ABSTRACT
The terrorist attacks of 9/11 brought an urgent, necessary call to protect the safety and security of the nation’s Critical Infrastructure/Key Resources (CI/KR). Most of these efforts have been to deter/prevent a terrorist attack through vulnerability assessment and increased physical security (e.g. “gates, guns and guards”). Just as the federal government was getting on solid ground with the National Infrastructure Protection Plan (NIPP). This provided a glimpse into these concerns and brought increased attention back upon this long standing marine safety mission. Ironically the 2006 “Safe Seas” exercise tested almost the very scenario of the COSCO BUSAN one year ago to the day of the spill. “Safe Seas” and other major drills (like “TOPOFF”, etc.) are tremendous tools for government and private sector stakeholders to enhance preparedness to response and test existing security and infrastructure protection systems.

Given the above, traditional Oil Spill Response (OSR) is now part of a broader, more complicated systems-approach to domestic Incident Management (IM). The United States Coast Guard’s Marine Environmental Protection (MEP) mission has required the unique military/regulatory service to forge a collaborative relationship with the oil and gas industry - or “sector” (as defined in the National Infrastructure Protection Plan NIPP). This government-to-industry partnership was born out of decades of marine safety prevention/response efforts most visible following the Oil Pollution Act of 1990 (OPA 90). Many involved in the field of emergency management: as well as their security counterparts recognize it is difficult to understand both IM and IP, despite the myriad of new and developing federal plans and doctrine as we pass the half way point of the first decade in the Post 9/11 “new normalcy.” Due to dynamic and synergistic partnership between the U.S. Coast Guard and the American Petroleum Institute (API) a coordination and communication opportunity was identified that resulted in a concept of simplifying the landscape via a “3 R+” concept.

The focus areas of this paper are:
• To bring increased clarity to the current and emerging state of interoperability between the government and the private industry sector.
• Provide a simplified “Big Picture” view of what private sector professionals (middle to upper management in the response/safety & health fields) need to know regarding the framework of the national system for our critical infrastructure and first line response, using the oil & gas sector as an example;

Note: Although the target audience for this paper/presentation are private sector professionals, primarily in the response and security fields, the plans highlighted and information outlined could apply to those working IM or IP in any industry or government sector.

THE OIL & NATURAL GAS INDUSTRY – A MODEL PRIVATE SECTOR PARTNER IN THE MARITIME DOMAIN
For many years the U.S. Coast Guard has forged strong collaborative partnerships with many stakeholders throughout the maritime industry. One of the strongest of these partnerships has been with the oil and natural gas (ONG) industry, or “Sector” as defined by the DHS. The relationship between the Coast Guard and the ONG has been focused primarily around the Marine Environmental Protection (MEP) mission area.

The importance of the ONG industry to national security and economics is obvious, yet the following displays the magnitude:

“Domestic petroleum assets are widely distributed, consisting of over 300,000 producing sites, 4,000 offshore platforms, 600 natural gas processing plants, 160,000 miles of liquid pipelines, numerous crude oil and liquefied natural gas (LNG) offloading ports and terminals, 144 refineries, 1,400 finished product terminals, 7,500 bulk stations and 170,000 gasoline retail stations.”

The vast majority of these assets are small, geographically remote and therefore do not present a significant security risk to the national economy, national security or public safety. However, the petroleum industry strongly supports taking prudent measures to effectively minimize security risks posed by acts of terrorism, where warranted.

FEDERAL GOVERNMENT PERSPECTIVE – THE DHS
To complete the focus on IM and IP, it was necessary to involve the Department of Homeland Security (DHS). The lead for IM
with the DHS resides with FEMA’s Incident Management System Division (IMSD), which was formed in the spring of 2007. Other key DHS stakeholders are the Offices of State & Local Coordination and the Private Sector Office (PSO).

As defined in the NIMS, the IMSD “provides strategic direction, oversight, and coordination of NIMS.” It also supports both routine maintenance and the continuous refinement of the NIMS and its components. The IMSD oversees and coordinates all aspects of NIMS, including the development of compliance criteria and implementation activities at Federal, State, tribal, and local levels, providing guidance and support to jurisdictions, emergency response providers and their associated organizations as they adopt the system. It oversees and coordinates publication of NIMS and its related products including the review and certification of training courses and exercise information.

