

U.S. PORT SECURITY

I. Introduction

The terrorist attacks of September 11, 2001, have focused world attention on the transportation industry and the opportunity to use parts of that system as weapons of mass destruction. As a result, the maritime industry is now faced with the realization that waterborne commerce to and from the United States will come under increased scrutiny.

This paper will outline the main affects that September 11 has had, and will have, on the maritime industry worldwide, and will outline the new legislation, regulations and initiatives that have, or are in the process of being, implemented in relation to port security.

II. New Departments, Legislation and Initiatives

The September 11 attacks have sparked a major debate on the security of ships, cargoes and crews, and especially on ports. The United States government has acted rapidly in implementing new regulations and initiatives with regard to security, which, for much of the maritime industry will, unfortunately, mean added cost and time. For shipowners, as we have already seen in past months, it will mean further detentions and delays for vessels traveling to the United States.

While welcomed, on the whole, by the shipping industry as an important step in circumventing the threat of terrorist attacks, the new measures are complicating life in the maritime business more than any single incident since the Exxon Valdez spill.

The following are a few of the new departments, statutes, regulations and initiatives that have been enacted, or in the process of being enacted.

The Department of Homeland Security (DHS)

Although federal agencies such as U.S. Customs, US Coast Guard, the Immigration and Naturalization Service (INS) have implemented new and revised programs, a major proposal has been the formation of the Department of Homeland Security (DHS).

The cabinet-level department would absorb up to 68 other federal agencies in an effort to put forth one coordinated program to address, develop and coordinate the implementation of a comprehensive national strategy on security in the United States. Agencies such as the U.S. Border Patrol, U.S. Customs, INS and the newly formed Transport Security Administration (TSA) are proposed to come wholly under complete control of the new DHS. The assimilation of other federal agencies, such as the FBI and the U.S. Coast Guard will only partly fall under this new organization. The measure was proposed last year by the Bush Administration and has been agreed in most respects by the Congress. However, the enactment of the legislation necessary to implement the proposal has stalled due to a debate over the power of the Executive to hire and fire personnel. This is no small matter, as the new agency would have the largest number of federal employees outside the Department of Defense.

Of prime interest to shipowners and operators is the role to be played in the new Department by the US Coast Guard. In recent remarks, ADM Thomas Collins, Commandant of the Coast Guard since May of this year, has stated that the core characteristics of the service – military, maritime, and multimission – would be preserved should the new Department be authorized. However, he also stated that, as part of a new Department with an expanded security mission, the service must deal with a new reality. In that respect, he admitted that the Coast Guard does not now have the capabilities envisioned under the legislation creating DHS, and would have to expand the size of the organization by 5-10% (the Coast guard currently consists of about 37,000 personnel in uniform, 5,800 civilians, and 1,500 reservists), as well as embark on a major capital improvement effort. Therefore, unless supplementary funding is provided in separate legislation not yet proposed, the Coast Guard will face severe problems under the proposed re-organization.

The Transportation Security Administration (TSA) - Enacted

The Transportation Security Administration (TSA) was formed as part of the Department of Transportation under the Aviation and Transportation Security Act of 2001. Admiral James Loy, the retiring Commandant of the Coast Guard was appointed head of the agency by President Bush, and the appointment was ratified by the Senate shortly thereafter. Under the legislation which formed the agency, the TSA has been tasked with coordinating the security efforts of transportation related industries. Among the initiatives sponsored by the TSA are, a new Transportation Workers' Identification Card System, and regulations concerning advance manifests of passengers and crewmembers.

Port Security Grant Program

The Port security Grant program was established through the Dept. of Defense Appropriations Act for FY 2002 (PL-107-117) to enhance maritime security. The grants are coordinated through the Transportation Security Administration of the Department of Transportation, and administered primarily through the Maritime Administration, with assistance from the U.S. Coast Guard.

