, and revising such regulations, including issuing regulations and security directives.
- Serving as the primary liaison for transportations security to intelligence and law enforcement communities.
- Identifying and undertaking research and development activities necessary to enhance transportation security.

ROBERT T. STAFFORD DISASTER RELIEF AND EMERGENCY ASSISTANCE ACT (STAFFORD ACT)[11]

The Stafford Act provides comprehensive authority for response to emergencies and major disasters – natural disasters, accidents, and intentionally perpetrated events. It provides specific authority for the Federal government to provide assistance to State and local entities for disaster preparedness and mitigation, and major disaster and emergency assistance. Major disaster and emergency assistance includes such resources as:

- The provision of Federal resources, in general.
- Medicine, food, and other consumables.
- Work and services to save lives and restore property, including:
    - Debris removal.

[10] Public Law 107-71, November 19, 2001, 115 Stat 597.
[11] Public Law 93-288, 88 Stat. 143 (May 22, 1974), as amended, codified at 42 U.S.C. 68.

- Search and rescue; emergency medical care; emergency mass care; emergency shelter; and provision of food, water, medicine, and other essential needs, including movement of supplies or persons.
- Clearance of roads and construction of temporary bridges.
- Provision of temporary facilities for schools and other essential community services.
- Demolition of unsafe structures that endanger the public.
- Warning of further risks and hazards.
- Dissemination of public information and assistance regarding health and safety measures.
- Provision of technical advice to State and local governments on disaster management and control.
- Reduction of immediate threats to life, property, public health and safety.

- Hazard mitigation.
- Repair, replacement, and restoration of certain damaged facilities.
- Emergency communications, emergency transportation, and fire management assistance.

DISASTER MITIGATION ACT OF 2000

This Act amends the Stafford Act by repealing the previous mitigation planning provisions (Section 409) and replacing them with a new set of requirements (Section 322). This new section emphasizes the need for State, tribal and local entities to closely coordinate mitigation planning and implementation efforts.

Section 322 continues the requirement for a State mitigation plan as a condition of disaster assistance, adding incentives for increased coordination and integration of mitigation activities at the State level through the establishment of requirements for two different levels of State plans – standard and enhanced. States that demonstrate an increased commitment to comprehensive mitigation planning and implementation through the development of an approved Enhanced State Plan can increase the amount of funding available through the Hazard Mitigation Grant Program (HMGP). Section 322 also established a new requirement for local mitigation plans and authorized up to seven percent of HMGP funds available to a State to be used for development of State, local and tribal mitigation plans.

UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM ACT OF 2001 (USA PATRIOT ACT)[12]

This Act outlines the domestic policy related to deterring and punishing terrorists, and the United States policy for Critical Infrastructure/Key Resource protection. It also provides

[12] Public Law 106-390, 114 Stat. 1552 (October 30, 2000).

for the establishment of a national competence for National Infrastructure Simulation and Analysis Center and outlines the Federal government's commitment to understanding and protecting the interdependencies among critical infrastructure.

MARITIME TRANSPORTATION SECURITY ACT OF 2002[13]

This Act directs initial and continuing assessments of maritime facilities and vessels that may be involved in a TSI. It requires DHS to prepare a National Maritime Transportation Security Plan for deterring and responding to a TSI and to prepare incident response plans for facilities and vessels that will ensure effective coordination with Federal, State, and local authorities. It also requires, among other actions, the establishment of transportation security and crewmember identification cards and processes; maritime safety and security teams; port security grants; and enhancement to maritime intelligence and matters dealing with foreign ports and international cooperation.

MAGNUSON ACT[14]

This Act provides the USCG with the authority to ensure the protection and security of vessels, harbors, and waterfront facilities against sabotage or other subversive activities. It authorizes the USCG to establish security zones to prevent damage or injury to any vessel or waterfront facility and to safeguard ports, harbors, territories, or waters of the United States.

PORTS AND WATERWAYS SAFETY ACT (PWSA)[15]

The PWSA grants the USCG broad authority to take action in response to safety and security issues within the port. For example, the USCG is authorized to establish safety or security zones both on land and water. Only authorized persons, vehicles, or vessels may enter a safety or security zone. Persons within a zone must obey the lawful orders of the COTP (see 33 C. F. R. Part 165). Further the PWSA implementing regulations at 33 C. F. R. Part 160 authorize the COTP to control vessels and facility operations to ensure the safety and security of vessels and waterfront facilities, as well as to protect navigable waters and the resources therein.

FEDERALISM

In regard to authority to preempt state action, when a USCG official takes action pursuant to this strategy, and that action implements or enforces an existing federal legal requirement for maritime security, it would be consistent with the Federalism principles set out in Executive Order 13132 to construe that action as preempting state laws or regulations that conflict with the existing federal legal requirement. This is because owners or operators of facilities or vessels, including those owned and operated by States, that may be subject to federal legal requirements for maritime security for both performance and operating standards, must have one uniform national standard that they must meet. Vessels and shipping companies, particularly, would be confronted with an

[13] Public Law 107-295, codified at 46 U.S.C. 701.
[14] 50 U.S.C. 191.
[15] 33 U.S.C. § 1221 et seq.

unreasonable burden if they had to comply with varying requirements as they moved from State to State. Therefore, the preemption principles enumerated by the Supreme Court in U.S. v. Locke, 529 U.S. 89 (2000) regarding field preemption of certain state vessel safety, equipment, and operating requirements extend to actions taken pursuant to this strategy which implement or enforce an existing federal legal requirement for maritime security, especially regarding the longstanding history of significant USCG maritime security regulation and control of vessels for security purposes. The same considerations apply to facilities, at least insofar as a state law or regulation applicable to the same subject for the purpose of protecting the security of the facility would conflict with a federal legal requirement; in other words, it would either actually conflict or would frustrate an overriding federal need for uniformity.

Finally, it is important to note that actions taken by the USCG pursuant to this strategy which implement or enforce an existing federal legal requirement for maritime security bear on national and international commerce, where there is no constitutional presumption of concurrent state regulation. Many aspects of federal legal requirements for maritime security are based on the U.S. international treaty obligations regarding vessel and port facility security contained in the International Convention for the Safety of Life at Sea, 1974, TIAS 9700; Rectification (1982), TIAS 10626, as amended, and the complementary ISPS Code. These international obligations reinforce the need for uniformity regarding maritime commerce.

The authorities of Federal agencies, other than the USCG, may also preempt state action due a need to maintain national uniformity, to satisfy international obligations, to carry out express Congressional intent, to comply with specific case law, or due to a history of longstanding regulation. All questions concerning specific agency authority to preempt state action must be referred to competent counsel.

Notwithstanding the foregoing position, the Federal government intends to consult with appropriate state officials and the private sector as set out in the strategy.

EXISTING INTERAGENCY INSTITUTIONS

Interagency cooperation has long been a cornerstone of effective governance. Multiple interagency groups provide for effective communications and cooperation across the spectrum of the supply chain.

HOMELAND SECURITY ADVISORY COUNCIL

At the upper levels of the Department of Homeland Security, the Homeland Security Advisory Council (HSAC) provides advice and recommendations to the Secretary on matters related to homeland security. The Council is comprised of leaders from State and local government, first responder communities, the private sector, and academia.

CRITICAL INFRASTRUCTURE SECTOR PARTNERSHIP

Critical infrastructure protection is a shared responsibility among Federal, State, local, and tribal governments and the owners and operators of the Nation's CI/KR. Partnerships between the public and private sectors are essential, in part because the private sector

owns and operates approximately 85% of the Nation's critical infrastructure. Government agencies have access to critical threat information, and each controls security programs, research and development, and other resources that may be more effective if discussed and shared, as appropriate, in a partnership setting.

Sector Partnership Structure

Homeland Security Presidential Directive 7 (HSPD-7) and the NIPP provide the overarching framework for a structured partnership between government and the private sector for protection of CI/KR. This sector partnership structure details the formation of Sector Coordinating Councils and Government Coordinating Councils as described below.

Sector Coordinating Councils (SCC)

SCCs foster and facilitate the coordination of sector-wide activities and initiatives designed to improve the security of the Nation's critical infrastructure. They are self-organized, self-led, broadly representative of owners and operators (and their associations) within the sector, and are focused on homeland security and critical infrastructure protection. DHS has a strong preference that each SCC be chaired by an owner and/or operator. Government agencies may suggest the inclusion of various parts of a sector but it is the responsibility of each SCC to identify the sector's boundaries, establish the criteria for membership, seek broad participation and representation of the diversity of the sector, and, establish the governance, business case, and work processes of the sector's SCC.

Government Coordinating Councils (GCC)

The GCC brings together diverse Federal, State, local and tribal interests to identify and develop collaborative strategies that advance critical infrastructure protection. GCCs serve as a counterpart to the SCC for each CI/KR sector. They provide interagency coordination around CI/KR strategies and activities, policy and communication across government, and between government and the sector to support the Nation's homeland security mission. GCCs coordinate with and support the efforts of SCCs to plan, implement and execute sufficient and necessary sector-wide security to support the CI/KR sector. GCCs can leverage complementary resources within government and between government and CI/KR owners and operators.

Critical Infrastructure Partnership Advisory Council (CIPAC)

The Critical Infrastructure Partnership Advisory Council (CIPAC) provides the operational mechanism for carrying out the sector partnership structure. The CIPAC provides the framework for owner and operator members of Sector Coordinating Councils (SCC) and members of Government Coordinating Councils (GCC) to engage in intra-government and public-private cooperation, information sharing, and engagement across the entire range of critical infrastructure protection activities.

Successful execution of the sector partnership structure requires an environment in which members of the SCCs and GCCs can interact freely and share sensitive information and advice about threats, vulnerabilities, protective measures, and lessons learned. CIPAC, which has been exempted from the requirements of the Federal Advisory Committee Act

(FACA), is the mechanism to allow meaningful dialogue on key critical infrastructure protection issues and agreement on mutual action between government and owner/operator entities.

CIPAC is a non-decisional body and includes sector members and government members. Sector members are the members that are owners and/or operators and the trade associations that represent them. Government members are the Federal, State, local and tribal government agencies (or their representative bodies) that comprise the GCC for each sector. The most current CIPAC membership list and further information is maintained on the Internet and can be found on the DHS CIPAC website.

CIPAC consists of "Joint Sector Committees" that are made up of the GCC members and eligible SCC members for each sector. For example, there is a Food and Agriculture Joint Sector Committee made up of Food and Agriculture GCC and SCC members. The CIPAC also includes one Joint Cross-Sector Committee, most likely to consist of the designated private sector and agency leads from each Joint Sector Committee.

JOINT TERRORISM TASK FORCE (JTTF)/NATIONAL JOINT TERRORISM TASK FORCE

A JTTF is a partnership between the Federal Bureau of Investigation, other federal agencies (notably DHS components such as CBP, ICE, the TSA and the USSS), State, local law enforcement, and specialized agencies, such as railroad police that are charged with taking action against terrorism.

In addition to the many regional JTTFs operating from FBI Field Offices, a National JTTF exists in Washington, DC that is composed of high-level representatives from numerous Federal agencies

INTEGRATED BORDER ENFORCEMENT TEAMS (IBETS)

To effectively combat cross-border criminal activity, American and Canadian law enforcement agencies take an international and integrated approach to their investigations.

Integrated Border Enforcement Teams (IBETs) core agencies are: the Royal Canadian Mounted Police (RCMP), the Canada Border Services Agency (CBSA), CBP, ICE, and the USCG.

IBET agencies share information and work together daily with other local, State and provincial law enforcement agencies on issues relating to national security, organized crime and other criminality transiting the Canada/U.S. border between the official Ports of Entry (POE).

AREA MARITIME SECURITY COMMITTEES (AMSCS)

The USCG has developed 45 AMSPs covering 361 ports, the Great Lakes, Inland and Western Rivers and the Outer Continental Shelf region. The USCG COTP, designated as FMSCs by the NMTSP under the MTSA of 2002[16], have facilitated and coordinated the development of these plans through Area Committees.

[16] As implemented in 33 C.F.R. Part 103.200.

Each FMSC has formed an AMSC, comprised of Federal, State, and local agencies, as well as members of the local maritime industry, in their areas of responsibility. The Committee process enhances the exchange of communications between the USCG, local agencies and maritime stakeholders. This cooperative spirit facilitates the creation and maintenance of comprehensive, coordinated AMSPs which provide for coordinated community-wide measures and support for incident management. The AMSPs and Committees serve as the cornerstone for developing and maintaining the first lines of defense at our Nation's ports.

During a response to an incident, the AMSCs may also serve as advisory groups, providing the COTP/FMSC with critical information relating to the port, including recommendations and guidance on prioritization of response operations and resumption/restoration activities.

VIII. STRATEGIC ELEMENTS

SUPPLY CHAIN STRATEGY OVERVIEW

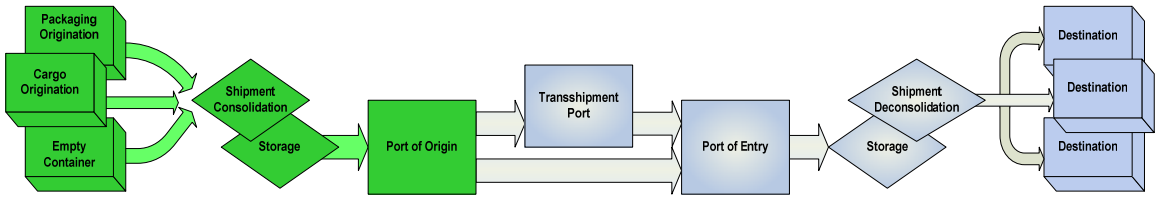
Given the multiple jurisdictions and sovereignty issues associated with the international supply chain, the DHS has developed a layered security strategy which applies specific preventative programs, often conducted as partnering initiatives with the international community.

Each program has at its core the fundamental concepts of risk management, targeting activities toward the highest risks at identifiable key nodes or transportation sectors within the supply chain in order to drive down the associated probability of an incident, vulnerability to an incident, or consequence arising from an incident. The key nodes within the supply chain provide logical arenas for programs, and taken as a whole the programs integrate to provide for an end-to-end supply chain security methodology.

Many of the programs also directly integrate into response and recovery activities. As an example, data derived from routine screening of inbound cargo by CBP can be used to prioritize vessels and cargoes for the resumption of trade.

An overview of how the programs within the Department interlock to provide for layered security in depth is contained in figure 8, Cargo Supply Chain Security Program Overview. In reviewing the figure, however, it should be noted that the beginning and end points of the programs may not apply to every situation within the supply chain. For instance, MTSA and the TWIC may or may not apply to Storage and Shipment Deconsolidation in all ports.

PREVENTION THROUGHOUT THE SUPPLY CHAIN



ORIGINATION TO PORT OF ORIGIN

The security of the international supply chain begins with the origin of the cargo. Through international standards such as the WCO "Framework of Standards to Secure and Facilitate Global Trade" and CBP's C-TPAT program, public-private and international partnerships engage in ensuring security is inherent in business practices from the beginning.

C-TPAT (Customs-Trade Partnership Against Terrorism)

C-TPAT seeks to enhance security measures across a company's entire supply chain by requiring close cooperation among its constituent entities, from importers, brokers, carriers and foreign manufacturers and suppliers.

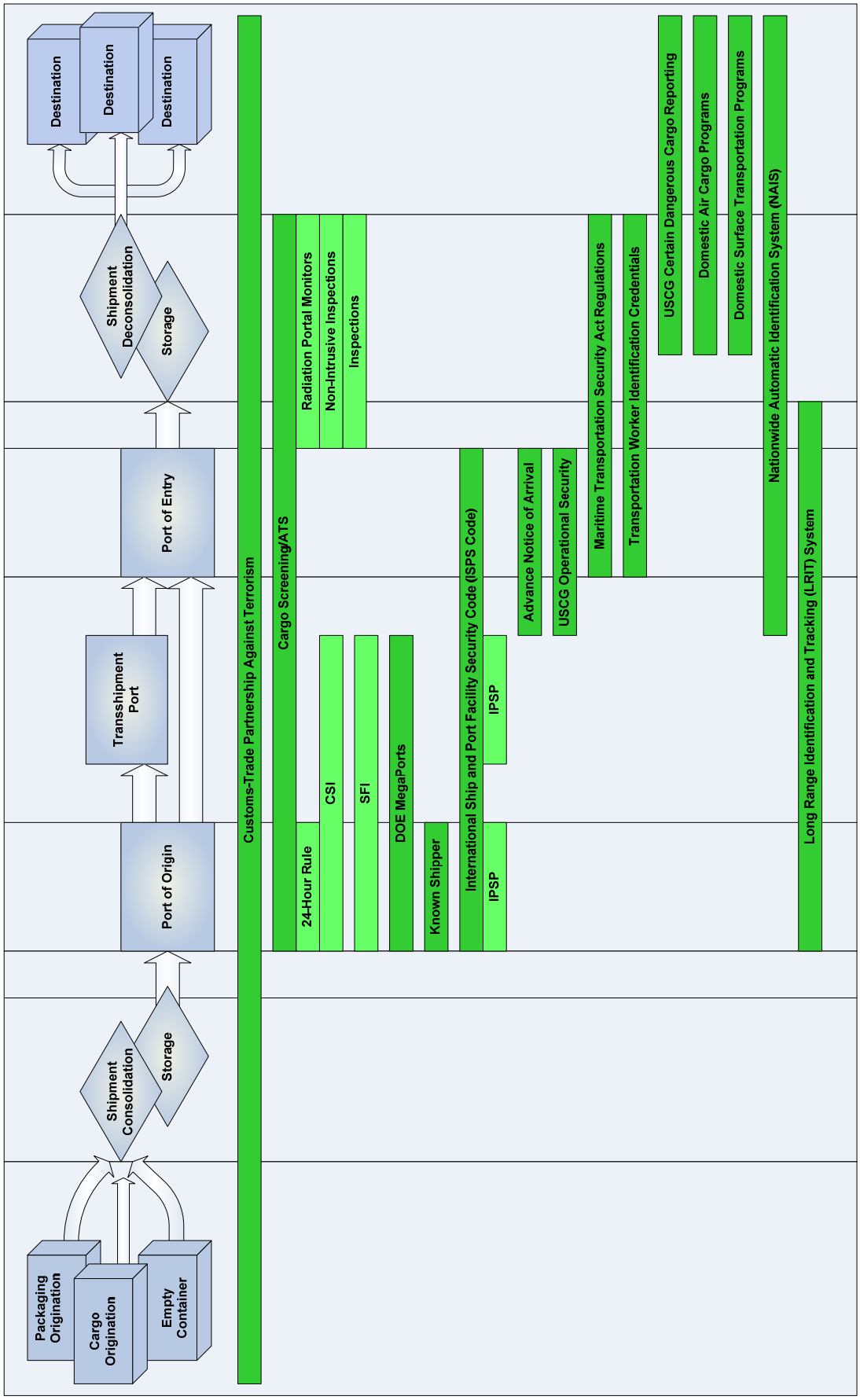


Figure 8: Cargo Supply Chain Security Program Overview.