There are several key areas where the evolving concerns of critical infrastructure owners and operators and other private sector involvement in the NIMS is unique and differentiated from historic emergency response field practices and traditional government agencies.

These areas need specific text additions to clarify unique concerns or issues of private sector & critical infrastructure. The bottom line is that NIMS involves more than the emergency response side of the house, but also participation from the Security/Infrastructure Protection (IP) paradigm, to be effective.

THE PRIVATE SECTOR PERSPECTIVE

Obviously private industry plays the largest role in both the number of incidents they handle and the scope of financial responsibility. To this end, the NIMS Plan recognizes the private sector role as follows:

“The private sector plays a vital support role in emergency management and incident response and should be incorporated into all aspects of NIMS. Utilities, industries, corporations, businesses, and professional and trade associations typically are involved in critical aspects of incident response.”

These organizations should prepare (e.g., planning, training, and exercises) for all-hazard events that may affect their ability to deliver goods and services. One of the things that is vital for the ONG sector (or any sector) professional is to embrace the need to continue to emphasize prevention and preparedness – not just response.

The first emphasis is that government must establish a common set of private-sector expectations, consistent with local, tribal, State and Federal roles, responsibilities, and Concept of Operations (CONOPS). These expectations are particularly important with respect to private sector organizations involved in Critical Infrastructure and Key Resources (CIKR) areas.

Additionally, private sector organizations need to continue to enter into more cooperative assistance agreements/compacts with agencies, non-government organizations (NGOs) and other private sector organizations.

An outstanding example of one such organization is the Business Executives for National Security (“BENS”) and the Emergency Management Assistance Compact (EMAC). To that end, during Hurricanes Katrina and Rita nearly 66,000 personnel were deployed under EMAC. These efforts may help to clarify the respective capabilities, roles, and/or expectations of the parties involved in preparing for and responding to, an incident.

The private sector may be a source for best practices in many areas of preparedness, emergency management, and response. According to the NIMS update, new material has emerged that better defines the preparedness role of NGOs including:

- NGOs and the private sector should be integrated into a jurisdiction’s preparedness efforts, especially in planning, training, and exercises.
- Memoranda of Agreement (MOA) should be established with NGOs and private sector organizations prior to an incident so each organization will be aware of the capabilities, expectations, and roles of the other.

In support of the many private sector industries are two NGO initiatives; the DHS led Business Roundtable and the Business Executive for National Security – a non-profit consortium.

As leaders of companies with over $4.5 trillion in annual revenues and more than 10 million employees, Business Roundtable’s chief executive officers play a critical role in assessing and managing risk. Since the 2001 terrorist attacks, United States corporations have spent billions on security planning and infrastructure protection. To further assist chief executive officers with protection and continuity issues, in February 2005 Business Roundtable published a comprehensive guidebook entitled Committed to Protecting America: CEO Guide to Security Challenges.” It provided strategic considerations and options for managing a wide range of homeland security risks, integrating primary areas of corporate management and drawing on corporate expertise to develop planning frameworks.

THE “3 R+ CONCEPT”

In developing this paper, we found the need to synthesize the many different operational paradigms that quantify the continuum of pre-event to post incident activities. (See figure 1)

There have been many versions of the security and response spectrum from prevent and protect to defend and deter, with some component of recovery and mitigation to cap it off.

The following is a simplified 3 step “R” approach from Resiliency to Response to Recovery. (With a final “R” for reference)

The 1st “R”:
Resiliency
(through Infrastructure Protection-IP)

Perhaps one of the most stated factsoids in the field of U.S. homeland security is that an estimated 85% of the nation’s critical infrastructure is privately owned. Over the past few years, the federal government has encouraged cataloguing of critical infrastructure through the establishment of the National Asset Database, a comprehensive inventory of all assets in the nation. The basis for the federal government’s role in critical infrastructure protection is a series of Homeland Security Presidential Directives (HSPDs) since the September 11, 2001, terrorist attacks. Many of the referenced national planning documents have a nexus to an HSPD. (See the enclosed reference at the end of the article)

The directive most applicable to the area of critical infrastructure protection is HSPD-7: Critical Infrastructure Identification, Prioritization and Protection. HSPD-7 establishes a national policy for federal departments and agencies to: “identify, prioritize, and protect the nation’s critical infrastructure,” which it defines as:

...”systems and assets, whether physical or virtual, so vital to the United States that [their] incapacity or destruction… would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

---

2 “Mechanisms for Collaboration EMAC & Katrina” by Mr. William L. Waugh, The Public Manager, Winter 06-07

3 The NIMS policy document was updated in 2007.

HSPD 7 designates lead federal agencies, known as sector-specific agencies, for each sector of the economy and charges those lead agencies with the following: collaborating with all relevant federal agencies, state and local governments, and the private sector, including key people and entities in their infrastructure sector; “conducting or facilitating vulnerability assessments for the sector; and encouraging risk-management strategies to protect against or mitigate the effects of attacks against critical infrastructure and key resources.”