The Act authorized up to \$92.3 million in competitive grants. The first round of grants, totaling \$92.3 million was awarded in June 2002. The priority set for the awards was based initially on the designation of strategic ports by MARAD (13 ports in all), controlled ports designated by the Coast Guard, and nationally economic important ports. Eligibility for the awards was established initially by the USCG captains of the Port and the Regional MARAD offices. The grants were awarded almost exclusively for security assessments and enhanced physical facility and operational security. The vast majority of the funds awarded went to state and municipal port authorities. Almost none of the money was awarded to the private sector, despite invitations from the federal government for private industry to apply. The next round of grants, which are expected to be announced in 2003, will likely be for infrastructure expenditures and enhancement of physical security measures. Some funds may be available for training programs, but no funds are likely to be available for capital projects.

The Maritime Transportation Anti-terrorism Act 2002 (MTAA)

Selected provisions of the MTAA

1. Grants Program

When enacted and signed into law the Act will authorize \$249 million in grants through FY 2005 to enhance maritime security, with \$7.5 million to be used for proof-of-concept technology, \$7.5 million to be used to reimburse ports for enhanced security measures undertaken since September 11, 2001, and provides for implementation for a maritime anti-terrorism plan approved by the Secretary of Transportation.

2. Assessment of Foreign Ports

The Secretary of Transportation will assess the effectiveness of security at foreign ports and will be authorized to deny entry to ships from foreign ports with inadequate security.

3. Implementation

The Secretary will be authorized to implement an interim final rule without regard to the provisions of the Administrative Procedure Act. This is significant because the Administrative Procedures Act normally requires a period for public hearings or comment before proposed regulations can be implemented.

4. Maritime Safety and Security Teams (MSST)

The Secretary will be required to establish maritime safety and security teams that will be trained to deter, protect against, and rapidly respond to threats of maritime terrorism. Shortly after September 11, 2001, the Coast Guard established ad hoc “strike teams” to board vessels arriving at key U.S. ports. Now, more formally organized under the *Sea Marshalls program*, the Coast Guard has boarded more than 10,000 vessels in the past year, 2,000 of which were in the port of New York alone. The current Sea Marshall program now administered by the Coast Guard will likely be replaced by the MSST’s, which are intended to be a quick response capability customized to meet a changing threat environment in the nation’s ports. (However, the Sea Marshall program is not likely to be phased out, but will be adapted to a different mission. There is current funding for special education and programs to be developed at the various maritime academies, and specifically at the U.S. Merchant Marine Academy.)

5. Background Checks

The Secretary will be given the power to ask the Attorney General to conduct background checks on applicants that will have access to secure areas. Although there has been much interest in and debate over this type of security provision, little of substance has been accomplished so far. Background checks and issuance of ID cards has been investigated, but there is no clear consensus on how such a program will be implemented. The only “major” step taken thus far is the issuance of a clarification of an existing regulation from the Coast Guard in August 2002, that from September 6, 2002, tamper-proof (laminated) ID cards, with the name of the person, a current photograph, and the name of the issuing authority, must be submitted to gain access to any marine facility in the U.S.

(presumably, a state drivers' license fulfills this requirement). To date we have seen no additional clarification of this requirement.

6. Security Plans

- a. The MTAA will create a National Security Plan (NSP), Regional Security Plans (RSP), local port security plans (PSP), the organizations to support them, and will require facilities and vessels to have security plans that are in coordination with the NSP/RSP and PSP structures. In anticipation of this requirement, the U.S. Coast Guard began working with local ports as early as November 2001 and, in January 2002, issued guidance in the form of a Navigation and Vessel Inspection Circular (NVIC) to local security committees to assist in the creation of a PSP. (The local port security committees are typically the Harbor Operations and Safety Committees formed by private industry and supported by the Coast Guard and local and state governments in the major ports of the United States. For example, the Harbor Ops Committee in New York is a committee of the Maritime Association of the Port of NY/NJ, and its membership includes vessel operators, tug companies, pilots, and personnel from the Port Authority, the Corps of Engineers, US Customs, INS, and the Coast Guard). The plans, many of which are now complete, are required under the NVIC to be submitted for approval by Dec 2003.