C-TPAT is a successful voluntary government-business initiative to build cooperative relationships that strengthen and improve overall international supply chain and United States border security. C-TPAT recognizes that CBP can provide the highest level of cargo security only through close cooperation with the ultimate owners of the international supply chain such as importers, carriers, consolidators, licensed customs brokers, and manufacturers. Through this initiative, CBP is asking businesses to ensure the integrity of their security practices and communicate and verify the security guidelines of their business partners within the supply chain.

At the end of January 2007, there were 6,375 certified members enrolled in C-TPAT and over 3,900 validations had been completed (61 percent). CBP will continue to use the validation approaches and strategies implemented throughout 2006 to reach 100 percent validations of all certified members due for validation or revalidation by the end of 2007. Revalidations based on risk will also be conducted to verify the effectiveness and efficiency of the C-TPAT member's supply chain security program and compliance with established C-TPAT security criteria. All certified partners will be revalidated not less than once every three years from the completion date of the initial validation. For importers, the revalidation process will focus on the foreign supply chain from the initial point of stuffing to the final destination where the cargo is cleared by CBP in the United States. This may include manufacturing sites, foreign logistics providers, and foreign ports. A risk assessment will be made to determine the actual sites to be visited. Revalidations will continue to be conducted jointly by CBP Supply Chain Security Specialists and the C-TPAT member's representatives.

On an annual basis, CBP will query its internal C-TPAT records management system and create a list of all C-TPAT certified and validated members that have not been revalidated within the last three years. This list will be utilized to determine the total number of members to be scheduled for revalidation in the upcoming year. CBP will then assess the number of personnel needed to perform these revalidations. Revalidations will be scheduled by CBP using risk management principles, to include factors such as high-risk countries of origin, use of non-related parties, and employment of a variety of supply chains. Additionally, as the enrollment sector with the greatest demonstrated risk for compromise, all certified United States/Mexico Highway Carriers will be revalidated on an annual basis.

CSDs (Container Security Devices)

The DHS Science and Technology Directorate has evaluated commercial off-the-shelf (COTS) CSD technologies. CBP, DHS Policy and S&T are working together to outline technical and operational requirements for the employment of CSDs that would have the capability to alert law enforcement authorities of any container door's opening and/or removal. These requirements include key performance requirements, communication capabilities, as well as documentation verifying sufficient testing has been completed.

This effort will further the development of C-TPAT requirements for Tier III participants including CSD requirements for the detection of door openings or removal, reliability and communication capabilities. Tier III is for those C-TPAT members that exceed minimum security criteria and demonstrate a commitment to the highest levels of supply chain security. DHS began consultations with the industry in early 2007 to ensure that the

device specifications and requirements can be incorporated within normal business practices.

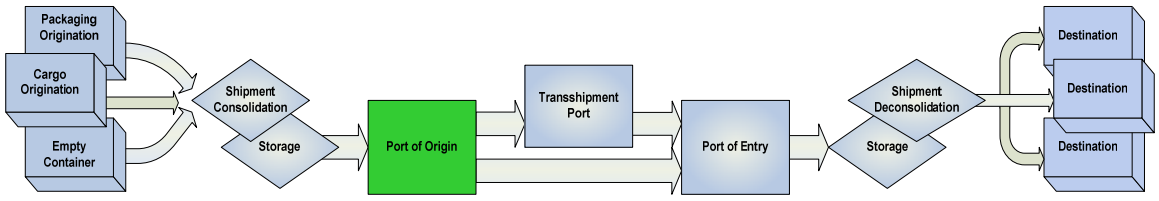
Following a technical review and any further testing by S&T, CBP will communicate a list of qualified CSD vendor solutions to C-TPAT participants.

S&T will continue to provide technical evaluations and vulnerability testing. Once approved CSDs are available, CBP will consult with the trade community to identify possible changes in C-TPAT requirements. It is important to note that the deployment of CSD technology only improves supply chain security as part of a broader supply chain security process that ensures the integrity of the shipment before the CSD is activated. Requiring such a device independent of a process to ensure that the container was secure before its application would have an adverse effect on security by creating the false impression that a dangerous shipment was secure. That is why this strategy is directed at C-TPAT. C-TPAT partners are committed to a comprehensive security process including procedures for securing containers at the point of stuffing. They also agree to open their global security procedures, including overseas operations, to CBP officer validation.

The CSD initiative is intended to accelerate the deployment of cargo security technologies that will further secure the international supply chain. Once an acceptable and cost effective CSD exists in the marketplace, the Department will determine the appropriate role for this technology in the overall supply chain security process. Because a readily available CSD may be one to two years away, it is premature to determine exactly how the CSD will be employed as part of C-TPAT protocols or any other supply chain security process, given the volatile nature of technological, environmental, and risk-based factors. Once approved CSDs become available, CBP will consult with the trade community to identify possible changes in C-TPAT requirements.

PORT OF ORIGIN

Ports of origin provide key consolidation nodes within the supply chain, as cargo is brought together and loaded on transport. This natural 'choke point' effect significantly leverages the effectiveness of security measures by providing a focal point whereby integrated security practices such as the screening of all inbound containers at entrances can be rapidly accomplished.



24-Hour Rule

Under the 24-Hour Rule requirement, manifest information on cargo destined for the United States must be provided 24 hours prior to a container being loaded onto a vessel in a foreign port. CBP may deny the loading of high-risk cargo while the vessel is still overseas.

CSI (Container Security Initiative)

CSI is a customs-to-customs partnership that addresses the threat to border security and global trade posed by the potential for terrorist use of a maritime container to deliver a weapon. CSI proposes a security regime to ensure all containers that pose a potential risk for terrorism are identified and inspected at participating foreign ports before they are placed on vessels destined for the United Sates. CSI is currently operational at 51 participating seaports which represent 82 percent of the cargo destined for the United States. CBP has stationed multidisciplinary teams of United States officers from both CBP and ICE to work together with host foreign government counterparts. Their mission is to target and prescreen containers and to develop additional investigative leads related to the terrorist threat of cargo destined to the United States.

The three core elements of CSI are:

- Identify high-risk containers. CBP uses automated targeting tools to identify containers that pose a potential risk for terrorism, based on advance information and intelligence.
- Prescreen and evaluate containers before they are shipped. Containers are screened as early in the supply chain as possible, generally at the port of departure.
- Use technology to scan high-risk containers to ensure that scanning can be done rapidly without slowing down the movement of trade. This technology includes large-scale X-ray and gamma ray machines and radiation detection devices.

Through CSI, CBP officers work with host customs administrations to establish security criteria for identifying high-risk containers. Those administrations use non-intrusive inspection (NII) and radiation detection technology to scan high-risk containers.

Sovereignty considerations make it difficult for DHS to set "standards" in a foreign country for their purchase of non-intrusive inspection (NII) systems. However, it is recommended that host nation counterparts purchase NII systems that meet the specifications of the WCO Customs Compendium, Container Scanning Equipment, Guidelines to Members on Administrative Considerations of Purchase and Operation, and language to this effect has been included in all arrangements with foreign CSI participants (called "Declarations of Principles") signed after May 2005. It should be noted that foreign CSI participants are to utilize NII equipment that either meets or exceeds the capability of NII equipment used by CBP domestically.

The goal is for CBP's overseas CSI teams to conduct 100 percent manifest review before containers are loaded on vessels destined for the United States. However, in those locations where the tremendous volume of bills does not allow for the overseas CSI team to perform 100 percent review, CSI targeters at the National Targeting Center provide additional support to ensure that 100 percent review is accomplished. Through the use of the overseas CSI teams and the CSI targeters at the National Targeting Center, CBP is able to achieve 100 percent manifest review for the CSI program.

CBP has developed three automated tools for statistical analysis, an evaluation database to track and analyze any deficiencies identified during the evaluation process of the CSI

ports, and a NII utilization database that tracks the use of NII equipment at CSI ports to include the downtime of the equipment. The third tool is a web-based statistical database that tracks daily and weekly examinations at the CSI ports as well as shipment volumes, shipments by region and ATS scoring.

CBP also conducts CSI port evaluations covering: 1) pre-deployment training, 2) administrative functions, 3) examinations, 4) targeting, 5) intelligence, and 6) investigations.

CSI, a reciprocal program, offers its participant countries the opportunity to send their customs officers to major United States ports to target ocean-going, containerized cargo to be exported to their countries. Likewise, CBP shares appropriate, agreed-upon information on a bilateral basis with its CSI partners.

SFI (Secure Freight Initiative)

The SFI is a joint DHS and Department of Energy (DOE) program which builds upon existing port security measures by enhancing the U.S. government's ability to gather data on containers as they transit across the supply chain. Phase 1 of Secure Freight, announced by the Secretary of Homeland Security on December 7, 2006, aims at fine-tuning systems to scan containers for nuclear and radiological materials overseas and to better assess the risk of inbound containers.

The initial phase of Secure Freight involved the deployment of a suite of proven nuclear and radiological detection devices, including radiation portal monitors (RPM) and non-intrusive inspection (NII) equipment, at six foreign ports: Port Qasim in Pakistan; Puerto Cortes in Honduras; Southampton in the United Kingdom; Port Salalah in Oman; Port of Singapore; and the Gamman Terminal at Port Busan in Korea. Beginning in mid 2007, all containers from the first three ports and a limited selection from the latter three ports will be scanned for radiation before departing for the United States. In addition, CBP will continue to evaluate the pilot system being used in Hong Kong. Vital lessons will be learned based on the unique footprints and logistical challenges of these selected ports and will inform future deployments. These conclusions will be outlined in a report required under SAFE Port Act Section 231(d) which will be submitted to Congress in April 2008.

Increasing containers scanned for a radiological or nuclear presence is the beginning of Secure Freight; however, the goal of enhancing the data available on containers as they transit the supply chain extends to commercial information as well. As soon as an importer places an order, the stream of information related to these goods, and the future shipment begins. Throughout the supply chain, additional pieces of information related to that shipment are developed and distributed as part of traditional commercial practice. Currently only certain pieces of information, such as manifests and entry data are required by DHS. However, additional pieces of information on a shipment would provide a more complete picture. In future phases of the SFI, such as the Security Filing (10+2) Initiative, additional data elements will be collected, combined with the physical movement data, and integrated into the analysis process. Additional commercial information increases knowledge about a shipment, increasing confidence in its legitimacy and integrity, further focusing resources on true threats.

Data gathered on containers bound for the United States in foreign ports participating in the SFI is transmitted in near real-time to CBP officers working in overseas ports and to CBP's National Targeting Center. This data is combined with other available risk assessment information, such as required manifest submissions, to improve risk analysis, targeting and the scrutiny of high-risk containers overseas.

ATS (Automated Targeting Systems)

CBP thoroughly screens 100 percent of all shipments destined for the United States through the Automated Targeting Systems. "Screening" is defined as a visual or automated review of information about goods, including manifest or entry documentation accompanying a shipment being imported into the United States, to determine the presence of misdeclared, restricted, or prohibited items and to assess the level of threat posed by such cargo. Shipments identified as high-risk are then examined either overseas at a participating CSI port or when the shipment arrives in the United States.

The Advance Electronic Cargo Information requirements mandated in the Trade Act of 2002 (including the 24-Hour Rule) ensure that relevant data is available in the Automated Manifest System allowing CBP to effectively evaluate all inbound shipments using the ATS before vessel loading. ATS uses manifest and entry declaration data from the Automated Commercial System (Automated Manifest System and Automated Broker Interface) and enforcement data from the Treasury Enforcement Communications System (TECS) to provide targeting functionality for cargo.

ATS provides decision support functionality for CBP officers working in Advanced Targeting Units (ATUs) at United States ports of entry and CSI ports. The system provides uniform review of cargo shipments for identification of the highest threat shipments, and presents data in a comprehensive, flexible format to address specific intelligence threats and trends. ATS uses a rules-based program to highlight potential risk, patterns, and targets. The rule sets established by ATS are used to identify high-risk activities or conditions that are activated in association with a shipment and are weighted to quantify risks. The rule sets are based on the best practices and knowledge base of experienced CBP personnel and other experts from outside of CBP. Through rules, the ATS alerts the user to data that meets or exceeds certain predefined criteria. National targeting rule sets have been implemented in ATS to provide threshold targeting for national security risks for all modes: sea, truck, rail, and air.

All inbound cargo, including freight remaining on board, is currently screened through ATS. This analysis may be performed at the National Targeting Center in Reston, Virginia, as well as at the local manifest review units at each United States port of entry. The advanced data is analyzed, a risk-assessment performed, and all shipments identified as high-risk (defined as meeting or exceeding a predetermined ATS threshold) are examined at either the CSI port or upon arrival into the United States using radiation scanning equipment and NII technology. All examination findings are recorded in ATS and/or ACS.

DOE Megaports

Under its Megaports Initiative, which began in 2003, the DOE National Nuclear Security Administration (NNSA) teams with other countries to enhance their ability to scan container cargo at major international seaports for nuclear and other radioactive materials. DOE/NNSA provides radiation detection equipment and associated communications systems to host nation authorities, provides training on the use of the equipment, and provides technical support to host nation officials and law enforcement officers. In return, NNSA requires that data be shared on detections and seizures of nuclear or radiological material that resulted from the use of the equipment provided.

DOE/NNSA's Megaports program and CBP's CSI program are collaborative efforts. These two programs complement one another and build upon a risk-based approach to securing the international supply chain. DOE/NNSA's Megaports Initiative works with foreign governments to install specialized radiation detection equipment in order to deter, detect, and interdict illicit shipments of nuclear and other radioactive materials.

TSA Known Shipper Database

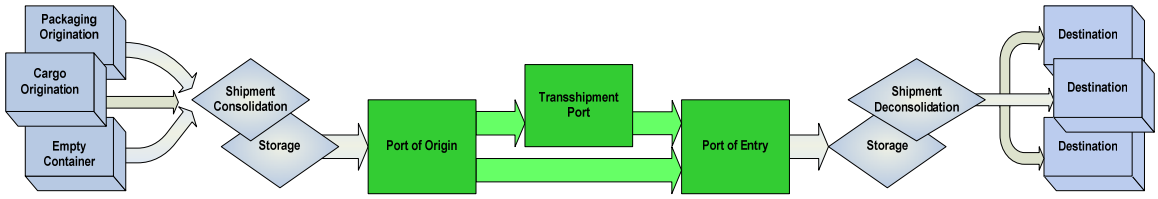
The Known Shipper database provides a systematic approach to assess risk and determine the legitimacy of shippers. Passenger Air Carriers and Indirect Air Carriers must comply with a broad range of specific security requirements to qualify, their clients as Known Shippers. Air Carriers and Indirect Air Carriers may use TSA's database if approved by TSA.

International Port Security Program

The USCG has established the IPS Program to assess the effectiveness of anti-terrorism measures in the ports of our trading partners. The program visits ports overseas and evaluates the effectiveness of port security measures in foreign countries. The USCG uses a country's implementation of the ISPS Code as a primary indicator of the effectiveness of such measures. The IPS Program also promotes the effectiveness of the ISPS Code by working with foreign governments to improve port and vessel security. USCG International Port Security Liaison Officers (IPSLOs) are assigned to various locations both in the U.S. and overseas and visit foreign port facilities to share knowledge and expertise and to maintain situational awareness of security conditions. In this capacity, IPSLOs coordinate and dialogue with CBP CSI personnel in the countries they visit. The information the IPS Program gathers about foreign port security is used by the USCG to continuously update the targeting protocols that are used to determine the security risk posed by each foreign flagged vessel intending to visit the United States. Furthermore, should a country be found to not have effective anti-terrorism measures in place, the USCG imposes conditions of entry on vessels arriving from that country's ports in accordance with the MTSA of 2002.

PORT OF ORIGIN TO UNITED STATES PORT OF ENTRY

The maritime link in the typical international supply chain serves as a physical convergence point for large numbers of shipments. Once delivered to the foreign port facility, containers and other types of cargo are moved in an aggregate bulk manner across water. A standard container vessel carries thousands of containers. This physical reality presents both opportunities and challenges to supply chain security.



The International Ship and Port Facility Security Code (ISPS Code)

Port facilities and commercial vessels are heavily regulated by both international organizations and individual States. The IMO, responding to the attacks on September 11, 2001, produced the *International Ship and Port Facility Security Code*. The ISPS Code contains a mandatory section and a guidance section of security standards for port facilities and vessels. These security regulations set a minimum acceptable standard for security fundamentals such as facility and vessel security plans, physical security, security audits, personnel responsibilities, training and exercises. The mandatory section of the ISPS Code went into effect on July 1, 2004. The vast majority of countries that trade by sea are in compliance with the ISPS Code. In affect, the ISPS Code ensures a robust supply chain security regime from the time cargo enters a foreign port facility, through its transport over water, and until it is released from the domestic port terminal.

Cargo that is traveling towards the United States will fall under the security regime of the ISPS Code once it enters a foreign port facility and begins travel across the ocean. Obviously, the ISPS Code also applies to the United States.

MDA (Maritime Domain Awareness)

MDA is the effective understanding of anything associated with the global maritime domain that could impact the United States' security, safety, economy, or environment. A range of Federal departments and agencies coordinate closely to identify threats as early and as distant from our shores as possible. Unifying United States government efforts and supporting international efforts will help achieve MDA across the Federal government, with the private sector and civil authorities within the United States, and with our allies and partners around the world.

NAIS (Nationwide Automatic Identification System)

In compliance with the MTSA of 2002, emerging homeland security requirements, and the need to improve vessel traffic services (VTS) and navigational safety, the USCG is implementing a Nationwide Automatic Identification System (NAIS) that will support MDA of the Nation's territorial waters and adjacent sea areas. The Automatic Identification System (AIS) is an international standard for ship-to-ship, ship-to-shore, and shore-to-ship communication of information, including vessel identity, position, speed, course, destination and other data of critical interest for navigation safety and maritime security. AIS equipment is required domestically and internationally aboard

most commercial vessels[17]. The information provided by the NAIS project will support all of the Nation's maritime interests – from the safety of vessels and ports through collision avoidance, to the safety of the nation through detection, traffic management, and classification of vessels when they are still thousands of miles offshore – and particularly support the requirements for MDA.

NAIS will complement other surveillance and intelligence systems greatly by aiding the essential process of identifying vessels requiring further investigation and action. NAIS information will be displayed in the USCG National Maritime Common Operational Picture (COP) and shared, along with correlated data and intelligence as appropriate, with other DHS and Federal agencies. Unclassified portions of the COP will also be available to local port partners in support of security and safety operations. This information will be invaluable to agencies, such as CBP, ICE, and the TSA, as it will provide real-time location data on all major cargo and other commercial vessels in the maritime domain. The system is expected to be fully implemented and operational by 2014.

LRIT (Long Range Identification and Tracking of Vessels)

The IMO Maritime Safety Committee (MSC) at its 81st session in May 2006 adopted new regulations for the LRIT together with associated performance standards and functional requirements, and, at its 82nd session in December 2006, designated the International Mobile Satellite Organization (IMSO) as the LRIT "Coordinator.