The Sector Specific Agencies (SSA) also are required to collaborate with the private sector to develop information-sharing and analysis mechanisms and to work with industry to identify, prioritize, and coordinate the protection of critical infrastructure and key resources. They facilitate the sharing of information about physical and cyber threats, vulnerabilities, potential protective measures, and best practices for all hazards response.

The 2nd R: Response (through Incident Management)

Since the creation of the National Incident Management System (NIMS) policy in 2005, the role of private industry is still emerging and often difficult to understand compared with that of their government counterparts. For example, even though the private sector is clearly recognized in the revised NIMS plan, they are not required to be “NIMS compliant.” This is problematic as the government agencies they will be working with are required to be [NIMS compliant].

Although the new National Response Framework (NRF) is far easier to read and understand than its predecessors—the Federal Response Plan (FRP) and the National Response Plan (NRP) - it is still another major document to find, print and digest for the average private sector professional. Regardless of the difficulty, industry professionals in the OSR and Security fields need to better develop concepts of operations; manage expectations in real events and illustrate communication mechanisms so that industry can be more interoperable with their government partners.

The Coast Guard had long been a leader in the use of the Incident Command System (ICS) when it reorganized its existing shore command structure (Groups and Marine Safety Offices) to single commands called “Sectors.” The concept was based around the need to provide one command in a geographic area for control over all local CG operations.

While the overall missions remained the same, the only new section created was that of the Incident Management Division (IMD). The IMD pulled expertise from the Marine Safety (Marine Environmental Response, Inspections, etc.) and the traditional “Group” or small boat station operations (Law Enforcement, Search and Rescue, etc.) career paths. Initially, IMDs were understaffed and had no real clear idea of their mission and most Sectors placed the function of Marine Environmental Response (MER) as the sole responsibility of IMD. According to Coast Guard “Document One” these are the primary strategic mission objectives for IMDs are:

- Protect the marine environment and living marine resources of Sector AORs;
- Strengthen Sector preparedness and mitigation efforts against acts of terrorism, natural disasters, or other emergencies;
- Provide scalable and robust all-hazard response capabilities;
- Strengthen Sector recovery plans and capabilities; and
- Provide scalable and robust all-hazard recovery assistance.

The challenge is the Coast Guard has to be able to have an Incident Management Team (IMT) that is capable of responding to all types of incidents, and then seamlessly transition them into Incident Command System structures during large scale events – often in a multi-jurisdictional situation. This is quite counterintuitive within the CG as the traditional missions of SAR, Marine Casualty investigations, vessel inspections, and blue-collar law enforcement missions were previously conducted separately by individual divisions working independently of each other.

While the CG transitions to this new IM structure, the private sector, especially the OSR industry, should understand the underlying principles and missions of the Incident Management professional that they will work with during an incident. This is best accomplished by being conversant with the NIMS and NRF, etc. Industry should also realize that they need to understand the CG is looking beyond specific problems and/or issues, but at a much more comprehensive all-hazards response posture.

The 3rd R: Recovery

Although the heroic Search and Rescue (SAR) actions in the response and mitigation phases following Hurricanes Katrina & Rita were impressive, the environmental efforts were often very problematic. Lessons learned on recovery issues following the significant disruption of the MTS during Hurricane Katrina were additionally identified and reported on by the Maritime Recovery and Restoration Task Force (MR TF). The Final Report of the (MR TF) indicated that the Coast Guard should serve as the leader for MTS recovery a National Transportation Security Incident (NTSI) or and any other incident that would significantly impact the MTS. Resumption of commerce and recovery of the marine transportation system (MTS) following a significant disruption is a significant issue of concern for Congress, federal agencies, and industry. The Maritime Transportation Security Act (MTSA) of 2002 required that the National Maritime Transportation Security Plan (NMTSP) include a plan to restore cargo flow following a National Transportation Security Incident (NTSI). This concept was reiterated in HSPD 13 and the National Strategy for Maritime Security (NSMS). Subsequently, strategic concepts supporting efficient recovery of the MTS were documented in the Maritime Infrastructure Recovery Plan (MIRP). The Coast Guard’s 2006 Strategy for Safety, Security and Stewardship (referred to as CGS) identifies it as one of the USCG Commandant’s top 6 strategic priorities.