- b. Security Plans for Vessels

The MTAA will require private owners and operators of many vessels to have a US Coast Guard approved Vessel Anti-terrorism Plan (VAP), which will be managed in much the same way as the current Vessel Response Plans under OPA 90.

It will require the VAP to be submitted to the U.S. Coast Guard for approval prior to January 1, 2003. If these plans are not reviewed and approved by the U.S. Coast Guard by January 1, 2003, vessels may be barred from operating in the United States. Some of the features of the VAP will include: (1) identification of a Qualified Individual who, just like the VRP under OPA 90, will be pre-authorized to implement the plan; (2) identifying and ensuring by contract the availability of personnel and equipment necessary to deter or respond to a catastrophic emergency; (3) providing training and drills of the plan including government initiated unannounced drills; and (4) to provide VAP updates every five years and resubmit for approval after every major change.

- c. Intended SOLAS Amendments

In December 2002, the IMO will hold a Diplomatic Conference on maritime security to implement new regulations enhancing ship and port security and to prevent shipping from becoming a target for international terrorism. A number of areas of the SOLAS Convention are being considered for amendment, the most far-reaching being the proposed International Ship and Port Facility Security Code (ISPS Code) which would be implemented through a new Chapter XI/2 of the Safety of Life at Sea Convention (SOLAS).

The IMO has stated that the code is designed to provide a standardized, consistent framework for evaluating risk, enabling governments to determine the appropriate

response to the level of threat and vulnerability which exists currently.

The IMO states that the code provides several ways to achieve this:

1. For ships and shipping companies, the requirements are likely to include ship security plans, ship security officers, company security officers and certain onboard equipment;
2. Security plans and security officers for port facilities are also to be covered by the code;
3. Ships would be subject to a system of survey, verification, certification and control to ensure that their security measures are implemented, while port facilities would also be required to report certain security-related information to the contracting government concerned, which in turn would submit a list of approved port facility security plans, including location and contact details, to the IMO.

The amendments are planned to come into force in July 2004.

The above IMO proposed measures are similar to the MTAA's proposals in the United States, in particular, those relating to security plans. On this basis, the U.S. Coast Guard has been working closely with the IMO to attempt to find common ground in order that uniform regulations can be implemented on an international scale. Should common ground be found, it is likely that the resulting measures will eventually become part of the ISM Code. Regardless of whether the U.S. Coast Guard and the IMO come to an agreement on these new security measures, or implement measures independent of each other, there are common elements favored by the two organizations and, therefore, there are actions that vessel owners can take now in order to make their vessels more secure, and in order to reduce the risk of their vessels being delayed through inspections and detentions.

The following are a few recommendations to consider:

4. Designate a company security officer who can act on behalf of the company to implement overall security related actions;
5. Designate individual security officers for each individual vessel;
6. Initiate a security training program for vessel crewmembers;
7. Implement or review existing company guidelines on security, in particular, on controlling access to the vessel, making security rounds, searching the vessel, accountability of crew, emergency procedures etc.;
8. Review the security procedures used by vendors that are routinely used by the company and vessels, especially crewing suppliers; and

9. Review the adequacy of existing deck lighting, gangway access, means of locking or securing exterior hatches and doors, alarm systems, and alerting systems on all vessels.

Container Security Initiative (CSI)

The events of September 11 have led to demands for greater security measures for ships and cargoes, especially container cargoes. Approximately 90% of the world's cargo moves by container each year, nearly 50% of the value of all U.S. imports arrive via 16 million containers. Since the attacks, the possibility of shipping a "dirty bomb" in a container, and using containers as, effectively, cruise cabins by potential terrorists, is no longer *unforeseeable*.

The downside of the efficiency which containerization brought to supply was the difficulty of controlling exactly what was in the boxes. In the event of a serious threat, U.S. authorities have indicated that the country would close its borders in the event of a serious threat, and the movement of containers to and from the US would cease. Doing this, even for a brief time, would have an enormous and catastrophic impact on commerce all over the world, and that is why the US and other countries are putting so much effort into container security.