The new regulation on LRIT is included in SOLAS Chapter V on Safety of Navigation, through which LRIT will be introduced as a mandatory requirement for the following ships on international voyages: passenger ships, including high-speed craft; cargo ships, including high-speed craft, of 300 gross tonnage and upwards; and mobile offshore drilling units.

The SOLAS regulation on LRIT establishes a multilateral agreement for sharing LRIT information for security, search and rescue purposes, among SOLAS Contracting

---

[17] In accordance with 46 U.S.C. § 70114, the following vessels must have a properly installed, operational, type approved AIS:

(1) Self-propelled vessels of 65 feet or more in length, other than passenger and fishing vessels, in commercial service and on an international voyage.

(2) Notwithstanding paragraph (1), the following, self-propelled vessels, that are on an international voyage must also comply with SOLAS, as amended, Chapter V, regulation 19.2.1.6, 19.2.4, and 19.2.3.5 or 19.2.5.1 as appropriate:

(i) Passenger vessels, of 150 gross tonnage or more.

(ii) Tankers, regardless of tonnage.

(iii) Vessels, other than passenger vessels or tankers, of 50,000 gross tonnage or more.

(iv) Vessels, other than passenger vessels or tankers, of 300 gross tonnage or more but less than 50,000 gross tonnage.

(3) Notwithstanding paragraphs (1) and (2), the following vessels, when navigating certain specific areas with Vessel Traffic Service centers:

(i) Self-propelled vessels of 65 feet or more in length**,** other than fishing vessels and passenger vessels certificated to carry less than 151 passengers-for-hire, in commercial service;

(ii) Towing vessels of 26 feet or more in length and more than 600 horsepower, in commercial service;

(iii) Passenger vessels certificated to carry more than 150 passengers-for-hire.

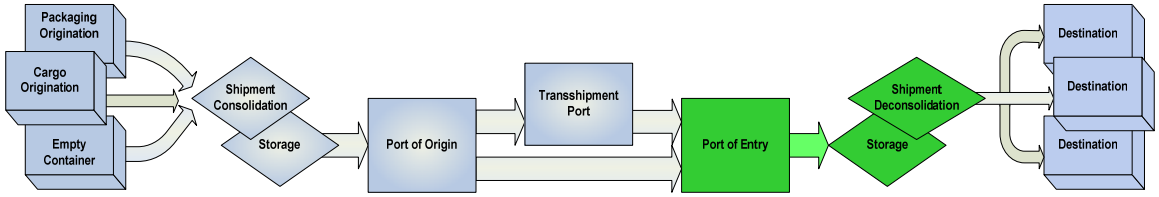
Governments, in order to meet the maritime security needs and other concerns of such Governments. It maintains the right of flag States to protect information about the ships entitled to fly their flag, where appropriate, while allowing coastal States access to information about ships navigating off their coasts. The SOLAS regulation on LRIT does not create or affirm any new rights of States over ships beyond those existing in international law, particularly, the United Nations Convention on the Law of the Sea (UNCLOS), nor does it alter or affect the rights, jurisdiction, duties and obligations of States in connection with UNCLOS.

The LRIT information ships will be required to transmit include the ship's identity, location and date and time of the position. There will be no interface between LRIT and AIS. One of the more important distinctions between LRIT and AIS, apart from the obvious one of range, is that, whereas AIS is a broadcast system, data derived through LRIT will be available only to the recipients who are entitled to receive such information and safeguards concerning the confidentiality of those data have been built into the regulatory provisions. SOLAS Contracting Governments will be entitled to receive information about ships navigating within a distance not exceeding 1000 nautical miles off their coast.

The regulation is expected to enter into force on January 1, 2008 and will apply to ships constructed on or after December 31, 2008 with a phased-in implementation schedule for ships constructed before December 31, 2008. LRIT is intended to be operational with respect to the transmission of LRIT information by ships starting from December 31, 2008, with full implementation contingent upon the progress of the IMSO in its role as LRIT Coordinator.

UNITED STATES PORT OF ENTRY

The greatest layer of direct control over the supply chain by the United States government is upon the entry of cargo into domestic territorial waters and Ports of Entry. Here, regulatory oversight provides for compliance at all levels of the security system.



Advance Notice of Arrival

Under domestic regulations, vessels that intend to enter the United States must give advance notice of arrival.[18] The information that is submitted is immediately vetted by both the USCG and CBP to determine the relative risk of the vessel, the crew, any passengers and the cargo. The COTP will grant or deny permission to enter the waters of the United States.

[18] The applicability to vessels is set by vessel size and/or operation. The time required for advanced notice of arrival is determined by expected transit time. The regulations are found in 33 C.F.R. § 160.

Operational Security Measures

The USCG and other agencies may apply targeted operational risk reduction measures to ensure a vessel's visit does not pose a threat to the United States. Typical operational security measures include security boardings, escorts by a USCG or other law enforcement vessel, or having a team of law enforcement officers riding with the vessel to ensure its positive control. Operational security measures are conducted with a random element of scheduling and are scalable based on local or national security threat levels.

Regarding targeting of vessels for security measures, the nature and amount of dangerous cargoes on a vessel is a factor. Examples are bulk flammable liquids and packaged radioactive materials. The USCG has in-depth understanding of local port operations, as well as databases of historical vessel information that facilitates the recognition of suspicious maritime operations. Many ports now are equipped with either active or passive ship surveillance systems or other MDA programs. The USCG actively manages port activities to isolate risky operations or dangerous cargoes from sensitive areas or activities.

All of these layered security systems work together to ensure that a visiting foreign flagged vessel arrives at its intended berth in a safe, secure and timely manner. Again, while focused on vessel security, all of these activities contribute to cargo and supply chain security.

The Maritime Security Regulations

The United States has implemented a port facility and vessel security program as required by Congress and its international obligations under the ISPS Code. The program requires a high level of security for all port facilities and vessels operating within the United States. The USCG reviews all security plans for port facilities and vessels that are regulated under its maritime security regulations found in 33 C. F. R. Parts 101 through 106. These regulations are performance-based; meaning that the port facilities and vessels can use security measures that work best for their environment and operations so long as the measures meet the performance standards in the regulation. Once approved in their respective security plans, the USCG ensures the port facility or vessel is operating in accordance with the plan. Deficiencies are addressed promptly, and failure to operate in accordance with an approved security plan will result in the USCG COTP terminating the operations of the port facility or vessel. All of these security requirements serve to protect and secure cargo in transit.

Another security resource in the maritime portion of the international supply chain is the AMSC. 46 U.S.C. § 70112 authorizes all port areas of the United States within the geographic area designated as a COTP AOR, or ‘zone,’ to be covered by an AMSC. The committee consists of a broad representation of Federal, State, local and tribal members, as well as industry, academia and other stakeholders. A primary responsibility of the AMSC is to assist the COTP acting as the FMSC in producing and updating an AMSP. This plan describes the roles and responsibilities of stakeholders in protecting port critical infrastructure and preventing TSIs. Each plan also documents contingency response

organizational elements and general recovery priorities for TSIs.[19] The plans address cargo issues for the port(s) covered. The committees are valuable forums for all port stakeholders to discuss security issues and conduct planning for incidents that impact domestic and international supply chains.

Transportation Worker Identification Credential

While on the terminal, cargoes are protected from access by unauthorized persons by the TWIC program. The TWIC program requires that transportation and/or port workers who need unescorted access to secure areas successfully complete a background check. The workers are issued an identification card that incorporates biometric information. This allows security personnel to control access to secure areas of vessels and port facilities to only those who are authorized to be there.

CBP Cargo Screening

Once ashore, containers and cargo remain secure at domestic port facilities until released by CBP.

Currently, CBP thoroughly screens 100 percent of all shipments destined for the United States through the Automated Targeting Systems, including freight remaining on board. Those shipments identified as high-risk are then examined either overseas at a participating CSI port or when the shipment arrives in the United States. Conveyances that are identified as high-risk undergo an examination. CBP defines an "examination" as a physical inspection of a conveyance and/or the imaging of a conveyance, using large-scale non-intrusive inspection (NII) technology, for the presence of anomalies that could indicate illicit materials or contraband.

CBP is currently utilizing large-scale X-ray and gamma ray machines and radiation detection devices to scan cargo. The acquisition and deployment of radiation detection equipment is coordinated closely with DHS' Domestic Nuclear Detection Office (DNDO). Presently, CBP operates over 913 radiation portal monitors (RPMs) at our Nation's ports (including 342 RPMs at seaports), utilizes over 180 large scale non-intrusive inspection devices to examine cargo, and has issued 14,150 handheld-held radiation detection devices. DNDO is currently developing next-generation technologies for CBP and other operators that will provide improved detection capabilities. These next-generation systems will be gradually introduced at our nation's ports beginning this calendar year. Also, over 600 canine detection teams capable of identifying narcotics, bulk currency, human beings, explosives, agricultural pests, and chemical weapons are deployed at our ports of entry.

NII (Non-Intrusive Inspection) and Radiation Scanning Technology

The use of NII systems dramatically enhances CBP's ability to inspect conveyances and cargo for components of weapons of mass destruction, articles, and instruments used to support terrorist activities, narcotics, undeclared currency, and contraband, while facilitating legitimate commercial traffic through the Nation's ports. The NII Systems Program (Large Scale) is an essential component of CBP's multi-layered enforcement strategy. Technology and equipment must be matched with the conditions and

[19] defined at 46 U.S.C. § 70101.

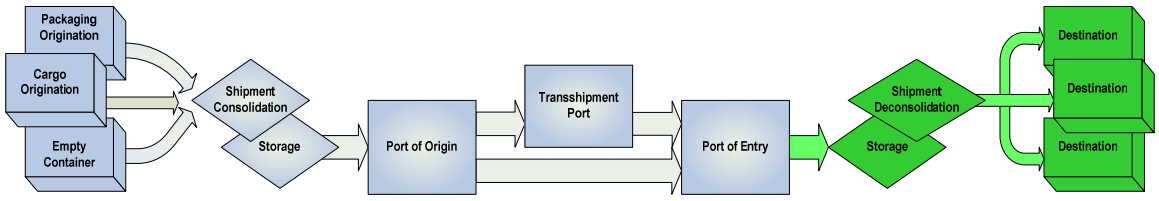
requirements at each inspection point, including domestic ports of entry, border patrol checkpoints, and overseas ports, based upon a scientific analysis of the individual operational conditions at each location. CBP has conducted a scientific analysis of both large and small volume ports to determine the current, and potentially increased effectiveness of the Large Scale NII Systems Program inspection efforts. The analysis included modeling and simulation as well as site visits to gather the necessary information. The volume of containers moving through the port, the number of NII systems available at each port, and the types of cargo (density) received at each port was taken into consideration in the analysis.

The information generated by this effort will contribute to the increased effectiveness of the Large Scale NII Systems Program through enhanced deployment, use of higher capability systems, and the investigation and implementation of alternative inspection concepts of operations demonstrated through pilot programs. In support of CBP's primary mission, NII systems provide a safe and efficient means to effectively scan a wide variety of cargo entering our country through a variety of conveyances without significantly delaying or impeding commerce. At present, 180 large-scale gamma ray and X-ray imaging systems are deployed to our Nation's ports of entry, 60 of which are in seaports. Additionally, CBP has deployed 14,150 personal radiation pagers (PRDs), which detect the presence of radiation, and 617 radiation isotope identification devices (RIIDs), which identify the type of radiological source present.

In addition to screening for risk, CBP scans conveyances, baggage, and cargoes with RPMs and other radiation detection equipment for the presence of radiation. CBP defines "scanning" as a passive means of checking a conveyance, baggage or cargo for illicit nuclear or radiological materials. RPMs are currently deployed at land border ports of entry, as well as seaports.

PORT OF ENTRY TO DESTINATION

The majority of the supply chain security regime internal to the United States is accomplished via domestic government agency activities, e.g. chemical facility security regulations and transportation regulations.



Certain Dangerous Cargo Tracking

On the inland rivers of the United States, the USCG requires that vessels carrying "certain dangerous cargoes"[20] (CDC's) report their movements. The Inland River Movement Center specifically tracks such domestic shipments, mostly made via

[20] defined at 33 C.F.R. § 160.204.

commercial barges. In the coastal regions, CDC's transport is monitored through the Advance Notice of Arrival system. This allows the USCG to apply security measures (e.g., vessel escorts and positive control boardings) to ensure that the vessels and cargo do not pose an unacceptable threat to local populations or infrastructure.

Highway Security

The United States DHS and the TSA have primary responsibility for transportation security, with the Federal Motor Carrier Safety Administration (FMCSA) providing support in the highway sector. TSA works closely with the FMCSA and the highway industry on a daily basis to address highway security issues. In addition, TSA, FMCSA, and the Pipeline and Hazardous Materials Safety Administration (PHMSA) have jointly worked with the highway industry to build upon highway infrastructure security efforts through vulnerability assessments, development of voluntary security action items, and rulemakings.

The highway transportation mode consists of privately owned vehicles traveling on publicly maintained roads. The U.S. vehicle fleet includes 15.5 million trucks and 750 thousand buses. The motor carrier freight industry consists of 1.2 million motor carriers, 9.7 million workers (including 3.3 million drivers), and 42,000 HAZMAT trucks. Seventy-five percent of U.S. communities depend solely on trucking for the movement of commodities. The U.S. highway infrastructure includes 46,700 miles of Interstate highway, 114,700 miles of other National Highway System roads, 582,000 bridges over 20 feet of span, and 54 tunnels over 500 meters in length. Although almost this entire infrastructure is used in the delivery of goods, only a small number of assets are considered critical to the international supply chain. While the buses are not usually part of the international supply system, both trucks and buses may be used as vehicles to attack infrastructure supporting the system. TSA is using the following means to enhance the security of this system of systems:

- **Corporate Security Review (CSR)** - The CSR provides a general review of the ability to protect surface transportation critical assets. A team of transportation security experts visits critical highway assets, trucking companies, and bus operators. In reviewing the operator's security plan, the review focuses on physical and personal security, as well as response and recovery planning.
- **HAZMAT Truck Tracking Pilot** - Congress provided TSA with multi-year grants to examine a pilot program to track the movement of hazardous material by truck. The pilot examines the ability to track and intercept cargo conveyances deemed to be a significant risk to national security. The pilot includes the following four goals: (1) Identify and evaluate at least three technically different, but commercially available solutions to track trucks in all 50 states; (2) Develop and evaluate a prototype for a centralized truck tracking center; (3) Develop and evaluate a non-proprietary universal interface that will allow alerts and tracking information to be transmitted from all commercially available tracking systems to a prototype truck tracking center; and (4) Evaluate the feasibility of utilizing the developed universal interface to pass tracking information between a truck tracking center and a 24-hour government intelligence operations center. If successful, the program will lead to an operational system, subject to funding.

- **Enhanced Security Measures for Highly Hazardous Materials** - TSA is taking a risk-based approach to identify high risk substances and working with industry and government stakeholders to develop voluntary measures to reduce the risk. TSA, working with Federal and private sector partners, has been collaborating to identify hazardous materials that pose the greatest risk from terrorist activities. Industry and government agencies have been sharing information to develop voluntary enhanced security measures for motor carriers transporting these highly hazardous materials by truck.
- **Federal Security Clearances for State Departments of Transportation -** TSA is working with state departments of transportation (DOT) to facilitate granting of federal security clearances for state personnel. With the proper Federal security clearance, the state DOTs can gain access to sensitive information from both state and federal sources and thereby be better prepared to act in times of crisis.
- **REAL ID Act -** The REAL ID Act was passed by Congress to address driver's licenses issuance loopholes existent in many States that allow applicants to conceal their true identify to secure a driver's license under fraudulent circumstances. The 9/11 Commission identified most of the licenses used for identification by the 9/11 terrorists as fraudulent in some respects. DHS, in cooperation with the Department of Transportation (DOT), was charged by Congress in May 2005 with instilling security elements into State driver's licensing procedures to enhance confidence in drivers' licenses as a form of identification when presented for access to official federal programs or access points. Although States may choose to **not** follow the regulations that are established, only non-REAL ID compliant licenses will not be accepted as valid identification by Federal agencies beginning May 11, 2008. Since State driver licenses are the base document authorizing commercial drivers licenses (CDL), this measure will also reduce fraud in CDL issuance.
- **Hazmat Threat Assessment** - TSA implemented the Hazmat Threat Assessment Program to meet the requirements of Section 1012 of the USA PATRIOT ACT, which prohibits States from issuing a Hazardous Materials Endorsement (HME) on a CDL without first determining whether or not an individual seeking to transport hazardous materials poses a security risk. TSA requires commercial drivers who seek to apply for, renew or transfer an HME on their State-issued CDL to undergo a security threat assessment administered by TSA. This assessment includes a fingerprint-based FBI criminal history records check, an intelligence-related check and immigration status verification.
- **Federal Law Enforcement Center Training (FLETC) of Roadside Enforcement Officers** - TSA sponsored the creation of a training curriculum developed by FLETC to instruct State, local and municipal law enforcement officers to recognize, report and interdict efforts to use commercial truck or bus resources as targets of or tools for delivery of terrorist attacks. Starting with officers who are currently engaged in roadside safety enforcement, training is focused on interview techniques, behavior pattern recognition and fraudulent document identification. Trainees are also provided with lines of reporting responsibility that may be distinctly different and in addition to standard criminal reporting.

Rail Security

The United States DHS and the TSA have primary responsibility for transportation security, with the Federal Railroad Administration (FRA) providing support in the railroad sector. TSA works closely with the FRA and the railroad industry on a daily basis in addressing railroad security issues.

Privately-owned freight railroads connect industries and businesses with each other across the country and with markets overseas, moving 42 percent of all intercity freight, as measured in ton-miles, including 67 percent of the coal used by electric utilities to produce power, and chemicals used in manufacturing and water purification. Seven Class I railroads haul over 90 percent of the rail cargo in the United States, with the remaining 10 percent being transported by 30 regional railroads and over 500 local railroads. Typically railroads move about 1.7 to 1.8 million carloads of hazardous materials (hazmat) yearly, with roughly 105,000 of these carloads being toxic inhalation hazard (TIH) materials, such as chlorine and anhydrous ammonia.

The major freight railroads developed and adopted security plans beginning in 2002 based on comprehensive risk analyses, and the best practices of the Intelligence Community, that address the security of not only hazmat but of freight in general. The Association of American Railroads (AAR) has established guidance for the freight railroads in the form of a model strategic security plan. The railroad industry has also developed a detailed protocol (AAR Circular OT-55-I) on recommended railroad operating practices for transportation of high-risk hazardous materials (including TIH). FRA, TSA, and the Pipeline and Hazardous Materials Safety Administration (PHMSA) have jointly worked with the railroad industry to build upon the railroads' security efforts through vulnerability assessments, development of voluntary security action items, and rulemakings.

Regulations are currently in-place that require each shipper and carrier of significant quantities (amounts requiring a placard) of hazmat to adopt and comply with a security plan. Under this regulation, security plans must include an assessment of security risks and appropriate countermeasures or mitigation strategies, or both, to address those risks. The plans must, at a minimum, address three specific areas: the security of company personnel; unauthorized access to company property; and the security of hazmat shipped or transported by the company from its origin to its destination. Both DHS and DOT have proposed rulemakings in development that would enhance the security planning requirements and would require specific operational procedures to enhance the security of high consequence materials such as explosives and toxic inhalation hazards.