The 2007 formation of the MTS Recovery Units (MTSRU) is evidence that Recovery/Surge Units supporting the post incident recovery of the Marine Transportation System (MTS) infrastructure assessment and recovery.

The + R

“References”

Most industry managers are of the opinion that even though government plans and policies are important, they only want to know: “what is important to my operation” or simply stated – what do I need to know. The one handout [enclosure 1] to this article is an overview of the principle references.

In an era where managers and senior professionals are inundated with documents and references to the point of information overload, we wanted to simplify and with just a short synopsis of the major federal plans.

COLLABORATION IN ACTION

USCG INDUSTRY TRAINING

The idea for this article came from lessons learned in a USCG Industry Training Program (IT) conducted by LCDR Dennis Branson.

For over forty years, the Coast Guard has assigned active duty commissioned officers to conduct short term “Industry Training” (IT) with the maritime industry. The stated program objective is
to “prepare them for mid-management and executive level positions in the Coast Guard.” There are multiple areas of emphasis and selection is made for: Merchant Industry Training (MIT), Marine Environmental Protection Training (MEPT), Port Safety & Security Industry Training (PSIT) and Investigation Industry Training (IIT). The primary objective of the training is stated as follows:

“To develop the participant's conceptual and analytical capability by observing and working in a marine industry operational mid-management position. The participant is given a unique and valuable opportunity to observe and evaluate the actions, reactions and interactions of marine industry at the mid to executive management level to gain a better operational perspective.”

Following discussions with senior leaders in the Incident Management field, LCDR Branson determined to focus his IT program on the emerging state of private sector integration into the National Incident Management System (NIMS). Leveraging the close proximity of USCG Headquarters to ExxonMobil’s Global “Downstream” headquarters (located in Fairfax Virginia), LCDR Branson had the unique opportunity to get an inside perspective of the largest publicly traded integrated oil and gas company in the world. Working in the Emergency Preparedness & Response (EP&R) Division provided a glimpse into the following topics:

- Oil Spill Response (OSR), prevention, & exercise preparedness
- Business Continuity Planning (BCP)
- Pandemics

While working on the ExxonMobil program, a second opportunity presented itself for LCDR Branson to become involved in an even broader industry perspective of ONG issues in working with the Emergency Response Policy division at the American Petroleum Institute (API). Located in Washington, DC, API is the main U.S. trade association for the oil and natural gas industry representing about 400 member corporations involved in production, refinement, distribution, and many other aspects of the industry. Per their mission statement, API:

- Represents the petroleum industry to the public, Congress and the Executive Branch, state governments and the media;
- Negotiates with regulatory agencies, represents the industry in legal proceedings;
- Participates in coalitions;
- Works in partnership with other associations to achieve our members’ public policy goals.

API conducts much of its work through internal staff committees, as well as with representatives of the member companies. Two vital working groups are the semi-annual API Spills Advisory Group (SAG) and Emergency Preparedness & Response (EP&R) Managers committee which have participated from government and industry alike. Under the IT program responsibilities, LCDR Branson also participated in the API security committee meetings on multiple occasions and was able to provide informational briefings on current Coast Guard operations and IM concepts to API staff and member company meetings. Leveraging many of the mutually-beneficial relationships developed under this initiative, recommendations were made to continue to leverage opportunities with the ONG through API and a major industry company like ExxonMobil.

NEXT STEPS...

Based on the work of LCDR Branson, API was asked by the ONG Sector Coordinating Council’s (SCC) to put together an Emergency Management (EM) work group to address potential coordination gaps between the ONG (and chemical industries) with regulating federal agencies. Initial discussions indicated that the focus of this EM workgroup would be for both oil, natural gas and the chemical industry’s incident management professionals. The SCC agreed and both the ONG and Chemical Sectors are represented on this workgroup. Discussion topics will be at the strategic decision making level on such topics as: business continuity planning, law enforcement (DOJ, FBI, EPA) relations, consolidating spill exercises and certification.