CSI is a program through which U.S. Customs is establishing agreements with other nations' customs organizations to craft security criteria for identifying high-risk containers, develop and implement pre-screening processes to target containers before loading, and deploy technologies to screen certain containers before loading, at major non-U.S. container ports. Specifically, the program allows US Customs officers to be based overseas at major container ports to coordinate, but not conduct, inspections of outbound boxes destined for North America. The bilateral CSI is aimed initially at the 'top 20' foreign container ports accounting for 70% of unitized import volumes.

The initiative has been signed by the Netherlands, France, Belgium, Germany, Singapore, and Canada, despite strong opposition from the European Commission, which fears that the agreement will undermine competition among member state ports. The concern is that bilateral agreements will favor Europe's container 'hub ports' and reinforce their domination by becoming *de facto* the only-accepted trade channels for US exports. In addition, the proposed U.S. legislation could create a gap between US and IMO regulations governing port assessments, and other maritime issues.

The European Commission would like to see a global consensus, led by concerted and considered international debate in the proper forum. Specifically, Brussels prefers a multinational approach, based on security measures discussed and endorsed by the International Maritime Organization.

Customs-Trade Partnership Against Terrorism (C-TPAT) In 2002, US Customs also implemented another initiative, aimed at increasing security by both shippers and Carriers. The program is entitled Customs-Trade Partnership Against Terrorism (C-TPAT). C-TPAT is a joint government-business initiative to build cooperative relationships that strengthen overall supply chain and border security. The program was designed to recognize that Customs can provide the highest level of security only through close cooperation with the ultimate owners of the supply chain— importers, carriers, brokers, warehouse operators and manufacturers. Through this initiative, US Customs is asking businesses to ensure the integrity of their security practices and communicate their security guidelines to their business partners within the supply chain.

Businesses must voluntarily apply to participate in C-TPAT. Participants sign an agreement that commits them to the following actions:

- Conduct a comprehensive self-assessment of supply chain security using the C-TPAT security guidelines jointly developed by Customs and the trade community. These guidelines, which are available for review on the Customs website, encompass the following areas: Procedural Security, Physical Security, Personnel Security, Education and Training, Access Controls, Manifest Procedures, and Conveyance Security.
- Submit a supply chain security profile questionnaire to Customs.
- Develop and implement a program to enhance security throughout the supply chain in accordance with C-TPAT guidelines.
- Communicate C-TPAT guidelines to other companies in the supply chain and work toward building the guidelines into relationships with these companies.

C-TPAT is intended to offer businesses an opportunity to play an active role in a worldwide supply chain security initiative, and to ensure a more secure supply chain for their employees, suppliers and customers. Beyond these essential security benefits, Customs will offer other potential benefits to C-TPAT members, including:

- A reduced number of inspections (reduced border times)
- An assigned account manager (if one is not already assigned)
- Access to the C-TPAT membership list
- Eligibility for account-based processes (bimonthly/monthly payments, e. g.)
- An emphasis on self-policing, not Customs verifications

C-TPAT is currently open to all importers and carriers (air, rail, sea), and Customs plans to open enrollment to a broader spectrum of the trade community in the near future. Applicants must submit signed agreements to Customs, which will represent their commitment to the C-TPAT security guidelines. Applicants will also submit a supply chain security profile questionnaire at the same time they submit their signed agreements or within a specified time thereafter. All information on supply chain security submitted by companies applying for the C-TPAT program will be confidential. Customs will not disclose a company's participation in C-TPAT without the company's consent.

Customs will be looking for carriers to join C-TPAT to enhance existing security practices and better address the terrorism threat to international air, sea, and land shipping. The agency has stated that it will work to ensure that C-TPAT participation does not require duplicate work for current Customs Carrier Initiative Program (CIP) participants. CIP participants already subscribe to the importance of security from a narcotics-smuggling perspective and are well positioned to expand their security focus to encompass anti-terrorism.

III. Port Operations Changes in U.S. Ports

Armed Guards

After an incident in March 2002, when several Pakistani citizens jumped a ship in Virginia and illegally entered the country, the INS and US Coast Guard have been requiring foreign-flag vessels to hire armed guards to keep their crews on board during port calls.