Where rail security involves port facilities or infrastructure regulated under the MTSA of 2002, the regulated facilities are required to consider rail security in their Facility Security Plans. Similarly, where rail security falls under a geographic area in which an AMSP is required, the AMSP is required to include it. However, this does not entail the direct inclusion of the rail plans and may merely be its acknowledgement and alignment. Such alignment is best accomplished through participation by the rail industry in the appropriate AMSC.

Air Cargo Security

TSA employs a multi-layered system in air cargo. By not relying on any single security initiative, the Department seeks to strengthen the entire system and introduce unpredictability that can't be manipulated. The layers TSA employs in air cargo include;

- Allowing only known shippers to offer cargo for passenger-carrying aircraft.
- Using canine teams throughout the cargo system.
- Deploying hundreds of dedicated cargo-only aviation security inspectors to conduct scheduled and unscheduled compliance inspections in cargo facilities.
- Requiring air carriers to physically inspect some cargo.

In addition to the above measures, TSA utilizes transportation security officers at over 250 small airports to screen all cargo at these airports and requiring random screening in addition to the above measures.

Rules changes made in November 2006 require high risk cargo to be 100 percent screened just like checked baggage before being placed on passenger aircraft. This includes packages presented to air carriers at the airport or other facilities and packages requested to be placed on a specific flight. Additionally, TSA removed all exceptions for screening air cargo on passenger planes. Absolutely all cargo is eligible for screening without exception.

PERFORMANCE MEASURES

Measuring the effectiveness of the various program implementations requires metrics specific to the objectives of the programs. For the primary programs, the measures of effectiveness are displayed in Table 3.

INCENTIVES FOR VOLUNTARY PRIVATE SECTOR MEASURES

Through voluntary programs such as C-TPAT, the private sector is able to improve security, optimize performance and reduce the risk of loss and unauthorized access of their goods that are moving through the global supply chain. This translates into greater supply chain integrity and stronger brand recognition.

C-TPAT also provides private sector companies with an opportunity to help the U.S. government in protecting the homeland and global supply chain against acts of terror.

In return for securing their supply chain, CBP provides C-TPAT members with certain incentives or benefits. The chief benefits of participation in C-TPAT are:

- Eligibility for participation in special programs, such as:
    - The Importer Self-Assessment Program (ISA) and removal from audit pools.
    - Participation in Customs' Automated Commercial Environment (ACE).
    - Account-based monthly/bi-monthly payments.
    - The Free And Secure Trade (FAST) program on the United States/Canada and Unites States/Mexico borders.

Program	Reference Page No.	Goal	Metric
Automated Targeting System	69	100% Screening[21] of Inbound Cargo Containers	Percent screened.
International Port Security Program	70	Assess effectiveness of anti-terrorism measures in foreign ports (as described in Title 46 U.S.C. Section 70108).	Percentage of ports assessed.
		Reassess foreign ports every three years.	Percentage of ports assessed.
Customs-Trade Partnership Against Terrorism	63	Certification of all Tier-1 C-TPAT applicants within 90 days of application.	Percentage of certifications completed within 90 days.
Customs-Trade Partnership Against Terrorism (cont.)		Validation of all Tier 1 C-TPAT participants within 1 year of certification.	Percentage of validations within 1 year.
		Revalidations of all C-TPAT companies not less than once every four years.	Percentage of companies revalidated within 4 years.
Container Security Initiative	67	Conduct 100% manifest reviews prior to containers being loaded on vessels destined for United States.	Percentage of manifest reviews completed.
Radiation Portal Monitors/Non-Intrusive Imagine Devices	39	Deploy RPM and NII devices to scan at least 98% of containers entering the United States by sea.	Percentage of containers scanned.

Table 3: Program Performance Measures

- A reduced number of inspections (resulting in reduced border transit times).
- Front-of-the-line privileges.
- Being part of CBP's overall business continuance model that will allow cargo to move during trade resumption scenarios.
- An assigned Supply Chain Security Specialist.
- Access to the C-TPAT membership list.

[21] "Screening" is defined as a visual or automated review of information about goods, including manifest or entry documentation accompanying a shipment being imported into the United States, to determine the presence of misdeclared, restricted, or prohibited items and assess the level of threat posed by such cargo.

Participants avoid the possible consequences of non-participation, including possibly greater cargo scrutiny, additional examinations, more reviews and audits, and more requests for information.

INTERNATIONAL STANDARDS

As described earlier, the IMO produced the ISPS Code that went into effect in July 2004. The ISPS Code contains both mandatory and guidance sections for security of vessels and port facilities. For the majority of the world that trades by sea, the ISPS Code remains the premier security regime in the maritime mode of transport.

The WCO is an international body that provides a mechanism for countries to coordinate activities of customs administrations. As the premier international body for customs matters, the WCO has a great interest in supply chain security. In June 2005 the WCO published the *Framework of Standards to Secure and Facilitate Global Trade* (the "SAFE Framework"). The WCO Framework was developed with four principles in mind: 1) the commitment to harmonize the advance electronic cargo information requirement on inbound, outbound, and transit shipments; 2) the application of a consistent risk management approach to address security threats; 3) the preferable use of non-intrusive detection equipment to effect Customs examinations of high-risk containers and cargo; and 4) the provision of benefits to businesses that meet minimum supply chain security standards and best practices. This voluntary framework sets security standards in two pillars: the customs-to-customs network arrangements and the customs-to-business partnerships.

In June 2006, the WCO approved and published guidelines for authorized economic operators (AEOs) to operate under the SAFE Framework. The AEO concept is designed to be the international set of standards that leads to mutual recognition by Customs authorities. The AEO concept will give customs benefits to companies that volunteer to maintain stringent supply chain security standards as set out by Customs Administrations. A premise of the concept is that participants will require their business partners to also improve their security practices, thus promoting security up and down supply chains. CBP's C-TPAT is an example of an AEO program.

The United States government, led by CBP and the USCG, is currently working to link the new initiatives of the WCO to the established structures of the IMO. The goal is to further strengthen security measures within the maritime domain, which is an important link and convergence point of most international supply chains.

Additionally, as trading partners establish their supply chain security programs the United States Government, through the Department of State and CBP, are seeking to establish mutual recognition agreements with them. Such agreements, negotiated on a bilateral, government-to-government basis, will significantly streamline the validation processes of AEOs.

The International Organization for Standardization (ISO) has also contributed a series of standards to improve supply chain security. ISO has produced Publicly Available Specifications (PAS) on security management systems, best practices for implementing supply chain security, requirements for bodies providing audit and certification of supply chain security management systems, and other topics. These specifications give

industries around the globe a standard starting point to work on improving supply chain security, without having to design the standards from scratch. The specifications may be recognized or adopted by governments, thus giving industry an incentive to work towards improved security. Implementation of these recognized standards is a factor used in evaluating the security processes of C-TPAT participants, and as appropriate they may be included by reference into agency regulations.

Applicable ISO/PASs include:

- ISO/PAS 17712, Freight Containers – Mechanical Seals.
- ISO/IEC 18000 (series), Information Technology – Radio frequency identification for item management.
- ISO/FDIS 18185 (series), Freight containers – Electronic seals.
- ISO/PAS 28001, Specification on Best Practices for Implementing Supply Chain Security, assessment and plans.
- ISO/PAS 28003, Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems.

IMPLEMENTATION SCHEDULE, PRIORITIES, AND MILESTONES

Calendar Year 2007:	Publish second Final Rulemaking implementing Transportation Worker Identification Credential access requirements and the use of electronic readers.
April 11, 2007	Publish updated guidelines for C-TPAT Tier 1 participants.
April 11, 2007	Publish updated guidelines for C-TPAT Tier 2 participants, including validation schedules.
July 10, 2007	Initial report to Congress containing the *Strategy to Enhance International Supply Chain Security*, including resumption of trade protocols.
December 31, 2007	Scan at least 98 percent of all containers entering the United States by sea for radiological and nuclear material, using Radiation Portal Monitors and Non-intrusive Imaging Devices.
December 31, 2007	All containers entering 22 highest volume United States ports to be scanned for radiation.
January 1, 2008	IMO regulations on Long Range Identification and Tracking of vessels enter into force.
March 31, 2008	Complete initial round of foreign port assessments to determine the effectiveness of anti-terrorism measures.
September 25, 2008	Transportation Worker Identification Credentials required for maritime workers requiring unescorted access to secure areas of port facilities, outer continental shelf facilities, and vessels regulated under the Maritime Transportation Security Act of 2002.

October 13, 2008	Publish C-TPAT Tier 3 participant criteria, including benefits.
December 31, 2008	Long Range Identification and Tracking (LRIT) of vessels operational with respect to the transmission of LRIT information by ships.
Calendar Year 2009	Salvage Response Plans and port-level resumption of trade considerations incorporated into Area Maritime Security Plans.
July, 2010	Final *Strategy to Enhance International Supply Chain Security* publication and delivery to Congress.

IX. RESPONSE AND RECOVERY

Many types of incidents or threats may have significant impact on the ability of cargo to move throughout the United States transportation system including transportation disruptions (such as TSIs and large-scale natural disasters) and others. Response to significant incidents will be conducted under the NRP.

Response activities include measures and operations to neutralize or counter a continuing active threat, to minimize damage to life and property from the effects of the incident and support basic human needs, to stabilize the situation (i.e., prevent further damage or threats), and to maintain the supply chain infrastructure and flow of trade.

For the purposes of this strategy, response to support resumption of trade consists of those measures, operations and activities in incident areas that are needed to set the stage for recovery activities as described in a later section.

Response addresses the short-term, direct effects of an incident or incidents, including activities that are elements of both response and recovery, such as infrastructure damage assessments.

There is an unclear line between actions that are considered "response" and those considered "recovery" in any given situation. Therefore, close cooperation within the unified command structure will be necessary to correlate, coordinate and optimize performance of response and recovery tasks. In this regard, determination and assessment of infrastructure impacts and transportation disruptions must be designed to concurrently support assessment of the primary and secondary effects of an incident including supply chain interdependencies.

LEAD AGENCY MISSION EXECUTION.

The Federal lead agency for overseeing and coordinating mission execution is the Department of Homeland Security.

Incident Management.

Incident management activities will conform to the NRP and the NIMS structures and processes. Specific agency roles are delineated in the NRP, as well as other applicable national strategies, directives, plans and protocols. Resumption of Trade measures and incident support activities in non-incident areas will normally observe steady-state coordination and communications unless otherwise directed by DHS.

Incident Command.

This strategy requires use of an all-hazard-compatible ICS process.

Incident command for actions taken in response to nationally significant incidents will conform to NRP and NIMS structures and processes.

Consistent with the basic premise of the NRP that incidents are generally handled at the lowest jurisdictional level possible; incident command will be exercised at that jurisdictional level, consistent with applicable laws and regulations.

Incident command will be supported by the NRP coordinating structures observing applicable protocols and procedures.

Unified Commands.

A Unified Command (UC) will be established in advance of actual incidents insofar as is practicable, for example, for forecast landfalls of major hurricanes.

For no notice incidents, initial response will be through existing steady-state operations and implementation of first response and contingency plans and protocols. A UC will be implemented as soon as is practicable thereafter.

Entities identified through preparedness planning will provide subject matter experts, technical and administrative personnel needed to staff the UC.

The UC will mobilize appropriate Federal, State, local and tribal governments as well as private sector organizations to support response and recovery operations.

The UC will be supported by coordinating structures and ESFs under the NRP.

Identification of Appropriate Initial Incident Commander (IC).

The IC will often be prescribed or pre-designated by statute, regulation, policy, agreement or other applicable directive.

The initial IC will normally be an organizational entity with first response jurisdictional authority and capabilities consistent with NRP constructs and applicable laws and regulations. IC responsibility may shift as an incident evolves.

The Incident Commander may or may not be a Federal official. In certain circumstances, a Federal official may be required to serve as IC.

For TSIs in or near ports or coastal areas generally involving vessel and maritime cargo movement/supply chain transportation disruptions, the USCG COTP will typically serve as IC.

COTPs have lead responsibility for determining restrictions on port operations, and authorizing movement of vessels, during and following an emergency affecting the port community.

Where the maritime element of incident management is an element of a cross-jurisdictional incident for which an individual from another entity is serving as IC, the COTP will serve as supporting IC or component commander for maritime elements of incident management.

Utilization of Recovery Units under the NIMS.

A recovery unit should be established in the ICS Planning Section. The unit will be responsible for planning infrastructure recovery and resumption of trade for transportation disruptions and for coordinating these plans with the Operations Section and the Incident/Unified Command.

Guidelines for the Recovery Unit Leader role are contained in the USCG Incident Management Handbook, COMDTPUB P3120.17 series, which is adopted for use in support of this strategy.

Recovery Unit activities will be supported by application of all-hazard-compatible facilitation of recovery coordination arrangements and Salvage Response Plans and procedures contained in AMSPs as well as oil and hazardous materials mitigation provisions of Area Contingency Plans (ACPs) for coastal areas.

LEAD AGENCY MISSIONS.

DHS, as lead agency, will exercise overall lead under this strategy.

- DHS will provide national level policy and coordinating guidance through NRP and steady-state structures per the NRP and it's supporting national-level plans and directives.
- DHS will assess the situation and set and disseminate the appropriate HSAS level.
- DHS will determine, in consultation with supporting agencies insofar as is practicable, whether and when to designate a developing emergency situation as an INS.

DHS will be supported in lead agency mission execution by the TSA, CBP and the USCG for transportation disruptions within their respective domains. This support will be correlated with each agency's related responsibilities as a Sector-Specific Agency responsible for Transportation CI/KR within their domains under the NIPP and its implementing directives and protocols.

Overall Coordination of Federal Activities

During a national TSI or a transportation disruption rising to the level of an Incident of National Significance, the overall coordination of federal incident management activities is executed through the Secretary of Homeland Security. Other Federal departments and agencies carry out their incident management, emergency response, and recovery authorities and responsibilities within this strategy's overarching coordinating framework.

The Secretary of Homeland Security utilizes multi-agency structures at the headquarters, regional, and field levels to coordinate efforts, and provides appropriate support to the incident command structure.

At the federal headquarters level, incident information sharing, operational planning, recovery, and deployment of federal resources are coordinated by the NOC and its component elements. Issues beyond the Secretary's authority to resolve are referred to the appropriate White House entity for resolution.

In the field, the PFO or the FCO, as appropriate, represents the Secretary of Homeland Security. Overall Federal support is coordinated through a JFO. JFO's provide support to local Incident Command structures and coordinates efforts to address broader regional impacts on the incidents. As part of the Multi-Agency Coordination System (MACS), the JFO does not supplant the on-scene Incident Command or Area Command, but supports and provides broader coordination of incident-related activities. Execution of tactical operations and coordination remains the responsibility of the Incident/Area Commander(s).

For terrorist incidents, the Attorney General, acting through the FBI, executes the primary responsibilities for coordinating and conducting all federal law enforcement and criminal investigation activities. During a terrorist incident, the local FBI Special Agent-in-Charge (SAC), or FBI Headquarters designee, coordinates these activities with other members of the law enforcement community, and works in conjunction with the PFO, who coordinates overall federal incident management activities. The framework created by these coordinating structures is designed to accommodate the various roles of the Federal government during and after an incident.

In the event of multiple incidents, a Unified Area Command may be established to oversee the management of multiple ICS organizations or to oversee the management of a very large or complex incident that has multiple incident management teams engaged.

At the local level, on-scene incident command and management organization is located at the Incident Command Post (ICP). Designated incident management officials and responders from Federal, State, local and tribal agencies, as well as private-sector and nongovernmental organizations are typically on site at the ICP. When multiple command authorities are involved in a response or recovery effort, the ICP may be led by a Unified Command, which is comprised of officials who have jurisdictional authority of functional responsibility for the incident under appropriate law, ordinance, or agreement. The ICP will be located within the immediate vicinity of the incident site, the location having been selected by the primary jurisdictional authority. Each incident will generally have a unique ICP.

SUPPORTING AGENCY MISSIONS.

Supporting agencies will implement appropriate agency and multi-organizational response and contingency plans in support of the NRP.

Incident Alerts and Notifications.

All supporting agencies will expeditiously communicate incident alert and notifications to DHS using prearranged steady-state and emergency protocols.

Essential information pertaining to transportation disruptions and associated disruptions of international trade information will be forwarded to DHS and shared with partnering agencies as available to support development of a common operational picture (COP), assessment of the situation, and DHS determinations regarding designation of the incident as an INS.

Force Protection.

Supporting agencies will implement force protection measures as appropriate.

Continuity of Operations (COOP).

Supporting agencies will implement comprehensive and effective Continuity of Operations and Continuity of Government programs in order to ensure the preservation of our form of government under the Constitution and the continuity performance of National Essential Functions under all conditions. Supporting agencies will ensure that continuity planning occurs simultaneously as programs are developed and executed to

provide for seamless execution of essential functions during normal operations and during response and recovery operations.

NRP Execution.

Supporting agencies will provide the following as required.

- Support for Incident Command Posts including an official to serve as incident commander, where appropriate.
- Support for Joint Field Offices (JFO).
- Provision of PFO when directed by DHS.
- Provision of SFO.
- Staffing of national-level NRP structures.

INCIDENT, DAMAGE, TRANSPORTATION DISRUPTION AND TRADE DISRUPTION ASSESSMENTS.

For incident areas, determination and assessment of incident effects within incident areas will be conducted as quickly as is practicable. This activity will be coordinated under the UC when established and communicated through NRP structures. Prospective effects to transportation and international trade will be determined insofar as is practicable, consistent with overriding response requirements.

For non-incident areas, the incident effects on transportation and international trade will be determined using steady-state structures. A Unified Command may be established to support resumption of trade if necessitated by the tempo of security and recovery activities in non-incident areas.

Transportation Security Administration (TSA).

The TSA will provide oversight and management of appropriate response actions within the aviation and surface transportation sectors, in accordance with the NRP and the various transportation sector specific plans.

Transportation Security Administration Federal Security Directors (FSDs) and Assistant FSDs for Law Enforcement will coordinate emergency response operations on behalf of TSA.

As necessary, TSA may supply operational support in the form of TSA officers, e.g. canine explosive-detection teams.

TSA will coordinate its activities with CBP and the USCG via participation in the Unified Command and/or Recovery Unit, and via the AMSCs.

United States Coast Guard (USCG).

This section will discuss only response actions associated with movement of vessels and cargo (i.e. related to the supply chain). Response activities impacting trade flow and vessel movement may include:

- Adjustments in MARSEC and Force Protection Levels for incident and non-incident areas will be considered and directed, if necessary, as a first response to

significant incidents. However, such actions will be taken in a deliberate and measured fashion, based on the type of incident or threat, so as to balance security concerns with facilitation of trade and to minimize disruptions to trade flow.