A recommendation that came directly from the Industry Training program’s final report was for Coast Guard Headquarters to consider developing a senior level program for higher ranking Officers to work with the industry through major trade associations like API. One final initiative resulting from the IM-IT work is the possibility that the DHS IMSD might develop an exportable training course to explain the NIMS and the new NRF through a simplified approach like the “3 R’s” concept.

The ONG and Coast Guard example of partnership, through close field work and cooperative programs like Industry Training, will continue to be a leader in government to private industry

ENCLOSURE (1) TO INCIDENT MANAGEMENT NATIONAL PLANS

The following plans and policies are critical for private sector managers in the Emergency Preparedness & Response (EP&R), Security and Safety fields.

National Contingency Plan (NCP)

The subsequent pollution following the sinking of the M/V TORREY CANYON and sitting Presidents, Congress, and a number of Federal agencies, molded together a vast plan to deal with the most massive environmental hazards. From a plan that began with responsibilities for five Federal agencies and no statutory authority, the National Contingency Plan has been expanded and revised over time. Today this plan brings together the expertise of fifteen Federal agencies, state and local government responders, owners and operators of oil and hazardous substance facilities and vessels, and has statutory authority in several big name environmental laws such as the Clean Water Act (CWA), the Comprehensive Environmental Response, Compensation, Liability Act (CERCLA) and the Oil Pollution Act of 1990 (OPA 90).

The Superfund is the Federal government’s program to clean up the nation’s uncontrolled hazardous waste sites. Under the Superfund program, abandoned, accidentally spilled, or illegally dumped hazardous waste that pose a current or future threat to human health or the environment are cleaned up. To accomplish its mission, EPA works closely with communities. Potentially Responsible Parties (PRPs), scientists, researchers, contractors, and state, local, tribal, and Federal authorities. Together with these groups, EPA identifies hazardous waste sites, tests the conditions of the sites, formulates cleanup plans, and cleans up the sites.

The National Response Framework (NRF)

DHS Preparedness and FEMA co-chaired an interagency effort to revise and rewrite the National Response Plan (NRP). The rewrite focused on 17 key issues identified in the Post-Katrina review related to emergency response operations, structures, roles, and responsibilities identified in the 2004 version of the NRP. The review also focused on key positions in National and regional levels and their alignment based on current NIMS guidance. The new document now called the National Response Framework (NRF) represents a substantial revision to the NRP in organization and

---

5 USCG Marine Safety Manual Volume I, Chapter 7
6 Formed November 30, 1999, by the merger of Exxon and Mobil
ExxonMobil is ranked the largest company in the world.
7 API Policy Statement, dtwd May 7, 2007
structure. The NRF is clearly written to aid better understanding of agency roles and missions. As an example, key features of the National Incident Management System (NIMS) are emphasized and presented as priority concepts within the NRF. Many of these are current NRP concepts but the workgroup, using lessons learned from Katrina and other situations, sought to specifically highlight and focus on those features intended to strengthen federal, state, and private industry efforts. It is important to note that the new document relies heavily on existing concepts and principles; the intent was not to create a new system but rather to strengthen and clarify the existing one.

A major goal of the NRF is to integrate current plans and operations in the national system with out impacting day-to-day operations. The NRP sought to do this as well so this revision simply charts a clearer course to achieve the goal of scalable response and preparedness efforts. The NRF relies on an integrated interagency approach to response and preparedness. Our Sectors interact with their state, local and private industry counterparts everyday in preparedness forums such as Area Maritime Security Committees, Area Contingency Plan and Port Readiness Committees. These efforts represent real, working examples of how the NRF hopes to lead the broad number of federal, state, local, and private industry entities toward an integrated “all risk all hazard” approach to preparedness and response.

The attachment to this paper lists the key changes and is certainly not all-inclusive. CG-3RPP is drafting a message to summarize and clarify existing Coast Guard response management and preparedness guidance while laying out a series of easily implemented policy improvements. The message will also explain how ongoing Coast Guard efforts clarify our connections and obligations under the NRF as well.

The National Incident Management System (NIMS) Policy

HSPD 5 is the Management of Domestic Incidents: “To enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system.”

The National Incident Management System provides a systematic, proactive approach guiding departments and agencies at all levels of government, the private sector, and nongovernmental organizations to work seamlessly to prepare for, prevent, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life, property, and harm to the environment.