These demands for armed guards have primarily been imposed on the Gulf Coast but are now cropping up in the East and West Coast. However, there is little or no consistency in the imposition of the requirement of armed guards, it being very much at the discretion of the INS and U.S. Coast Guard. Guards have been required at one port, but not at other ports.

This has created much uncertainty and ambiguity, which has been compounded by new rules imposed by the Justice Department which allows the INS to issue a detain-on-board order or demand for guards without giving any reason whatsoever. Crews have been detained on board their vessels at US ports often on the sole basis of their nationality (in most cases Middle Eastern or South Asian) and without any reason, let alone any indication of any real or imminent threat to the port or its surroundings.

These requirements for armed guards are hitting ship owners with unexpected and unfair expenses. In August 2002 Skaarup Shipping's bulker Farland was hit with a demand for armed guards at Port Arther in Texas which cost the owner about \$11,000 and sparked a dispute with the charter on who should foot the cost.

Standard charter parties do not contain a clause to determine who foots the bill, which has instigated disputes between owners and charterers on who should pay. Owners and charterers should consider adding a clause in their charter parties to apportion the costs accordingly. However, many in the industry have argued that the expense of posting security guards to keep crews from shore should be borne by the ports themselves.

In this regard, Bimco and the ICS (International Chamber of Shipping) have submitted a joint paper to the IMO demanding that the cost of keeping port facilities secure should be borne by the port itself. The joint paper makes a distinction between 'ship security' responsibility for which should be borne by the owners, and 'port facility security', responsibility for which should be borne by the port.

The two bodies are pushing for this provision to be part of the proposed amendments to the SOLAS Convention, which is expected to be ratified by the end of this year.

Guard Service is generally not mandated when the ship has a crew list or all crewmembers have individual visas. However, the US State Department is planning elimination of the crew list visa shortly. For now, vessel owners would be advised to attempt to provide their crew members with individual visas in order to attempt avoid undue delays and expense.

Boarding Parties and Advance Arrival Notices

One outgrowth of OPA '90 was the establishment of a database in the U.S. Coast Guard of all vessels reported entering U.S. ports, with the intent of developing the ability to identify possibly sub-standard vessels before they entered the U.S.. With this database and an analysis of vessels boarded over time, the Coast Guard developed a Boarding Matrix to guide them in their choice of vessels to be boarded. The Matrix is based on a number of factors, including the time of the vessel's last call in the U.S., the flag of the vessel, etc. Since September 11, 2001, all vessels arriving in U.S. ports have been required to give 96 hours notice of arrival to the Coast Guard. Armed with all the information from the arrival notices and the Boarding Matrix, the Coast Guard is now able to identify perceived security risks and target such vessels for boarding well in advance of the suspect vessel's arrival. In some cases, the identified vessels are met outside the port in territorial waters and boarded for inspection by the Coast Guard. The vessels may also receive follow up visits after berthing, assuming they are allowed into the port. (In one recent case, during a second boarding by Coast Guard personnel on a vessel in New York, while searching for stowaways, the radiation detectors of the boarding party indicated a radioactive source on the vessel. The ship was sent to anchorage outside the port under armed guard and was boarded by special investigation teams from a variety of federal agencies. The ship was eventually allowed back into port when it was discovered that the source of the radiation was radon (a naturally occurring radioactive gas) contained in a shipment of ceramic tiles. Needless to say, the delays and expenses were considerable.

24-Hour Advance Manifests

The U.S. government has also announced plans to require ships bound for the US to provide cargo manifests 24-hours before a container is loaded in a foreign port.

One of the most potentially disruptive and challenging of a range of recent US-brokered moves to craft a more watertight international maritime security regime, is the requirement for this 24-hour advance notice of contents of US-bound containers before loading at a foreign port. This will have a major impact on carriers. Currently the system has become so speedy and sophisticated, with just-in-time delivery, that providing information on goods after the ship has sailed has become the norm.