- The USCG will conduct time-sensitive incident notification in accordance with pre-established protocols, including immediate direct communication by field units to the USCG national command center, and interagency consultations and coordination per Maritime Operational Threat Response (MOTR) protocols.
- The Commandant, USCG, will set appropriate MARSEC and Force Protection levels.
    - The USCG, in consultation with CBP, will implement National Response Options Matrix (NROM) protocols based on available information.
    - The NROM consultation will assess and determine the appropriate MARSEC Level, security control measures, denial of entry needs, whether any vessels need to be expelled from United States ports and waters, and force protection conditions.
    - For urgent situations, the local COTP has been authorized to make unilateral MARSEC changes as a security control measure in advance of national-level MARSEC determinations.
    - All MARSEC determinations will consider the HSAS level, risk, threat, and prospective effects on transportation and trade. Increases in MARSEC Levels will be localized and targeted to the maximum extent practicable consistent with the situation.
- The USCG will implement security risk mitigation measures in both incident and non-incident areas. In incident areas, this activity generally takes the character of prevention measures conducted concurrently, and in some case in conjunction with, response operations as resources permit. Maritime security measures in non-incident areas will normally be conducted as a prevention activity to minimize transportation and trade disruptions.

  Maritime security measures include, but are not limited to:

    - Waterborne, shoreside, and aerial patrols.
    - Security boardings.
    - Vessel escorts.
    - Establishment and enforcement of fixed security zones.
    - Establishment of offshore presence.
    - Surge operations.
    - Investigation of anomalies.
    - Control of port access, activity and movement.
    - Deployment of specialized antiterrorism and counterterrorism assets.

- Military outload security support.
- Fulfillment of COTP and FMSC responsibilities.
- Implementation of procedures for response incorporated into AMSPs and supporting FSPs and VSPs.

The USCG will conduct agency-specific response according to predetermined plans and procedures within incident areas.

For the purposes of this strategy, response activities will seek to establish a basis for resumption of trade within incident areas and to support interim resumption of disrupted cargo flow through non-incident areas.

Response at the incident command level will be guided by the USCG Incident Management Handbook (USCG IMH), COMDTPUB P3120.17 series, which is adopted for use in support of this strategy. The USCG IMH incorporates linkages to applicable response and contingency plans, directives, policies and other documents.

Determination and assessment of incident effects to the MTS within incident areas will be conducted as quickly as is practicable. This activity will be coordinated under NRP constructs when implemented.

The USCG will conduct incident, damage and transportation disruptions assessments within its functional and mission areas of responsibilities.

The USCG, as the Sector-Specific Agency (SSA) for maritime CI/KR, will serve as the maritime domain central point of contact for facilitating determination and assessment of incident effects on the MTS and its included maritime CI/KR.

Assessments will be designed to develop information needed for response operations and to support recovery planning, including resumption of trade. Insofar as capabilities, resources, and available information permit, this will include planning for incident and non-incident areas and include:

- CI/KR Sector trade interdependencies.
- Associated incident effects.
- Recovery needs (for both principal government and industry stakeholders).
- Recovery capabilities (for both government and industry stakeholders).

Stakeholder entities, such as the AMSC and Area Committee (AC), may provide advisory service in a supporting role to the UC within the incident area and may also make members available for service in UCs.

The determination and assessment of incident effects to the MTS outside of incident areas will be conducted as a recovery activity through regional and national incident management structures, as well as through normal modalities, e.g. the normal industry assessment and response process to port infrastructure capacity changes.

U.S. Customs and Border Protection (CBP).

CBP is responsible for screening and evaluating cargo, crew, and passenger movement into and out of the United States. CBP and the USCG will work jointly to make initial cargo and vessel movement response decisions and to execute those decisions in a coordinated fashion in order to minimize the initial impact on trade flow and to resume normal trade flow as quickly as possible. Similarly, CBP and the TSA will work jointly to address air cargo issues.

CBP will consult with the USCG regarding MARSEC Levels and implementation of National Response Options Matrix (NROM) protocols based on available information.

During Incident Response in the maritime environment, CBP will perform several important functions. These include acting as a supporting agency to the USCG in local response, implementing their own Incident Management directives, activating the National Response Options Matrix (NROM) in conjunction with USCG , and depending on the impact of the incident, carrying out additional responsibilities as set forth in the NRP.

First, at the local level, CBP will participate in the Unified Command with the USCG and other agencies and will contribute personnel and assets as applicable and according to the magnitude of the incident. For a relatively small incident this may be confined solely to the Incident Command and a moderate participation in, for example, the Operations Section. For a significant incident this may include robust participation in the Incident Command, Joint Field Office, and all ICS Sections. If necessary, CBP can also move designated mobile response teams to the affected port.

Second, CBP will activate plans to manage incident response both internally and externally. Internally the agency will activate its Incident Management Coordination Directive, heightening CBP's ability to maintain situational awareness, develop various courses of action for agency leadership, and implement incident response. At the headquarters level CBP may also participate in the DHS Incident Management Planning Team through both its standing and augment staff.

Externally, CBP and the USCG will jointly activate the NROM. The NROM will provide the Commandant and Commissioner with a menu of immediate, pre-planned security response options to implement throughout the maritime transportation system. This will allow the system to remain open, although at a heightened security level, in order to allow cargo to flow while working to prevent a second or subsequent attack.

Finally and also at the national level, should the incident rise to the threshold of an Incident of National Significance and initiate activation of the NRP, CBP may find itself in the role of force provider. As the largest law enforcement agency in the United States Government, CBP will likely make a large contribution to ESF #13, Public Safety and Security. Other supported ESFs may include Search and Rescue, Transportation and Communications. As outlined in the NRP, ESF assignments will be coordinated by the NRCC. Deployed ESF resources will flow to the affected area and, under the authority of the CBP SFO at the JFO, be tasked for support of local and federal responders.

Federal Emergency Management Agency

As the lead component within the DHS for managing federal response and recovery efforts following any national incident, the Federal Emergency Management Agency will coordinate all NRP activities in accordance with the NRP.

Immigration & Customs Enforcement

ICE has a history of supporting other Federal, state, local and tribal agencies and organizations during declared emergencies and disasters though the NRP ESF process. As required by the NRP, during Robert T. Stafford Act supported/funded incidents of national significance or other designated incidents, the ESF process is utilized to accept and execute appropriate mission assignments to support our nation. ICE shall provide resources for response and support in anticipation of or during an incident through the ESF process. All mission assignments shall be authorized by the ICE Office of the Assistant Secretary prior to acceptance and coordinated through the National Incident Response Unit (NIRU) for tracking purposes. Even though ICE-accepted ESF mission assignments are often coordinated through ESF-13 Public Safety and Security, ICE may accept mission assignments from any ESF to support the NRP.

Dispute Resolution

Disputes will be resolved at the lowest organization level possible, consistent with NIMS principles and NRP constructs where in place, and through steady-state constructs elsewhere. Disputes that threaten the continuity, integrity or safety of response and recovery operations will be resolved immediately, or if this cannot be accomplished, immediately referred to the next higher organizational level with sufficient information to support decision making.

RECOVERY

LEAD AGENCY MISSION EXECUTION:

Following an incident that severely impacts the transportation system, the overall coordination of federal incident management activities is executed through the Secretary of Homeland Security.

The DHS goals following an Incident of National Significance (INS) that adversely impacts the transportation system are two fold:

- Facilitate achieving the optimum balance between ports, waterways, and cargo security, and the recovery of transportation capabilities.
- Minimize disruption to the United States economy from unnecessarily constrained cargo flow.

When dealing with the resumption of commerce and recovery of the transportation system, it is important to understand that the incident management activities will have two distinct aspects:

- Recovery of infrastructure components that have been damaged or rendered inoperable due to the incident.

- Application of security measures or other assurance that components of the transportation system, both within the incident area and the non-incident ports, are secure in order to provide a sufficient level of confidence that future movements of cargo and conveyances will not pose a substantial risk of additional attacks or incidents.

Incident Command per NIMS

Recovery actions following an incident of national significance that significantly impacts the functionality of the transportation system or the ability of cargo to flow through the transportation system will be carried out in accordance with the NRP and the NIMS as part of the overall response management system. At the incident site/area, recovery actions typically occur simultaneously with response actions within the first few days, and may continue for many weeks or even months. Non-impacted ports may also be involved in execution of recovery actions to support the overall national effort to facilitate rapid trade resumption.

Coordination of Federal Activities

The simultaneous conduct of incident response and recovery operations, the restoration of passenger and cargo flow, add a new dimension for federal decision makers. Therefore, a JFO, separate from the JFO supporting response operations at the incident site, may be established to support the coordination of recovery operations with Federal, State, local, tribal, nongovernmental and private sector organizations. This is consistent with the potential for the scope and complexity of an incident to create a demand for multiple JFOs.

Identification of Appropriate Incident Commander

When multiple command authorities are involved in a response or recovery effort, which will be the case following an INS, a Unified Command will be established which is comprised of officials who have jurisdictional authority or functional responsibility for the incident under an appropriate law, ordinance, or agreement.

Notwithstanding the Unified Command concept, USCG COTPs fulfill a unique role in supporting the Department of Homeland Security's overall responsibility for recovery of the MTS and resumption of commerce. COTPs/FMSCs have lead responsibility for determining re-opening of port facilities and movement of vessels following an emergency affecting a port community. Thus, while they will work closely with port community and agency partner stakeholders during port related response and recovery, the COTP retains the final decision authority for planning and executing port re-opening or vessel movement priorities at the field level. USCG COTPs are therefore designated as the appropriate field level incident commander to lead MTS recovery, port re-opening, and vessel movement actions. Specific roles and responsibilities of the USCG for the resumption of trade and recovery of the MTS are outlined on pages 10 and 11 of the MIRP.

Utilization of Recovery Units under the NIMS

NIMS provides a standardized yet flexible response management system that is sized and contains various elements appropriate to the needs of each specific incident. Following

incidents of national significance that significantly disrupt the transportation system and/or commerce flow, the local level incident command structure must include a precise focus on infrastructure recovery and commerce resumption. To address this need, a Recovery Unit will be embedded within the Planning Section of the Incident Command organization. The purpose of the Recovery Unit is to track and report on the status of the transportation system, understand critical recovery pathways, recommend courses of action, provide all stakeholders with an avenue of input to the local response organization, and provide the Incident/Unified Command with recommended priorities for cargo resumption in accordance with this strategy.

Private sector involvement with the Recovery Unit is especially critical. The private sector possesses both the best information on inbound and outbound cargoes and day-to-day capabilities within the transportation sectors to identify alternate cargo processing sites. While the private sector will generally coordinate via AMSCs, a more direct engagement will also be warranted.

Expansion of Recovery Guiding Bodies to Regional/National Levels

While recovery management at the impacted area will be managed by a Unified Command, large scale incidents will almost certainly have impacts on cargo recovery which extend into regional or national scales. To most effectively manage these larger regional and national recovery and cargo flow issues, a Recovery Unit within the JFO Planning Section and the NOC Planning Section may be required, to assist the Response and Recovery Operations Branches.

Supporting Agency Mission Execution

Although the Secretary of DHS has the responsibility for the overall coordination of federal incident management activities following an incident that affects the transportation system, there are many other agencies inside and outside of DHS that have significant roles and responsibilities.

The identified agencies carry out their responsibilities by integrating into the local incident command response/recovery organization, the Joint Field Office/regional support organization, or the national response/recovery system elements, as appropriate, both for the impacted and the non-impacted areas.

Dispute Resolution

The multi-agency and highly complex nature of transportation system recovery management and commerce resumption operations is prime breeding ground for disputes among agencies with authority and responsibility for various aspects of incident response and recovery. Table 4 indicates the primary avenues of dispute resolution depending on the level of the response/recovery organization that the dispute occurs.

Protocols for the Redeployment of Resources as Necessary to Reestablish Trade

At the field level, for the incident site/region, resources are allocated by the incident/unified command organization to execute initial recovery. If a JFO is established, the PFO and the JFO Coordination team may become involved in making resource allocation decisions within the impacted site/region to ensure the recovery effort is properly aligned with regional or national priorities. If the incident site requires

resources beyond the scope of the responding JFO and COTP/FMSCs, those needs are addressed per the NRP by national level NRP elements or by each individual agency's leadership as appropriate.

	Key Government Stakeholders	**Dispute Resolution Forum/ Entity**
National Level	Federal agencies with jurisdiction and responsibility for matters affecting post-incident resumption of trade (see Chapter 8 and MIRP for listing of agencies)	1. Domestic Readiness Group 2. Secretary of Homeland Security 3. White House/Homeland Security Council
Regional Level	Agencies Participating in the JFO	1. JFO Coordination Group/PFO 2. Domestic Readiness Group or through appropriate agency chains of command for consideration by higher authority
Field Level	Federal first responders, State, local, and tribal agencies with authorities and jurisdiction for matters affecting post-incident resumption of trade (see Chapter 8 and MIRP for listing of agencies)	1. Unified Command principles to gain consensus 2. Agency with primary jurisdiction or functional responsibility over the matter in dispute makes final decision

Table 4: Dispute resolution

Resources may also need to be reallocated among the non-impacted ports nationally to best facilitate rapid resumption of trade flow (which equates to rapid screening, inspection, and authorization for entry for both cargo and vessels). Resources may be needed to carry out additional security measures associated with cargo/vessel movement, or simply to handle increased scanning or inspection volume created by infrastructure damage or delays at the incident site/region. Since each situation is unique, it is not possible to prescribe ports that will receive additional resources to scan, inspect, and clear cargo and vessels following an incident. The Commandant of the Coast Guard and the Commissioner of Customs will jointly monitor the strategic status of maritime trade flow to determine resource adjustments necessary to ease critical delays or shortages using the steps outlined in the MIRP (pages 32-39). Strategic trade flow elements of information include items such as:

- A delay in the movement of vessels/cargo at the incident site that is creating significant negative regional or national impact with regard to specific commodities.
- Similar delays in non-incident port(s).

- A regional or national need for specific commodities.
- The availability of non-incident port(s) that can accommodate increases in trade flow for specific commodities.
- The identification of alternate port(s) preferred by the private sector to re-route specific commodity vessels or cargo.

The Commandant of the Coast Guard and the Commissioner of Customs will consult one another regarding national priorities for adjustments in trade flow and plans to reallocate resources to non-incident site ports. This will ensure that both vessel screening/inspection/clearance resources and cargo screening/inspection/clearance resources are augmented jointly as needed and in alignment with the national strategic purpose. Coordination will be conducted with the DOT, TSA and infrastructure owners (e.g., terminals, transportation providers, etc.) with respect to intermodal connection of cargo movement via rail, highway and pipeline from/to the port cargo terminals.

RESUMPTION OF TRADE

In general, trade may be viewed as entering or departing the United States via one of three modalities: surface transportation (rail or vehicular), air transportation, or the maritime domain.

It is the policy of the DHS that a response to a terrorist incident will not be an automatic shutdown of the Nation's air, land, or sea ports. A prudent and measured response will be taken based on an assessment, including available intelligence, of incident specifics. In all modalities, elevated security activities triggered by the HSAS or by modality specific threat conditions (e.g., MARSEC Levels in the maritime domain, or an increase in the HSAS for a transportation segment such as aviation) will be used to achieve an appropriate level of security. The response to an incident must not unreasonably hinder the free flow of goods, while simultaneously reducing risk to an acceptable level.

To accomplish this objective, it is critical that pre-existing data and screening systems include the necessary information to fully screen cargo, including cargo already in transit and requiring additional risk-based analysis in a post-incident environment.

As outlined previously in Section VIII, Strategic Elements, multiple programs exist to ensure that appropriate information is obtained and screened during normal operations. This data will be used by the Recovery Unit, as discussed previously in this section, to establish priorities for cargo and commodity flow during a resumption or continuation scenario. Management of response and resumption of trade will therefore be accomplished wholly in accordance with the NRP.

As required by the SAFE Port Act, this strategy focuses on trade resumption and prioritization of maritime cargo, which represents 95 percent of the cargo tonnage that comes to the United States, and on container movement in specific. The final version of the strategy will be broadened to encompass air and surface modalities.

DHS components and agencies with trade-related missions (e.g., the USCG and CBP) are responsible for the development and execution of tactical plans intended to foster business continuations and provide for elevated security conditions. Such tactical plans

will be or have been developed with input from the trade community, though the final plans may by the nature remain classified or sensitive.

Protocols and Factors for Prioritization of Resumption of Trade:

At the local level, for the incident site or region, the Incident Commander or Unified Command will work with local stakeholders to analyze conveyance and facility specific information and needs, including local priorities for bidirectional commodity flow. Additionally, (for security related incidents), the Incident Commander or Unified Command will work with the USCG, CBP, and the TSA to integrate cargo/commodity and vessel screening, inspection, and clearance processes. This ensures the actions of all agencies to authorize and sequence conveyance and cargo/commodity movements are aligned with established priorities. Regional and national priorities will be integrated into the local decision making process when they are communicated by the JFO, DRG, or in some cases agency leadership.

Local prioritization for cargo or commodity movement is based on several factors:

- The security status of the vessel.
    - Is the vessel cleared for entry into a United States seaport based on established or incident specific screening procedures?
    - Are resources available to inspect or otherwise clear the vessel for entry, if necessary?
    - Is any of the cargo on the vessel suspect, or deemed 'high risk' by CBP's ATS using any new revised risk scoring based upon the incident?
    - Are resources available to implement required security measures on the vessel's inbound and outbound transit?
    - Is the vessel operated by a trusted partner, such as a validated participant in the C-TPAT program?
- The ability of vessels to transit to and from its berth.
    - Are there berthing/space/facility issues?
    - Are there waterway functionality issues (no obstructions, operating Aids to Navigation (ATON), etc.)?
- The capacity of the port infrastructure to offload the cargo or commodity and move it from the port.
    - Are there labor issues?
    - Are there inter-modal issues?
    - Are there space or facility issues?
    - Is there CBP resource availability to clear cargo or commodities once landed?
- Commodity needs.
    - What are the national priorities?

- What are the regional priorities?
- What are the local priorities (seasonal, etc.)?

- The need for the vessel to move cargo out of the port (e.g., grain shipments needed to be shipped in order to avoid shutting down other transportation modes such as railways).

These factors must be continually assessed and integrated by the Incident Commander/Unified Command, in consultation with the USCG COTP/FMSC, the CBP Port Directors, the TSA Federal Security Director, ocean carriers, and terminal operators to establish daily priorities for vessel/cargo movement both into and out of port.

At the national level, the Secretary of Homeland Security, the DRG, or agency leadership as appropriate may set national priorities for vessel and cargo movement based on the incident specific and extended impacts. The Commandant of the Coast Guard, the TSA Administrator, and the Commissioner of CBP will continually assess the security or intelligence status, as the situation dictates, to make adjustments to nationally established security requirements for cargo and vessels. This may include changes in security levels and/or changes in the risk factors (or weights on the risk factors) to be assessed in the vessel, cargo or commodity screening and clearance processes. This assessment will be coordinated with the Department of Transportation with respect to intermodal connection of cargo movement via rail, highway and pipeline from/to the port cargo terminals.