The five revised “Components” of the NIMS are:

1. Preparedness: this component has been significantly expanded to describe the specific measures and capabilities that emergency management/response personnel and their affiliated organizations should develop and incorporate into their overall preparedness programs. These capabilities will help enhance the operational preparedness which is necessary for all-hazards emergency management and incident response. Additionally, an overview of the relationship between NIMS and other preparedness efforts was added.

2. Communications & Information Management: The underlying concepts and principles of this component (which was heavily revised) reinforce the use of a flexible communications and information system with which emergency management/response personnel can maintain a constant flow of information throughout an incident.

3. Resource Management: This component involves the coordination, oversight, and processes necessary to provide timely and appropriate resources during an incident. Utilization of the standardized resource management concepts such as typing, inventorying, organizing, and tracking will facilitate the dispatch, deployment, and recovery of resources before, during, and after an incident.

4. Command & Management: The three major elements of this component are the Incident Command System, Multi-agency Coordination System (MACs) and Public Information Systems (PIS). Under the 2007 revision, all remain intact with added clarification and only minor changes in terminology.

5. Ongoing Management & Maintenance: This component was restructured to contain two subsection: National Integration Center and Supporting Technologies. The National Integration Center (NIC) section sets forth the responsibilities of the NIC (as it relates to the NIMS document). The Supporting Technologies discusses principles necessary to leverage science and technology to improve capabilities and lower costs.

FEMA has a free distance learning course that can be accessed on the internet at the following address: http://training.fema.gov/EMIWeb/IS/is700.asp

The National Infrastructure Protection Plan (NIPP)
The National Infrastructure Protection Plan (NIPP) was released by the DHS in 2006 and provides a structure for collaboration among the private sector, state governments, and federal agencies in protecting Critical Infrastructure and Key Resources (CI/KR). The “backbone” of the NIPP is a network of industry-specific, Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) through which representatives of the private sector will share information, collaborate and develop strategies for protecting critical infrastructure with the government.

The industry-based SCCs are the principal focal point for private sector coordination with the government on critical infrastructure protection activities and issues. Membership of the SCCs will vary by sector but should include a broad base of owners, operators, associations, and other entities within each sector. A private sector cross-sector council has also been established to address cross-sector issues and interdependencies. In other words, GCCs are the public-sector counterparts to the SCCs and are designed to provide interagency and cross-jurisdictional coordination. The various industry sector and government coordinating councils are themselves coordinated through the partnership for critical infrastructure security composed of representatives of each of the sector coordinating councils, and the NIPP senior leadership council, composed of representatives of each GCC.

Sector-specific plans detailing with the application of the NIPP framework (across all critical sectors) were required to be completed by the end of calendar year 2006. Each of those sector-specific plans will include 8 components:

- Sector-specific profile and goals.
- An identification of assets, systems, networks, & functions.
- A sector-wide risk assessment.
- A prioritization of infrastructure.
- Outlines of a plan to develop and implement protective programs.
- Processes to measure progress.
- Research and development strategies.
- A sector management and coordination plan.

FEMA has a recently developed an interactive, home based course to introduce the NIPP at: http://training.fema.gov/EMIWeb/IS/is860.asp

Maritime Infrastructure Recovery Plan
As one of the 8 plans supporting the National Strategy for Maritime Security, the MIRP contains procedures for recovery management and provides mechanisms for national, regional, and local decision-makers to set priorities for redirecting commerce, a primary means of restoring domestic cargo flow. This plan is
employed when the Secretary of Homeland Security declares an actual or threatened Transportation Security Incident (TSI; 33 CFR 101.105) that occurs under, in, on, or adjacent to waters subject to the jurisdiction of the United States, to be an Incident of National Significance (INS), in accordance with the criteria set out in the National Response Plan (NRP) and HSPD-5. Any such TSI declared to be an INS accordingly is referred to as a “national TSI.”

Additionally, the MIRP reflects the organizational constructs detailed in the NRF, as well as the use of Incident Command System (ICS) and Unified Command (UC) procedures. As such, the plan can be used for other similarly disruptive incidents requiring maritime infrastructure recovery management. Following an incident that triggers the implementation of this plan, the MIRP is used to guide the designees of the Secretary of Homeland Security in the decision making process to maintain the nation’s MTS operational capabilities, and if compromised, to restore transportation capabilities.