In addition to having to provide the ships' manifests to customs 24-hours before the cargo is loaded, the US Coast Guard is also requiring detailed information about a vessel's charterer in its advance notifications of arrivals. The information must be based on the Charterer holding "contracts for the majority of a vessel's cargo carrying capacity" and will be used by the Coast Guard to improve its identification of sub-standard vessels. Penalties for mistakes will be costly – as high as \$20,000 could be imposed for incorrect manifests.

Bill of Lading Descriptions

Heavy penalties will also be imposed for those using certain current phrases contained in standard bills of lading.

Under US bill S2424, Port Terrorism Prevention Act 2002, phrases such as 'freight of all kind', 'hazardous not other specified' and 'said to contain', or "any description that does not provide adequate information regarding the merchandise on any manifest required by the customs services" will be prohibited. Penalties for inaccurate manifests will be between \$10,000 and \$20,000.

Another requirement of the Bill is the manual checking of 10% of cargo on all vessels, which will cause delays in discharge and clearance procedures.

Fingerprinting

The US Department of Justice has further notified its intention to implement a so-called National Security Entry-Exit Registration System, under which foreign visitors deemed as a security threat will be fingerprinted at ports of entry including harbors.

The US Department of Justice has stated that these fingerprints will be matched against a database of known criminals and known terrorists. All nationals of Iran, Iraq, Libya, Sudan and Syria will be subjected to this check.

The scheme has already come into force at a few unspecified ports of entry as of September 11, 2002, and will be extended nationwide in October 2002. Again, this could mean further detentions and delays of vessels.

IV. Conclusion

Many changes have occurred in the last two years in relation to security, in particular, in the United States, which has instigated an enormous and rapid campaign to secure its borders. This has, inevitably, affected the way the maritime industry operates, in that there are a number of key security issues facing the maritime industry trading to and from the United States. These include increased scrutiny of cargo, increased scrutiny of vessels and their crews, and increased security precautions at marine terminals throughout the United States. Soon we shall also see many more changes on the international level. It is important to keep abreast of these changes, in the form of new legislation, regulations and initiatives, and it is important to be prepared for them. Being unprepared may very well increase the risk of long and costly delays.

Please feel free to contact us regarding any inquiries and/or comments relating to this article.

Chalos O'Connor, LLP
366 Main Street
Port Washington, NY 11050
Phone: 516-767-3600 / Fax: 516-767-3605
www.codus-law.com

APPENDIX

Glossary – Federal Agencies and Terminology

CDRG:	Catastrophic Disaster Response Group
CEPPO:	Chemical Emergency Preparedness and Prevention Office
CIAO:	Critical Infrastructure Assurance Office
COTP:	Captain of the Port (US Coast Guard)
CSIS:	Center for Strategic and International Studies
CT:	Counter-terrorism
DOD:	Department of Defense
DOT:	Department of Transportation
DOJ:	Department of Justice
DPC:	Domestic Policy Council
EO:	Executive order
EPA:	Environmental Protection Agency
FBI:	Federal Bureau of Investigation (DOJ)
FEMA:	Federal Emergency Management Administration
FRERP:	Federal Radiological Emergency Response Plan
FRP:	Federal Response Plan
GAO:	General Accounting Office
HSPD:	Homeland Security Presidential Directive
ICC:	Interagency Coordination Center
INS:	Immigration and Naturalization Service
MARAD:	Maritime Administration (DOT)
MSO:	Marine Safety Office (US Coast Guard)
MTS:	Maritime Transportation System
NAPA:	National Academy of Public Administration
NCP:	National Contingency Plan
NDPO:	National Domestic Preparedness Office (DOJ)
NIPC:	National Infrastructure Protection Center
NSDD:	National Security Decision Directive
NSPD:	National Security Presidential directive

PCCIP:	Presidential Commission on Critical Infrastructure Protection
PDD:	Presidential Decision Directive
TSA:	Transportation Security Administration (DOT)
USA-COE:	US Army – Corps of Engineers
USCS:	US Customs Service
USCG:	US Coast Guard
WMD:	Weapons of Mass Destruction