National commodity priorities may cover, but are not exclusive to:

- Emergency Needs: those goods necessary for the saving and continuation of life. Examples include personnel and supplies for medical response, restoration of power, and potable water.
- Response Needs: personnel and equipment necessary to conduct response operations at the incident site (i.e. fire boats).
- Community Needs: the incidents may create immediate shortages of necessary commodities that must be addressed. Examples are crude oil, heating oil and chemicals necessary for industrial continuity, and drinking water. Community needs may also have a delayed time component based upon "on hand" stocks. Industry, either via the Planning Section Recovery Unit, national advisory committees, and subject matter experts must be queried to identify these commodities.
- National Security: the incident may impact national security concerns, such as cargo movements via strategic outload ports in support of Department of Defense assets, requiring specific coordination or prioritization of support assets, e.g. small vessels to conduct escort duties.

Complicating the assessment of cargo priorities is the issue of non-homogenous cargoes, where vessels are not loaded with strictly C-TPAT participant's containers. It is highly likely that high priority cargo will be intermixed with cargo not targeted for priority handling and movement, or for preferential treatment (in the case of C-TPAT participants and mutually recognized Authorized Economic Operators). In such cases, CBP efforts to

clear landed cargo will initially focus on the priority goods, then on those designated for preferential handling, and as possible on other containers.

A general decision tree to assist the Incident Command/Unified Command in prioritizing conveyances, cargoes, or commodities is given in figure 9. It is recommended that a numerical scoring system be developed by the Recovery Unit, based on port-specific conditions, to rapidly assist in prioritization.

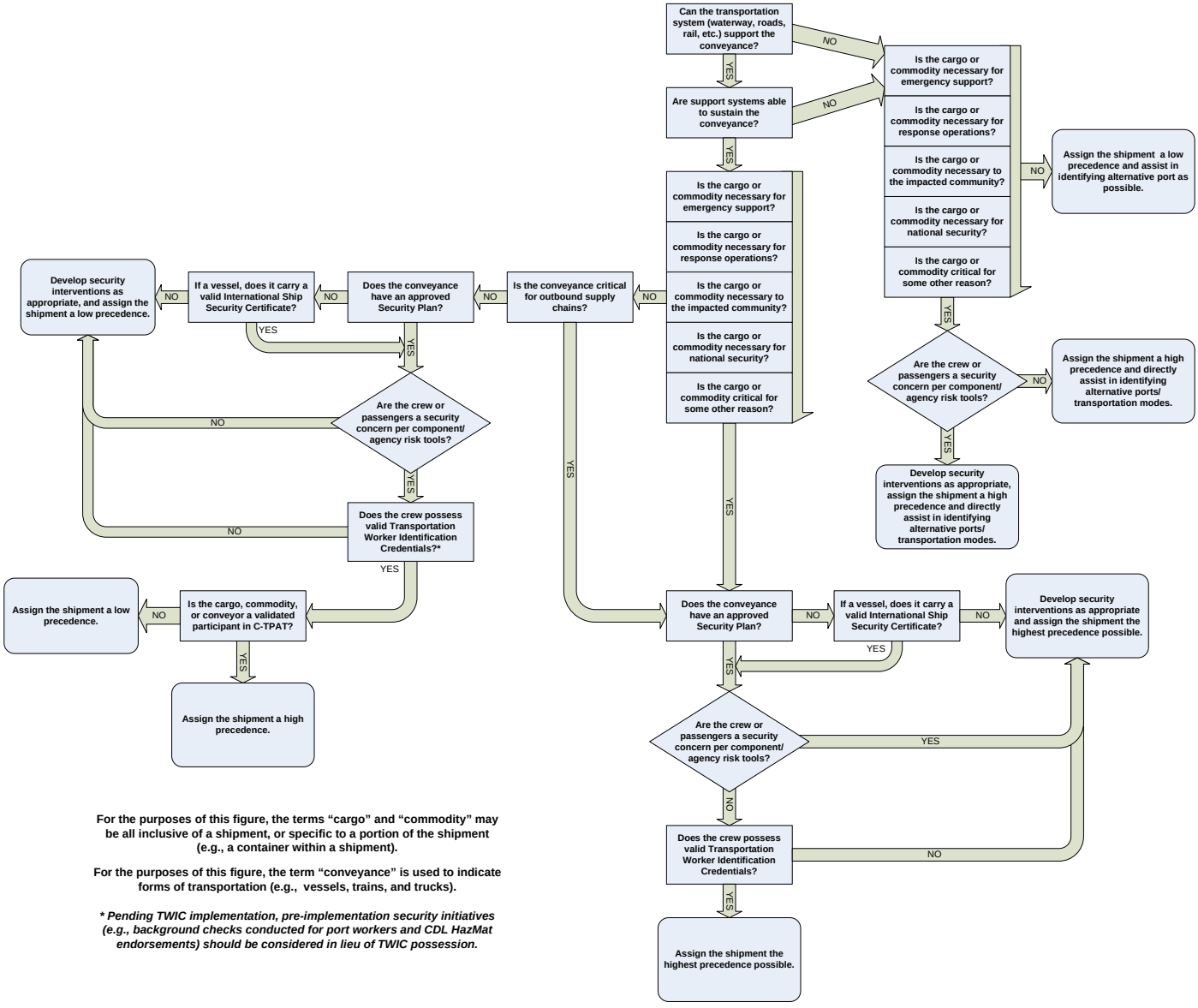


Figure 9: Conveyance/Cargo/Commodity Prioritization Decision Tree.

Vessel Prioritization

Directly following an incident, the Commandant of the Coast Guard and the Commissioner of CBP, at the national level, will determine the appropriate initial post-

incident measures to be executed to ensure the security of vessels and the cargo or commodities they carry entering the United States. Both the USCG and CBP subsequently will use risk management screening processes to determine clearance status or security measures needed for specific vessels or cargo to enter port. The USCG and CBP currently use numerous well established vessel, crew and cargo risk management tools, which are designed to identify lower risk vessels. For example, the following are some characteristics of lower risk vessels:

- Vessels with a history of compliance with safety and security regulations.
- Vessels with approved security plans.
- Vessels with no identified crew or passenger security concerns.

As a result, vessels with these attributes are more likely to gain clearance for entry more rapidly (requiring fewer or no security measures) than higher risk vessels. Conversely vessels that represent a great risk will be given a greater level of scrutiny and/or have control measures placed on them. The following are some of the existing risk based tools that USCG and CBP use to assess risk from vessels:

- Port State Control Safety and Security Matrix. A process by which vessels are scored on several factors. That score is then used to place vessels in one of four categories for risk[22]. The four categories then have scalable security measures that are applied to the vessels.
- High Interest Vessels Screening. A process that uses CBP's National Targeting Center capabilities to screen crew, vessel, and cargo information. The USCG uses a risk based tool similar to the Port State Control Safety and Security Matrix, but which uses real-time intelligence to determine high-interest vessels and crewmembers of interest[23].
- The Maritime Security Risk Assessment Model (MSRAM). The MSRAM provides COTPs/FMSCs a risk-based decision-making tool that assists in identifying critical infrastructure in U.S. ports, and allows the COTPs and their AMSCs to strategically use USCG and other law enforcement resources against the greatest risks.
- High Risk Crewmember Screening. A process in which CBP and the USCG work together to handle high risk crewmembers and to ensure that those crewmembers do not leave a vessel. High-risk crewmembers typically are those that do not have visas to enter the United States, have a prior criminal record, and are citizens of countries (called Annex VI countries) that have been determined to warrant additional monitoring in the interest of national security. If a vessel is determined to have a high-risk crewmember on board it will not be allowed to enter territorial waters or a port until a crew security plan is developed for the vessel and approved by CBP and the USCG.

---

[22] A detailed description of this process can be found in the U.S. Coast Guard Navigation and Inspection Circular 03-06. However, the tool is Sensitive Security Information and not available to the public.

[23] A detailed description of this process can also be found in the U.S. Coast Guard Navigation and Inspection Circular 03-06. However, the tool is classified SECRET and not available to the public.

INFORMATION SHARING AND COMMUNICATIONS

Recovery after an incident requires that information regarding the incident be available as rapidly as possible and continuing thereafter. Further, the information should be widely available from an authoritative source. This must include updates being promptly made and disseminated, through a variety of means which could include broadcast electronic mail, web portals, conference calls and telephone hotlines, or video teleconferencing, as appropriate. To the extent feasible, two-way communications to provide continuous feedback on questions arising from stakeholders should be enabled.

Communications and information sharing will be accomplished in accordance with the communications sections of the NRP, Section IV of the NMTSP, and where applicable the National Infrastructure Protection Plan.

A specific frequency of information transmission (sometimes referred to as 'Battle Rhythm') will be entirely dependant upon the availability of information, the means by which it is being communicated, and the availability of resources. Where possible, incident management personnel will attempt to provide for 24-hour access to information, or to negotiate an appropriate cycle to meet the needs of impacted entities such as facilities and vessels.

Intra-government

The NRP establishes a national structure for incident management with a clear progression of coordination and communication from the local level to regional and national headquarters levels. Figure 10 is a representation of the information flow between local level activities and national resumption of commerce and recovery management processes.

Additionally, for the maritime domain, agencies which participate in the national MDA program will have access to an MDA user-defined operating picture to use as the primary method for information sharing, situational awareness and collaborative planning.

Government - Private Sector

This strategy takes advantage of the organization in place under the NRP to communicate to the private sector when conducting recovery operations, using AMSCs as the primary means to communicate with the private sector and augmented at the national level by the NICC. Additionally, Section IV of the NMTSP describes how and when the Federal government will share intelligence with local, regional and national level partners following incidents of national significance.

Subject to security considerations, among the key information needed by the maritime industry and trade in the aftermath of an incident that affects one or more United States ports is:

- The location of the incident, specific to what port or facility is impacted.
- Identification of affected ports, including both the port(s) where the incident occurs and other ports that are anticipated to be impacted by diversions or increased security measures.

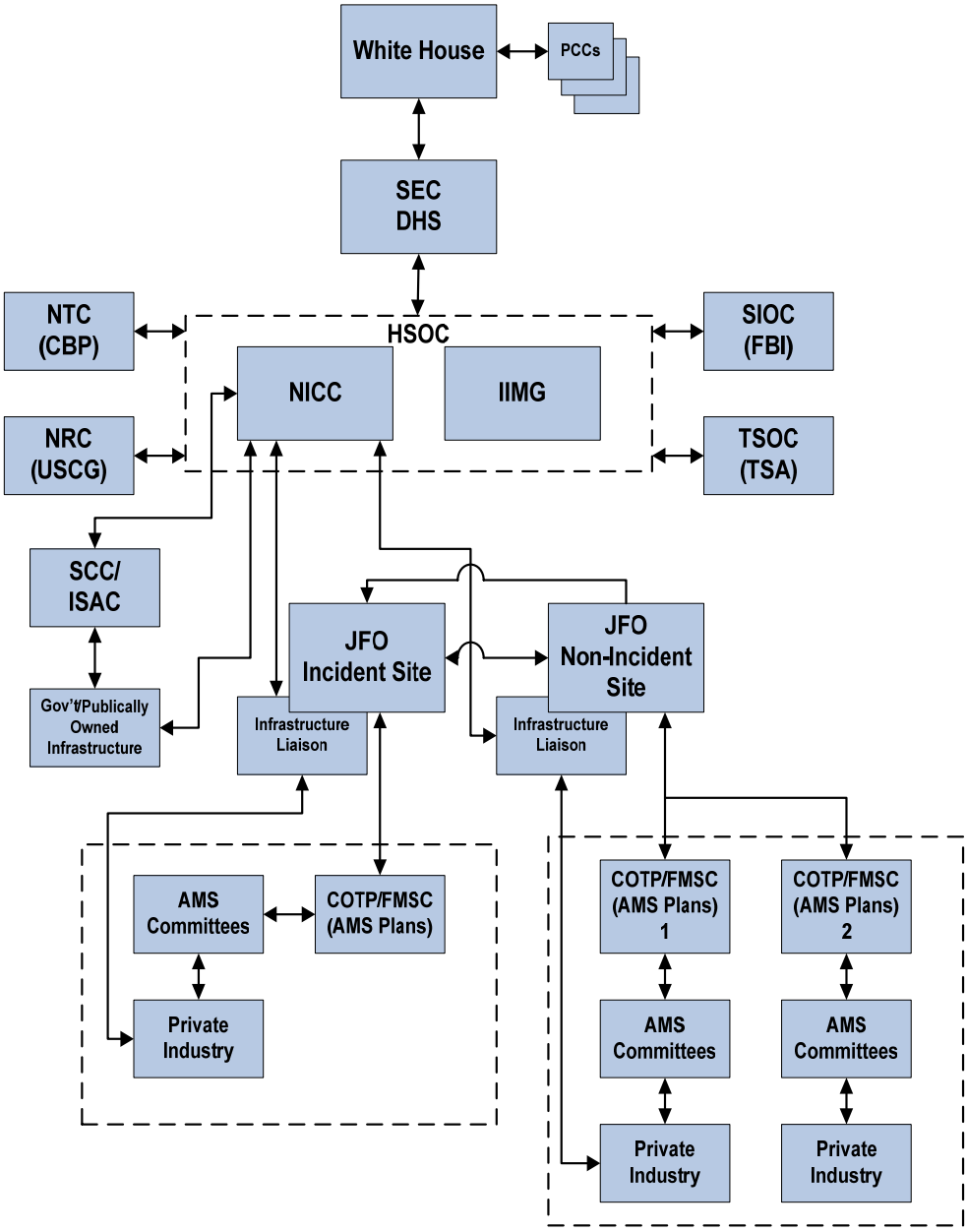


Figure 10: Department of Homeland Security Communication Flow Chart

- An assessment of the impact of the incident, including:
  - The extent of the damage to the port(s), terminal(s), critical waterways, road, and rail infrastructure.
  - The status of the impacted port(s) or terminal(s), e.g., if fully closed or partially operational.
  - The extent and anticipated duration of restrictions in the affected port(s) or terminal(s) and other U.S. ports (e.g., no movement in or out, 100 percent inspections being carried out, curfews, additional documentation requirements, etc.).

- Any impacts on support services, including surface transportation.
- Any restrictions on certain commodities, vessels, ports of lading, etc.
- Any collateral impacts on land borders, air cargo, etc.

- The expected duration of the incident and its impacts.
- Any possible alternate routing recommendations.
- The MARSEC Levels of all affected ports.
- The wait times at border crossing (which may impact cargo loading or the availability of transportation to support cargo off-loading).

The private sector is strongly encouraged to develop, as a means of advancing both normal operational efficiencies and response/recovery procedures, enhanced methods of communications between commercial stakeholders and governmental entities. Such communications systems could be developed either independently or via government-private sector partnerships along the lines of the Columbia-Snake Transportation Security Network (CSTSNet). It was developed via cooperative agreement between the Regional Maritime Security Coalition and the TSA.

Government - Government

The inter-connected nature of global trade makes communications between trading partners a priority in the management of post-incident trade resumption. Recognition of this has led to efforts by such trans-national organizations as the Asia-Pacific Economic Cooperation (APEC) to develop Trade Recovery Programs. The DHS has actively participated with our trading partners in such projects, consistently emphasizing that the establishment of transparency and trust relationships prior to an event are critical in the address of post-event conditions and that communications is an essential component of the process.

The primary channel for communications between the United States government and trade partner governments will be the Department of State. Such communications will be conducted in accordance with the NRP.

Key components of the government-to-government communications include:

- The characterization of the attack and identification of any immediate risks to ports, conveyances (e.g., aircraft, vessels, etc.), cargo/containers, and crewmembers.
- An initial damage and (potentially) contamination assessment, including:
  - The name of the affected ports/terminals.
  - The name of any affected private companies.
  - Damage to port infrastructure and equipment.
  - Damage to road/rail networks.
  - Damage to conveyances.
  - Damage to cargo/containers.

    - Contamination of impacted infrastructure, air, and water.
- Any waterway route changes, including where possible:
    - Sounding conducted.
    - Navigational obstructions.
    - Navigational aid changes.
    - The availability of assist vessels (e.g., tugs).
    - Any changes in harbor pilot requirements.
    - An estimate of the duration of waterway/port restrictions and/or closures.
- Any land route changes:
    - Route restrictions.
    - Route recommendations.
    - Estimated duration of route restrictions.
    - Port access restrictions.
- The current operating capacity of impacted ports.
- Current delays in impacted and non-impacted ports.
- An estimate of the capacity of non-impacted ports to accept rerouted trade.
- Any current needs (e.g., personnel, equipment, subject-matter expertise, etc.).
- An estimate of the duration before resumption of normal operations could be foreseen.
- The number and type of conveyances, cargo, or containers en route, both to and from the impacted and non-impacted ports.
- The number and type of shipments laden and at port.
- Any appropriate investigative findings, e.g. suspected individuals, suspected terrorist organization involvement, methods used to carry out an attack, the type of weapon and quantity of weapon used, etc.

X. TRAINING AND EXERCISE REQUIREMENTS

The combined efforts of the TSA and the USCG are providing a comprehensive approach to transportation security preparedness. Namely, PortSTEP sponsored by TSA, and the National Maritime Security Exercise Program (NMSEP) and Area Maritime Security Training and Exercise Program (AMSTEP) sponsored by the USCG. These jointly implemented programs contribute to meeting Congressional training and exercise mandates and bring together Federal, State and local governments and private institutions to test responses to specific transportation security events. The programs foster strong communication between public and private entities and enhance the ability of these groups to prevent, respond to, and recover from major TSIs.

TSA and the USCG have agreed to a delineation of responsibilities for the implementation of the PortSTEP and AMSTEP based on each agency's authorities. TSA is focused on the surface transportation security issues and USCG is focused on the water-side and maritime issues. The programs have many common processes, procedures, and design elements; however, the distinction lies in the different modal focus of the programs. That being said, all exercises are delivered through the USCG chaired AMSC within each port.

Through PortSTEP and AMSTEP, TSA and the USCG are assisting ports and the land transportation community to enhance transportation security preparedness by conducting exercises and providing tools that help identify planning gaps, assess plans, measure performance, collect and disseminate lessons learned and best practices, that can shape the policy that drives the Nation's transportation security preparedness initiatives. The cooperative working environment between TSA, the USCG, the Maritime Administration (MARAD), CBP, other Federal, State, and local government entities and the private sector through the AMSCs, is creating opportunities for all to take advantage of the lessons learned from previous efforts. The result of this approach is an increase in intermodal membership at each AMSC, and an increase in awareness, coordination and communication between the maritime and surface transportation sectors within the ports. The effective application of agency expertise avoids duplication of effort within the Federal government while preserving the distinct authorities of the agencies involved. Together the programs encompass the necessary scope to address the transportation security needs of the ports, whether the threat is from the water side or land side.

Through the use of the PortSTEP Business Information Center (BIC), a web-based information system intended to capture exercise information and to assist exercise planners in designing exercises, international supply chain issues can be incorporated into the program. As exercise data is captured within the system, exercise designers will be able to build upon lessons learned and best practices from the transportation security community. BIC is intended to be the single entry point into exercise information, tools, and reference materials and will satisfy certain SAFE Port Act requirements. It will also serve as the program's primary outreach mechanism to the surface transportation community.

TSA, in association with the USCG, is sponsoring delivery of 40 port security training exercises during a 36-month period from April 2005 through October 2007. It has also been effectively integrated with AMSTEP and other existing programs throughout the

government and private industry. In CY2006 PortSTEP and AMSTEP collectively sponsored 53 port security exercises. PortSTEP development will end in October 2007, culminating in a fully vetted and tested port and transportation security exercise pilot program that will serve as a model for security exercise programs for TSA and other government agencies. The USCG will continue to exercise the AMSPs and port security procedures and capabilities through the AMSTEP program and its All-Hazards/All-Threats planning and exercise approach. The TSA plans to apply the tools and services developed under PortSTEP to the other modes of surface transportation - rail, mass transit, pipelines, and highway. TSA is working to integrate initiatives such as passenger screening and other preparedness/response initiatives to present the community with a consistent program that addresses multiple aspects of the maritime threat environment.

PortSTEP, AMSTEP and the BIC provide a foundation for all types of training and exercise efforts and can be used as a platform to verify maritime activities including supply chain initiatives. TSA and the USCG have begun discussions on potential ways to expand the PortSTEP and AMSTEP models to all transportation modes and to form a regional approach to exercises, beyond just the port. Such regional exercises, involving industry participation, may also include appropriate participation by foreign trading partners.

Appendix A: LIST OF ACRONYMS

AC	Area Committee
AEO	Authorized Economic Operator
AMSC	Area Maritime Security Committee
AMSP	Area Maritime Security (AMS) Plan
AMSTEP	Area Maritime Security Training and Exercise Program
AOR	Area of Responsibility
APIS	Advance Passenger Information System
ATU	Advanced Targeting Units
BIC	Business Information Center
CBP	United States Customs and Border Protection
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosive
CBSA	Canadian Border Services Agency
CDC	Certain Dangerous Cargo
CEO	Chief Executive Officer
CERCLA	Comprehensive Environmental Response, Compensation, and Liability Act
CI	Critical Infrastructure
CI/KR	Critical Infrastructure/Key Resources
CIPAC	Critical Infrastructure Partnership Advisory Council
COA	Course of Action
COAC	Commercial Operations Advisory Committee
CONOPS	Concept of Operations
COOP	Continuity of Operations
COP	Common Operational Picture
COTP	Captain of the Port
CSD	Container Security Device
CSI	Container Security Initiative
C-TPAT	Customs-Trade Partnership Against Terrorism
CWA	Clean Water Act
DHS	Department of Homeland Security
DOC	Department of Commerce

DOD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DRG	Domestic Readiness Group
DSCA	Defense Support of Civil Authorities
ESF	Emergency Support Function
FACA	Federal Advisory Committee Act
FBI	Federal Bureau of Investigation
FCO	Federal Coordinating Officer
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
FMSC	Federal Maritime Security Coordinator
FOIA	Freedom of Information Act
FRA	Federal Railroad Administration
FSD	Federal Security Directors
FSP	Facility Security Plan
GAO	Government Accountability Office
GCC	Government Coordinating Councils
HAZMAT	Hazardous Materials
HMGP	Hazard Mitigation Grant Program
HSAC	Homeland Security Advisory Council
HSAS	Homeland Security Advisory System
HSC	Homeland Security Council
HSOC	Homeland Security Operations Center
HSPD	Homeland Security Presidential Directive
I&A	Office of Intelligence and Analysis
IAC	Interagency Advisory Council
IBET	Integrated Border Enforcement Teams
IC	Incident Commander
ICE	Immigration and Customs Enforcement

ICP	Incident Command Post
ICS	Incident Command System
ICSM	Integrated Supply Chain Management
IIMG	Interagency Incident Management Group
IMH	Incident Management Handbook
IMO	International Maritime Organization
IMSO	International Mobile Satellite Organization
INS	Incident of National Significance
IPSLO	International Port Security Liaison Officer
IPSP	International Port Security Program
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
ISPS	International Ship and Port Facility Security (Code)
JFO	Joint Field Office
KA	Key Asset
KR	Key Resource
LRIT	Long Range Identification and Tracking of Vessels
MARAD	Maritime Administration
MARSEC	Maritime Security Level
MDA	Maritime Domain Awareness
MIRP	Maritime Infrastructure Recovery Plan
MSPCC	Maritime Security Policy Coordinating Committee
MSRAM	Maritime Security Risk Analysis Model
MTS	Maritime Transportation System
MTSA	Maritime Transportation Security Act of 2002
MTSRU	Marine Transportation System Recovery Unit
NAIS	Nationwide Automatic Identification System
NFPA	National Fire Protection Association
NICC	National Infrastructure Coordination Center
NII	Non-Intrusive Inspection
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology

NMIC	National Maritime Intelligence Center
NMSAC	National Maritime Security Advisory Committee
NMTSP	National Maritime Transportation Security Plan
NNSA	National Nuclear Security Administration (DOE)
NOA	Notice of Arrival
NOAA	National Oceanic and Atmospheric Administration
NOC	National Operations Center
NRC	National Response Center
NROM	National Response Options Matrix
NRP	National Response Plan
NSC	National Security Council
NSMS	National Strategy for Maritime Security
NSPD	National Security Presidential Directive
NSTS	National Strategy for Transportation Security
NTC	National Targeting Center
NTSI	National Transportation Security Incident
OBP	Office of Border Patrol
OPS	Office of Pipeline Safety
PAS	Publicly Available Specification
PCC	Policy Coordinating Committee
PCII	Protected Critical Infrastructure Information
PFO	Principal Federal Official
PHMSA	Pipeline and Hazardous Materials Safety Administration
POE	Port of Entry
PortSTEP	Port Security Training Exercise Program
PRD	Personal Radiation Detector
PWSA	Ports and Waterways Safety Act
R&D	Research and Development
RCMP	Royal Canadian Mounted Police
RIID	Radiation Isotope Identification Device
RORO	Roll-on, Roll-off
RPM	Radiation Portal Monitor
RRCC	Regional Response Coordination Center

SAFE Port Act	Security and Accountability for Every Port (SAFE Port) Act of 2006
SARA	Superfund Amendments and Reauthorization Act
SBA	Small Business Administration
SCC	Sector Coordinating Council
SCO	Screening Coordination Office
SIOC	Strategic Information Operations Center
SLSDC	St. Lawrence Seaway Development Corporation
SOLAS	Safety of Life at Sea Convention
SSA	Sector-Specific Agency
TECS	Treasury Enforcement Communication System
TIH	Toxic Inhalation Hazard
TS	Technical Specification
TSA	Transportation Security Administration
TSI	Transportation Security Incident
TSOC	Transportation Security Operations Center
TSSP	Transportation Sector Specific Plan
TWIC	Transportation Worker Identification Credential
UC	Unified Command
UCS	Unified Command Structure
UNCLOS	United Nations Convention on the Law of the Sea
USACE	U.S. Army Corps of Engineers
USCG	United States Coast Guard
VSP	Vessel Security Plan
VTS	Vessel Traffic Services
WCO	World Customs Organization
WMD	Weapons of Mass Destruction

Appendix B: TERMS

Agencies: United States Executive branch departments, agencies, and establishments.

Area Maritime Security Committee: An Area Maritime Security Committee is established under the direction of the USCG Captain of the Port serving as Federal Maritime Security Coordinator and assist[s] in the development, review, and update of the AMSP for the COTPs area of responsibility. The AMSC's principal duty is to help the COTP to assess security risks to the port and determine appropriate risk mitigation strategies. AMSC members may include: United States Coast Guard, Federal, State, and local law enforcement, emergency response, port managers, labor representatives, etc. There must be at least seven members of the Committee. At least seven of the total number of members must each have five years or more experience related to maritime or port security operations.

Authorized Economic Operator: A party involved in the international movement of goods in whatever function has been approved by or on behalf of a national Customs administration as complying with WCO or equivalent supply chain security standards. Authorized Economic Operators include, inter alia, manufacturers, importers, exporters, brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses, and distributors.

Captain of the Port: The officer of the United States Coast Guard, under the command of a District Commander, designated by the Commandant for the purpose of giving immediate direction to all Coast Guard activities within an assigned Area of Responsibility. As designated by the National Maritime Transportation Security Plan under the Maritime Transportation Security Act of 2006 as implemented through 33 C.F.R. Part 103.200, the COTP is also the designated Federal Maritime Security Coordinator for his or her AOR. The COTP may, inter alia, prevent any person, article, or thing from boarding or being taken or placed on board any vessel, or entering or being taken into or upon or placed in or upon any waterfront facility whenever it appears to him or her that such action is necessary in order to secure such vessel from damage or injury or to prevent damage or injury to any vessel, or waterfront facility or waters of the United States, or to secure the observances of rights and obligations of the United States.

Cargo: Any goods, wares, or merchandise carried, or to be carried, for consideration, whether directly or indirectly flowing to the owner, charterer, operator, agent, or any other person interested in the vessel, facility, or Outer Continental Shelf facility, except dredge spoils.

Concept of Operations (CONOPS): A broad outline of assumptions or intent in regard to an operation or series of operations, designed to give an overall picture of the operation for clarity of purpose.

Container: The term ‘container’ has the meaning given the term in the International Convention for Safe Containers, with annexes, done at Geneva on December 2, 1972 (29 UST 3707).

Container Security Device: A device, or system, designed, at a minimum, to identify positively a container, to detect and record the unauthorized intrusion into a container, and to secure a container against tampering throughout the supply chain.

Critical Infrastructure: As defined in the U.S. PATRIOT Act so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. There are 13 "Critical Infrastructure Sectors" in the National Infrastructure Protection Plan under HSPD 7.

Disruption: See 'Transportation Disruption.'

Domestic Readiness Group (DRG): The White House convenes the Domestic Readiness Group on a regular basis to develop and coordinate implementation of preparedness and response policy and in anticipation of or during crises such as natural disasters and domestic terrorist attacks to address issues that cannot be resolved at lower levels and provide strategic policy direction for the Federal response. The DRG can also be convened at any time at the request of one of its members.

Examination: An inspection of cargo to detect the presence of misdeclared, restricted, or prohibited items that utilized nonintrusive imaging and detection technology.

Federal Maritime Security Coordinator: The USCG Captains of the Port have been designated by the National Maritime Transportation Security Plan and 33 C.F.R. Part 103.200 as the FMSCs for their respective COTP zones defined in 33 C.F.R. Part 3. They coordinate local security emergency response planning efforts with Federal, State, local, and private-sector organizations.

Framework of Standards ("Framework"): Voluntary World Customs Organization strategy to secure the movement of global trade in a way that does not impede but rather facilitates the movement of that trade.

Homeland Security Presidential Directives: Presidential decisions about the homeland security policies of the United States, issued by the Homeland Security Council. See "Maritime Infrastructure Recovery Plan" below.

Initial recovery: Differing from response, initial recovery is that period where impacted infrastructure and supporting activities within the incident area have been returned to service and are capable of operations or service at some level. Initial activities, policies or mitigation strategies aimed at initial recovery are considered to be achievable in 90 days or less.

Inspection: The comprehensive process used by the United States Customs and Border Protection to assess goods entering the United States to appraise them for duty purposes, to detect the presence of restricted or prohibited items, and to ensure compliance with all applicable laws. The process may include scanning, conducting an examination, or conducting a search. In the case of a vessel, an inspection is conducted by a boarding team and includes document reviews, cargo validation, equipment checks, and crew checks.

Interagency Planning Element: See National Operations Center - Interagency Planning Element.

Interagency Watch: See National Operations Center – Interagency Watch.

International Supply Chain: The end-to-end process for shipping goods to or from the United States beginning at the point of origin (including manufacturer, supplier, or vendor) through to a point of distribution to the destination.

Joint Field Office: The JFO is a temporary Federal facility established locally to provide a central point for Federal, State, local, and tribal executives with responsibility for incident oversight, direction, and/or assistance to effectively coordinate protection, prevention, preparedness, response, and recovery actions.

Key Asset: Individual targets whose destruction would not endanger vital systems, but could create local disaster or profoundly damage our Nation's morale or confidence. Key assets include symbols or historical attractions, such as prominent national, State, or local monuments and icons. In some cases, these include quasi-public symbols that are identified strongly with the United States as a Nation. Key assets also include individual or localized facilities that deserve special protection because of their destructive potential or their value to the local community.

Key Resources: Publicly or privately controlled resources essential to the minimal operations of the economy and government. There are four "Key Resource Sectors" in the National Infrastructure Protection Plan under HSPD 7.

Long-term Recovery: Long-term recovery is defined as that period in which infrastructure and supporting activities have been returned to pre-incident conditions or service or have the capacity or capability to operate or provide service at pre-incident levels. Activities, policies or mitigation strategies aimed at long-term recovery may take longer than 90 days. Long-term recovery as used in this strategy parallels long-term recovery measures associated with NRP ESF #14.

Maritime Domain: All areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances.

Maritime Domain Awareness: The effective knowledge of all activities associated with the global maritime environment that could impact the security, safety, economy, or environment of the United States.

Maritime Infrastructure Recovery Plan: The MIRP is one of eight plans supporting the National Strategy for Maritime Security. The MIRP's primary goal is to protect the United States economy from the effects of a maritime TSI. The MIRP provides guidance to individuals designated by the Secretary of DHS to help make decisions on maintaining or restoring transportation capabilities, in the event of a TSI.

Maritime Security (MARSEC) Level: The level set to reflect the prevailing threat environment to the marine elements of the national transportation system, including ports, vessels, facilities, and critical assets and infrastructure located on or adjacent to the waters subject to the jurisdiction of the United States. There are three MARSEC Levels:

- MARSEC I: Maritime security level for which minimum appropriate protective security measures shall be maintained at all times.

- MARSEC II: Maritime security level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a Transportation Security Incident.
- MARSEC III: Maritime security level for which further specific protective security measures shall be maintained for a limited period of time when a Transportation Security Incident is probable or imminent, although it may not be possible to identify the specific target.

Maritime Threats: Actionable knowledge of or acts of terrorism, piracy, and other criminal or other unlawful or hostile acts committed by terrorists, criminals, foreign States, and non-state actors, including such acts of proliferation concern.

Maritime Transportation Security Act of 2002: Signed on November 25, 2002, the MTSA enacted laws designed to protect the nation's vessels, ports, and waterways against a transportation security incident. It implemented the U.S. obligations under the International Ship and Port Facility Security Code, and was substantively implemented on July 1, 2004.

Maritime Transportation System: The system of waterways, ports and intermodal landside connections which allow the various modes of transportation to move people and goods to, from, and on the water.

National Infrastructure Coordinating Center: See National Operations Center - National Infrastructure Coordinating Center.

National Infrastructure Protection Plan: A family of 17 risk-based infrastructure protection plans for Homeland Security developed under HSPD 7, including 13 protection plans for "Critical Infrastructure Sectors" (including the Transportation Sector Security Plan), and 4 plans for protecting "Key Resources."

National Maritime Transportation Security Plan: A risk-based protection plan focused on protecting the public and managing security risks posed to maritime assets and infrastructure "on or adjacent to the waters subject to the jurisdiction of the United States." The NMTSP is required to "provide for efficient, coordinated, and effective action to deter and minimize damage from a transportation security incident." A TSI that has national impacts may be declared an Incident of National Significance by the Secretary of Homeland Security.

National Operations Center: Linking key headquarters components, including the former Homeland Security Operations Center, the NOC is comprised of five sub-elements: the Interagency Watch, the National Response Coordination Center, the Information and Analysis Component, the National Infrastructure Coordinating Center, and the Operational Planning Element.

National Operations Center – Intelligence and Analysis: I&A is responsible for interagency intelligence collection requirements, analysis, production, and product dissemination for the Department of Homeland Security. I&A coordinates or disseminates homeland security threat warnings, advisory bulletins, and other information pertinent to national incident management to Federal, State, regional, local,

and nongovernmental Emergency Operations Centers and incident management officials and relevant elements of the private sector.

National Operations Center – National Infrastructure Coordinating Center: The NOC-NICC monitors the Nation's critical infrastructure and key resources on an ongoing basis. During an incident, the NOC-NICC provides a coordinating forum to share information across infrastructure and key resources sectors through appropriate information-sharing entities such as the Information Sharing & Analysis Centers and the Sector Coordinating Councils. To foster information sharing and coordination, private sector representatives from the CI/KR may provide information to the NOC-NICC.

National Operations Center – Interagency Planning Element: NOC-Planning conducts strategic level operational incident management planning and coordination. NOC-Planning is responsible for strategic level operational planning, including coordinating response, recovery, and mitigation operational planning and interagency coordination with the NOC-NRCC; coordinating and sustaining Federal preparedness, prevention, and protection activities related to an Incident of National Significance or at the Secretary's direction; and coordinating preparedness, prevention, and protection operations and resource allocation planning with the appropriate Federal departments and agencies, the NOC-NRCC, the RRCCs, and the JFO.

National Operations Center - Interagency Watch: A standing 24/7 interagency organization fusing law enforcement, national intelligence, emergency response, and private sector reporting. The NOC-Watch facilitates homeland security information-sharing and operational coordination with other Federal, State, local, tribal, and nongovernmental Emergency Operations Centers.

National Operations Center - National Response Coordination Center: The NOC-NRCC monitors potential or developing incidents and supports the efforts of regional and field components, including coordinating the preparedness of national-level emergency response teams and resources; in coordination with Regional Response Coordination Centers, initiating mission assignments or reimbursable agreements to activate other Federal departments and agencies; and activating and deploying national-level specialized teams. In addition, the NOC-NRCC resolves Federal resource support conflicts and other implementation issues forwarded by the JFO. Those issues that cannot be resolved by the NOC-NRCC are referred to the Incident Advisory Council. During an incident, the NOC-NRCC operates on a 24/7 basis or as required in coordination with other elements of the NOC.

National Response Center: The NRC serves as the sole national point of contact for reporting all oil, chemical, radiological, biological and medical waste discharges into the environment within the United States and its territories. The NRC maintains agreements with a variety of Federal entities to make additional notifications regarding incidents that meet established triggering criteria. Under Coast Guard regulations the regulated maritime community is required to notify the NRC without delay of any breaches of security, suspicious activity or transportation security incidents.

National Response Coordination Center: See National Operations Center – National Response Coordination Center.

National Response Options Matrix: An automated response management tool used by the USCG and U.S. Customs and Border Protection to help manage the first 48 hours of a security incident. It provides senior leadership with pre-planned, short term security options to prevent further attacks and protect the Marine Transportation System, Maritime Critical Infrastructure and Key Assets, and high density population centers, following a maritime Transportation Security Incident.

National Response Plan: Last updated May 25, 2006, establishes a comprehensive all-hazards approach to enhance the ability of the United States to manage domestic incidents. The plan incorporates best practices and procedures from incident management disciplines—homeland security, emergency management, law enforcement, firefighting, public works, public health, responder and recovery worker health and safety, emergency medical services, and the private sector—and integrates them into a unified structure.