Timeline of National Security Incidents

1988:	PanAm Flight 103 (Lockerbie, Scotland)
1990:	Operation Desert Storm begins
1991:	Operation Desert Storm; Kuwait oil fires
1992:	Weapons inspections begin in Iraq (end in 1997)
1993:	Bombing of World Trade Center – NYC
1994:	Outbreak of Cryptosporidium – Milwaukee, WI
1995:	Unabomber attacks – various locations Sarin gas attack – Tokyo, Japan Bombing of Federal Building – Oklahoma City, OK
1996:	Bombing at Olympics – Atlanta, GA Bombing of US military barracks – Saudi Arabia
1998:	Bombing of US Embassies – Kenya, Tanzania
1999:	Salmonella outbreak – Oregon
2000:	Bombing of USS COLE – Yemen
2001:	World Trade Center and Pentagon attacks – NYC, Wash. DC Anthrax outbreak - various

Statutory and Regulatory Time Line

1974:	Disaster Relief Act
1988:	Disaster Relief and Emergency Assistance

	Act (Stafford Act)
1989:	Terrorism responsibility assigned to DOJ by Domestic Policy Council
1993:	Joint Resolution of Congress to strengthen federal interagency planning by FEMA
1994:	Stafford Act amended and Civil Defense Act repealed
1996:	Weapons of Mass Destruction Act (Nunn-Lugar-Domenici) Anti-Terrorism and Effective Death Penalty Act
2000:	Disaster Mitigation Act
2001:	Supplemental Act for Response and Recovery USA Patriot Act of 2001 Aviation and Transportation Security Act Defense Authorization Act

Executive Orders Timeline

1988:	EO 12656 – Assignment of emergency preparedness responsibilities EO 12657 – Emergency preparedness planning at commercial nuclear Powerplants
1989:	EO 12673 – Stafford Act authority delegated to FEMA
1993:	NSDD 66
1994:	EO 12919 – National defense industrial resources preparedness
1995:	PDD 39 – Policy on counter-terrorism
1996:	EO 13010 – Critical infrastructure protection
1998:	PDD 62 – Combatting terrorism PDD 63 – Critical infrastructure protection PDD 67 – Continuity of government
1999:	EO 13129 – Prohibit transactions with Taliban EO 13130 – National Infrastructure Assurance Council
2001:	EO 13228 – Homeland Security

EO 13231 – Critical infrastructure protection
HSPD 1 – Homeland Security Council
EO 13234 – Citizen preparedness
HSPD 2 – Immigration policies

FEDERAL PLAN TIMELINE

1988: National Security Emergency Plan (DOD)
1992: Federal Response Plan (Stafford Act)
1996: FRERP revised
1997: Terrorism Incident Annex to FRP adopted by FEMA
1998: Interagency Plan on Counter-terrorism prepared
1999: FRP revised
2001: Interagency Domestic Terrorism Concept of Operations Plan
Terrorism Attachment added to FEMA All-Hazard Planning Guide

Organizational Changes Timeline

1978: FEMA established and organized
1996: National Infrastructure Protection Commission
1997: Terrorism Coordination Unit (FEMA)
1998: NIPC under DOJ
NDPO created
CIAO established
Chemical Safety Board formed
2000: ICC formed
2001: Office of National Preparedness formed (FEMA)
Homeland Security Office established
Homeland Security Council formed
Transportation Security Administration formed (DOT)

Reports and Documents Timeline

- 1990: Presidential Commission on Aviation Safety and Terrorism
- 1992: GAO Report – federal, state, and local response capabilities
- 1993: EPA Report to Congress on Hazmat
- 1995: Various reports/analyses on Oklahoma City bombing
- 1997: FEMA and FBI report to Congress
PCCIP Report
- 1999: Hart/Rudman Report I
Gilmore Report I
- 2000: GAO Report on Counter-terrorism
Hart/Rudman Report II
National Commission on Terrorism Report (Bremer Commission)
- 2001: Gilmore Report II
Hart/Rudman Report III
CSIS Report on Chemical/Biological/Radiation threats
GAO Reports on Counter-terrorism
Gilmore Report III