National Security Presidential Directives: Presidential decisions about the national security policies of the United States, replacing both the Presidential Decision Directives and the Presidential Review Directives, issued by the National Security Council. (Unless otherwise indicated, however, past Directives remain in effect until they are superseded; e.g., HSPD-7, Critical Infrastructure Identification, Prioritization & Protection supersedes PDD-63, Protecting America's Critical Infrastructures).

National Strategy for Transportation Security: This plan outlines the Federal government's approach, in partnership with State, local and tribal governments and private industry, to securing the United States transportation system from terrorist threats and attacks, and prepares the Nation by increasing our capacity to respond. It also fulfills requirements of the Intelligence Reform and Terrorism Prevention Act of 2004.

National Targeting Center: U.S. Customs and Border Protection's NTC provides tactical targeting and analytical research supporting CBP and DHS anti-terrorism efforts. Supporting continuous operations, NTC is primarily staffed by CBP personnel who are experts in passenger and cargo targeting for air, sea and land operations in the inbound and outbound environments. The NTC staff develops tactical targets from raw intelligence in support of the CBP mission to detect and prevent terrorists and terrorist weapons from entering the United States. NTC supports all CBP field elements with additional research assets for passenger and cargo examinations. The center also works closely with the CBP Office of Intelligence and Immigration and Customs Enforcement agents to share information and to formulate their advisories. Working with CBP partners, the NTC has developed liaison programs within DHS and beyond. The NTC mission continues to evolve as a cornerstone in the war on terrorism. Centralized NTC targeting endeavors, combined with intra and interagency collaboration, assure CBP of a coordinated response to terrorist and national security events.

National Transportation Security Incident: A transportation security incident impacting more than one port or area that exceeds the capacity of a single Coast Guard Captain of the Port and other agencies within the area. Under the Maritime Transportation Security Act, the National Maritime Transportation Security Plan is required to reduce the risk of a "national transportation security incident."

Navigational Throughput: Navigational throughput is similar in some ways to "Service Flow" in highways: the maximum efficient (and safe) volume of traffic for a functional classification. For maritime, this might be a function of: Vessel size and design, degree of overtaking or meeting traffic (all sizes and those constrained by draft), volume of cross channel traffic (all sizes), weather, ice, tide and current, channel dimensions and design, short range aids to navigation, radio aids to navigation, radar, ECDIS, AIS, VTS, and pilotage. On the inland river system, a critical factor of navigational throughput is the ability of navigation locks to process individual tows consisting of a single towboat and a variable number of loaded and empty barges.

Positive Identification System: A system providing for a determination, based on reliable identification techniques, that the subject of a record search is in fact the subject intended to be entered into the record system. Identifications based solely upon a comparison of not unique identification characteristics or numbers shall not constitute positive identification.

Prevention: Actions taken to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions taken to protect lives and property as well as to secure cargo and trade.

Principal Federal Official: The PFO is the Federal official designated by the Secretary of Homeland Security to act as his/her representative locally to oversee, coordinate, and execute the Secretary's incident management responsibilities under HSPD-5. In certain scenarios, a PFO may be pre-designated by the Secretary of Homeland Security to facilitate Federal domestic incident planning and coordination at the local level outside the context of a specific threat or incident. A PFO also may be designated in a pre-incident mode for a specific geographic area based on threat and other considerations. PFOs typically are not "dual hatted" with any other roles or responsibilities that could detract from their overall incident coordination responsibilities. The Secretary may, in other than terrorism incidents, choose to combine the roles of the PFO and Federal Coordinating Officer (FCO) in a single individual to help ensure synchronized Federal coordination. In the event of an incident with no clear geographic boundaries (e.g., a cyber incident), a national-level PFO may be designated to coordinate Federal response activities.

Protocol: An action plan that describes how an activity should be performed.

Radiation Detection Equipment: Any technology that is capable of detecting or identifying nuclear and radiological material or nuclear and radiological explosive devices.

Recovery: Recovery consists of measures, programs, and other activities that are planned and applied across Critical Infrastructure and Key Resources Sectors consistent with the NRP CI/KR Support Annex to facilitate and support the resumption of trade within incident areas (those areas directly impacted by the effects of the incident) and non-incident areas (those areas indirectly affected by the consequences of the incident). Recovery also consists of measures and actions needed to resume trade at normal levels following the threat of an incident which necessitates heightened security and possible transportation restrictions affecting cargo flow.

Recovery measures are characterized as those that are needed to provide initial recovery and to provide the basis to facilitate and support long-term recovery and mitigation activities where required.

Recovery Unit: An organization element under the Planning Section of an Incident Command System responsible for planning infrastructure recovery and resumption of trade for transportation disruptions. A Recovery Unit may be tasked with tracking and reporting on the status of the overall transportation system, understanding critical recovery pathways, recommending courses of action, and providing all stakeholders with an avenue of input to the local response organization. A critical function of the Recovery Unit is the development and updating of prioritized recommendations for the Incident Commander/Unified Command on vessel and cargo movements and coordinating these plans with the Operations Section.

Regional Response Coordination Center: The RRCC is a standing facility operated by the Department of Homeland Security/Federal Emergency Management Agency that coordinates regional response efforts, establishes Federal priorities, and implements local Federal program support until a JFO is established in the field and/or other key DHS incident management officials can assume their NRP coordination responsibilities. The RRCC establishes communications with the affected State Emergency Operations Center and the NOC-NRCC, coordinates deployment of the Emergency Response Team–Advance Element to field locations, assesses damage information, develops situation reports, and issues initial mission assignments.

Response: Activities that address the short-term, direct effects of an incident. Such activities could include the execution of emergency operations plans, first responder operations, incident mitigation activities, and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity.

Restoration: The extent to which infrastructure has individually or collectively recovered or the extent to which trade has recovered is characterized as the level of restoration, expressed as a percentage or other suitable metric of pre-incident conditions or service, or as the capacity to operate or provide service at pre-incident levels, as appropriate. This characterization recognizes that an incident or incidents can potentially have profound effects on trade patterns and business interests and that a return to pre-incident condition or service does not necessarily mean that there will be a corresponding return to pre-incident trade patterns and conditions, although facilitation of the latter is a goal of this strategy.

Scan: Utilizing nonintrusive imaging equipment, radiation detection equipment, or both, to capture data, including images of a container.

Screening: A visual or automated review of information about goods, including manifest or entry documentation accompanying a shipment being imported into the United States, to determine the presence of misdeclared, restricted, or prohibited items and assess the threat level posed by such cargo. Screening of vessels entering the United States is conducted by the United States Coast Guard. In this context, vessel screening is a broad term meaning the review of information regarding a vessel's regulatory status, security history, history of prior ports, etc., to determine if inspections are required prior to entry, or security or operational control measures are necessary during port transit/entry.

Search: An intrusive examination in which a container is opened and its contents are devanned and visually inspected for the presence of misdeclared, restricted, or prohibited items.

Sector-Specific Agency: The term "Sector-Specific Agency" means a Federal department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category. Sector-Specific Agencies will conduct their activities in accordance with guidance provided by the Secretary of the Department of Homeland Security.

Security Zone: A security zone is a limited access area on the water or adjacent land area established by the USCG Captain of the Port subject to the terms and conditions specified in 33 C. F. R. §6.01–5. No person or vessel shall enter a security zone without the permission of the COTP. No person shall board or take or place any article or thing on board any vessel or waterfront facility in a security zone without the permission of the COTP.

Stafford Act: A Congressional Act to provide an orderly and continuing means of assistance by the Federal government to State and local governments in carrying out their responsibilities to alleviate the suffering and damage which result from disasters by revising and broadening the scope of existing disaster relief programs; encouraging the development of comprehensive disaster preparedness and assistance plans, programs, capabilities, and organizations by the States and by local governments; achieving greater coordination and responsiveness of disaster preparedness and relief programs; encouraging individuals, States, and local governments to protect themselves by obtaining insurance coverage to supplement or replace governmental assistance; encouraging hazard mitigation measures to reduce losses from disasters, including development of land use and construction regulations; and providing Federal assistance programs for both public and private losses sustained in disasters.

Strategic Information Operations Center: The United States Federal Bureau of Investigation SIOC is the focal point and operational control center for all Federal intelligence, law enforcement, and investigative law enforcement activities related to domestic terrorist incidents or credible threats, including leading attribution investigations. The SIOC serves as an information clearinghouse to help collect, process, vet, and disseminate information relevant to law enforcement and criminal investigation efforts in a timely manner. The SIOC maintains direct connectivity with the NOC and IAC.

Strategy: A document used by an organization to align its organization and budget structure with organizational priorities, missions, and objectives. According to requirements of GPRA, a strategy should include a mission statement, a description of the agency's long-term goals and objectives, and strategies or means the agency plans to use to achieve these general goals and objectives. The strategy may also identify external factors that could affect achievement of long-term goals.

Supply Chain Node: One of 13 standard security control points that provide the foundation to assess and model intermodal container threat scenarios, vulnerabilities, and various security counter measure and protection mechanisms. The 13 standard nodes are:

1. Supplier
2. Factory/Packaging
3. Empty container storage/dray
4. Drayage of cargo to consolidator (if stuffing is not at factory)
5. Container stuffing/sealing (consolidation)
6. Container storage (foreign)
7. Drayage to terminal (from factory or consolidator)
8. Foreign terminal
9. Ocean commerce
10. United States terminal
11. Inland drayage or rail transfer/transport (United States)
12. Deconsolidation (United States)
13. Business processes/information transmission, in particular, the process for booking and transferring containers

Transportation Disruption: Any significant delay, interruption, or stoppage in the flow of trade caused by a natural disaster, heightened threat level, and act or terrorism, or any transportation security incident (as defined in section 70101(6) of Title 46, United States Code).

Transportation Security Incident: The term 'transportation security incident' has the meaning given the term in Section 70101(6) of Title 46, United States Code:

> *A security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area. An 'economic disruption' does not include a work stoppage or other employee-related action not related to terrorism and resulting from employee-employer dispute.*

Transportation Sector Specific Plan: This plan describes a collaborative effort between the private sector, State, local and tribal governments, nongovernmental organizations, and the Federal government. This collaboration will result in the prioritization of protection initiatives and investments within and across sectors. It fulfills the requirements of Homeland Security Presidential Directive - 7.

Weapons of Mass Destruction: Any adversary capabilities that pose potentially devastating impacts, including chemical, biological, radiological, and nuclear weapons and high-yield explosives.

Appendix C: ADDITIONAL AUTHORITIES

In addition to the primary authorities contained in Section VII, there are multiple secondary authorities providing for Federal government regulation and control over the supply chain. Below are a few additional key examples.

CORPORATE AND CRIMINAL FRAUD ACCOUNTABILITY ACT OF 2002 (ALSO KNOWN AS THE SARBANES-OXLEY ACT)[24]

The Act applies to entities required to file periodic reports with the Securities and Exchange Commission under the provisions of the Securities and Exchange Act of 1934, as amended. It contains significant changes to the responsibilities of directors and officers, as well as the reporting and corporate governance obligations of affected companies. Among other things, it requires certification by the company's CEO and chief financial officer that accompanies each periodic report filed that the report fully complies with the requirements of the securities laws and that the information in the report fairly presents, in all material respects, the financial condition and results of the operations of the company. It also requires certifications regarding internal controls and material misstatements or omissions, and the disclosure on a "rapid and current basis" of information regarding material changes in the financial condition or operations of a public company. The Act contains a number of additional provisions dealing with insider accountability and disclosure obligations, and auditor independence. It also provides severe criminal and civil penalties for violations of the Act's provisions.

THE DEFENSE PRODUCTION ACT OF 1950 AND THE DEFENSE PRODUCTION REAUTHORIZATION ACT OF 2003

The Act provides the primary authority to ensure the timely availability of resources for national defense and civil emergency preparedness and response. Among other powers, the President is authorized to demand that companies accept and give priority to government contracts that the President "deems necessary or appropriate to promote the national defense," and allocate materials, services, and facilities, as necessary, to promote the national defense in a major national emergency. It also authorizes loan guarantees, direct loans, direct purchases, and purchase guarantees for those goods necessary for national defense. It also allows the President to void international mergers that would adversely affect national security. This Act defines "national defense" to include critical infrastructure protection and restoration, as well as activities authorized by the emergency preparedness sections of the Stafford Act. Consequently, the authorities stemming from the Defense Production Act are available for activities and measures undertaken in preparation for, during, or following a natural disaster or accidental or malicious event. Under the act and related Presidential orders, the Secretary of Homeland Security has the authority to place and, upon application, authorize State and local governments to place priority-rated contacts in support of Federal, State, and local emergency preparedness activities.

[24] Public Law 107-204, 116 Stat. 745 (July 30, 2002).

THE FREEDOM OF INFORMATION ACT[25]

This Act generally provides that any person has a right, enforceable in court, to obtain access to Federal agency records, except to the extent that such records are protected from public disclosure by nine listed exemptions or under three law enforcement exclusions. Persons who make requests are not required to identify themselves or explain the purpose of the request. The underlying principle of FOIA is that the workings of government are for and by the people and that the benefits of government information should be made broadly available. All Federal government agencies must adhere to the provisions of FOIA with certain exceptions for work in progress, enforcement confidential information, classified documents, and national security information. FOIA was amended by the Electronic Freedom of Information Act Amendment of 1996.

INFORMATION TECHNOLOGY MANAGEMENT REFORM ACT OF 1996[26]

Under section 5131 of the Information Technology Management Reform Act of 1996, the National Institute of Standards and Technology (NIST) develops standards, guidelines, and associated methods and techniques for Federal computer systems. Federal Information Processing Standards are developed by NIST only when there are no existing voluntary standards to address the Federal requirements for the interoperability of different systems, the portability of data and software, and computer security.

GRAMM-LEACH-BLILEY ACT OF 1999[27]

Among other things, this Act (title V) provides limited privacy protections on the disclosure by a financial institution of non-public personal information. The Act also codifies protections against the practice of obtaining personal information through false pretenses.

PUBLIC HEALTH SECURITY AND BIOTERRORISM PREPAREDNESS AND RESPONSE ACT OF 2003[28]

This Act improves the ability of the United States to prevent, prepare for, and respond to bioterrorism and other public health emergencies. Key provisions of the act, 42 U.S.C. 247(d) and 300(h) among others, address (1) development of a national preparedness plan by HHS that is designed to provide effective assistance to State and local governments in the event of bioterrorism or other public health emergencies; (2) operation of the National Disaster Medical System to mobilize and address public health emergencies; (3) grant programs for the education and training of public health professionals and the improvement of State, local, and hospital preparedness for and response to bioterrorism and other public health emergencies; (4) streamlining and clarification of communicable disease quarantine provisions; (5) enhancement of controls on dangerous biological agents and toxins; and (6) protection of the safety and security of food and drug supplies.

[25] Codified as 5 U.S.C. 552.
[26] Public Law 104-106, 110 Stat. 679 (February 10, 1996).
[27] Public Law 106-102 (1999), codified at 15 U.S.C. 94.
[28] Public Law 107-188, 116 Stat. 594 (June 12, 2002).

THE PRIVACY ACT OF 1974[29]

This Act provides strict limits on the maintenance and disclosure by any Federal agency of information on individuals that is maintained, including "education, financial transactions, medical history, and criminal or employment history and that contains [the] name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." Although there are specific categories for permissible maintenance of records and limited exceptions to the prohibition on disclosure for legitimate law enforcement and other specified purposes, the Act requires strict recordkeeping on any disclosure. It also specifically provides for access by individuals to their own records and for requesting correction thereto.

FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002[30]

This Act requires that Federal agencies develop a comprehensive information technology security program to ensure the effectiveness of information security controls over information resources that support Federal operations and assets.

CYBER SECURITY RESEARCH AND DEVELOPMENT ACT OF 2002[31]

This Act allocated funding to the National Institute of Standards and Technology and the National Science Foundation for the purpose of facilitating increased R&D for computer network security and supporting research fellowships and training.

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004[32]

This Act provides sweeping changes to the United States Intelligence Community structure and processes, and creates new systems specially designed to combat terrorism. Among other things, the Act:

- Establishes a Director of National Intelligence with specific budget, oversight, and programmatic authority over the Intelligence Community.
- Establishes the National Intelligence Council, redefines "national intelligence."
- Requires the establishment of a secure Information-Sharing Environment and an information-sharing council.
- Establishes the National Counterterrorism Center, a National Counter Proliferation Center, National Intelligence Centers, and a Joint Intelligence Community Council.
- Establishes, within the Executive Office of the President, a Privacy and Civil Liberties Oversight Board.
- Directs enhancements to maritime security.
- Directs enhancements to border security and immigration matters.

[29] Codified at 5 U.S.C. 552a.
[30] Public Law 107-296, Title X, 116 Stat. 2259, (November 25, 2002,)
[31] Public Law 107-305, 116 Stat. 2367, (November 27, 2002).
[32] Public Law 108-458, 118 Stat. 3638 (December 17, 2004).

- Requires the Director of the FBI to continue efforts to improve the intelligence capabilities of the FBI and to develop and maintain a national intelligence workforce.
- Requires DHS to develop and implement a National Strategy for Transportation Security and transportation modal security plans; enhance identification and credentialing of transportation workers and law enforcement officers; conduct R&D into mass identification technology, including biometrics; enhance passenger screening and terrorist watch lists; improve measures for detecting weapons and explosives; improve security related to the air transportation of cargo; and implement other aviation security measures.
- Enhances law enforcement authority and capabilities, and expands certain diplomatic, foreign aid, and military authorities and capabilities for combating terrorism.
- Requires expanded machine-readable visas with biometric data; implementation of a biometric entry and exit system, and a registered traveler program; and implementation of biometric or other secure passports.
- Requires standards for birth certificates and driver's licenses or personal identification cards issued by States for use by Federal agencies for identification purposes, and enhanced regulations for social security cards.
- Requires DHS to improve preparedness nationally, especially measures to enhance interoperable communications, and to report on vulnerability and risk assessments of the Nation's Critical Infrastructure/Key Resources.
- Directs measures to improve assistance to and coordination with State, local, and private sector entities.

THE CLEAN WATER ACT (CWA)[33] AS AMENDED BY THE OIL POLLUTION ACT OF 1990 (OPA)[34]

OPA streamlined and strengthened the United States government's ability to prevent and respond to catastrophic oil spills and established a trust fund financed by a tax on oil to clean up spills when the responsible party is incapable or unwilling.

COMPREHENSIVE ENVIRONMENTAL RESPONSE, COMPENSATION, AND LIABILITY ACT (CERCLA OR SUPERFUND)[35] AS AMENDED BY THE SUPERFUND AMENDMENTS AND REAUTHORIZATION ACT (SARA)[36]:

Superfund created a tax on the chemical and petroleum industries and provided broad federal authority to respond directly to releases or threatened releases of hazardous substances that may endanger public health or the environment.

[33] P.L. 95-217, 91 Stat. 1566 (December 27, 1977).
[34] 33 U.S.C. 2702 to 2761.
[35] 42 U.S.C. s/s 9601 et seq. (1980).
[36] 42 U.S.C.9601 et seq. (1986).