MTR
MARINE
TERRORISM
RESPONSE

Volume IV
TECHNOLOGY

Homeland Security
ODP
Office for Domestic Preparedness

U.S. Department of Homeland Security
United States Coast Guard

Port of Seattle

PUGET SOUND
MARINE FIREFIGHTING COMMISSION

February 2006

Marine Terrorism Response Plan

Volume IV—Technology

Developed by the

Port of Seattle

With assistance from marine stakeholders in the Port Regions of Seattle/Tacoma, Los Angeles/Long Beach, Houston, New Orleans, Miami/Jacksonville, Philadelphia/Camden, New York/New Jersey

Under grant from

Homeland Security

ODP

Office for Domestic Preparedness

RECORD OF AMENDMENTS

Amendment Number	Date of Amendment	Name of Person Entering Amendment	Signature

TABLE OF CONTENTS

SECTION A – OVERVIEW

1. General

As addressed in Volume I of the MTR Plan, technological tools can substantially aid efforts to mitigate the impacts of a Transportation Security Incident (TSI). The enormous quantities of information required to be collected and disseminated during a response cannot be handled effectively without the use of computers, the Internet, automated tracking devices, and various means of communications including satellite, VHF (very high frequency) or UHF (ultra high frequency), cellular voice communications, and e-mail.

The personnel staffing the Unified Command (UC), including the Operations, Planning, and Logistics sections, the various outlying command posts, and field personnel, should all have access to the latest communications, tracking, and information dissemination tools to assist them in carrying out an effective response.

This Volume of the MTR Plan provides amplifying information on the various technological tools that should be employed to aid emergency response which, for most entities, is evolutionary as funds become available and as the technologies evolve and become easier to obtain and support.

Technological tools (computers and associated hardware and software, tracking devices, and communications) need to be procured, developed, tested, supported, and ready to deploy prior to a response. Additionally, regional charts, maps, aerial photos, and listings on resources all need to be obtained and loaded into an MTR Network data management system in advance.

The components of a comprehensive technological program are graphically depicted below and explained briefly in this section as well as in greater detail in other sections of this Volume of the MTR Plan.

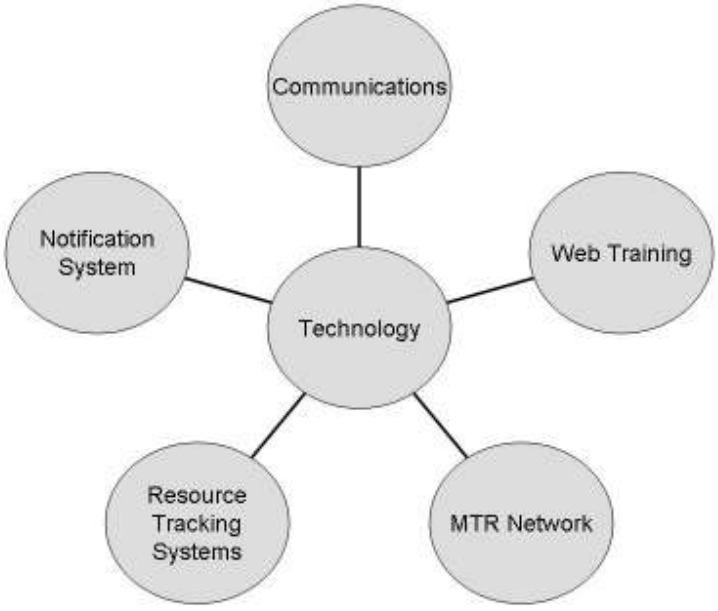


Figure A-1—The various Technological Components of MTR

2. Components of Technology Program

In Figure A-1 above, the components of technology are:

a. Communications

The deficiencies in reliable and effective communications are always a critique item in exercises and real incidents. While typically communications is considered radios and land line phones, through the evolution of technological developments, "communications" is evolving to include satellite, cellular, and voice over IP "phones", wireless PDA devices, e-mail and the internet. The challenges of communicating accurate and timely information to numerous responders and the public have become easier to accomplish through the application of these new emerging technologies.

b. Web Based Training

The challenge of training thousands of responders in the new, increasingly complex issues that need to be addressed in responding to terrorist and other incidents can be more efficiently accomplished by providing some aspects of response training over the internet web.

c. MTR Network

The development, management and support of a MTR Network that uses the internet to share near real time information to various responders is the only practical way of incorporating a large response organization. The onset of ICS has led to the stand up of enormous unified command centers that take considerable time to bring on line and cannot physically accommodate all the involved parties, thus stifling a response. A "virtual command post" that connects various agencies involved in a response through the MTR Network is the only viable way of coordinating a major response operation with asymmetrical incidents. The Coast Guard's Homeport System when matured and fully implemented may serve as the MTR Network or an independent commercial system such as WEB EOC may be preferred by the maritime response community for ease of access and use.

d. Resource Tracking Systems

As a large number of resources (persons, teams, vessels, vehicles, special equipment) are deployed, the opportunity for ineffective utilization develops when decision makers are unsure of the actual locations of those resources. There is technology available to easily track the location of resources through the use of satellite, VHF and cellular phone tracking systems with the information displayed and shared through the MTR Network. The challenge is to ensure the various tracking systems are available and can be displayed on one integrated display system.

e. Notification System

The initial notification of responders and involved parties can best be accomplished through automated call out systems supported by a web information system that can provide amplifying and updated information (i.e., MTR Network). Notification systems can be a component of the MTR Network or an independent system.

3. Technology Team

A Technology Team should be established to manage the Technology Program and to:

- Evaluate and inventory the technological tools presently available in the region.
- Identify additional technological tools that will assist response efforts.
- Select and identify means of procuring technological tools (computers, software, comms, remote sensors, tracking devices, etc.).
- Maintain technology equipment, software, and databases.
- Identify, train, and ensure availability of technicians to set up, maintain, and operate the technological tools, including support of a redundant server system to host the MTR Network when procured.

4. Technological Tools

The following available, and in many cases Commercial-Off-The-Shelf (COTS), technology should be evaluated, procured as appropriate and supported to aid emergency response efforts.

- Automated "notification system" to rapidly disseminate information, verify, and track receipt of information by designated key parties and provide amplifying information via the Web.
- Automated MARSEC increase notification and tracking system that communicates to the marine facilities and vessels the increase of security required to provide increased protection from further attacks and verifying which facilities have taken the actions outlines in their Security Plans.
- Interoperable communications: See Section H of Volume I (Communications) of the MTR Plan.
- Computers and required software to support command posts along with display projectors, LCD (Liquid Crystal Display) panels, WiFi (wireless Internet) systems for command posts, and wireless cell phone or alternative Internet access system to allow connection to the Internet without the need to connect to phone, DSL, cable, or T1 lines.
- A secure, password protected MTR Network that is pre-loaded with ICS forms, maps, charts, aerial photos, facility and vessel information, resource data bases, contact lists, and other information to aid a response.
- Real-time satellite, cell, and/or AIS (VHF-based Automated Identification System) resource tracking systems to track the locations of critical maritime and terrestrial response resources as well as special teams.
- Technology "Ready Kits" with computers, scanners, WiFi, software, digital cameras, projectors, and LCD panels for deployment to command posts.
- Software programs that provide trajectory analysis for chemical, biological, radiological, nuclear releases as well as comprehensive information on various chemicals.

5. Technological Readiness

Volume I of the MTR Plan discusses the readiness indicators that a response community should use to evaluate their level of preparedness and to aid in the identification of readiness gaps that should be addressed. The below graphic shows the readiness gauges, one of which is "Technology".

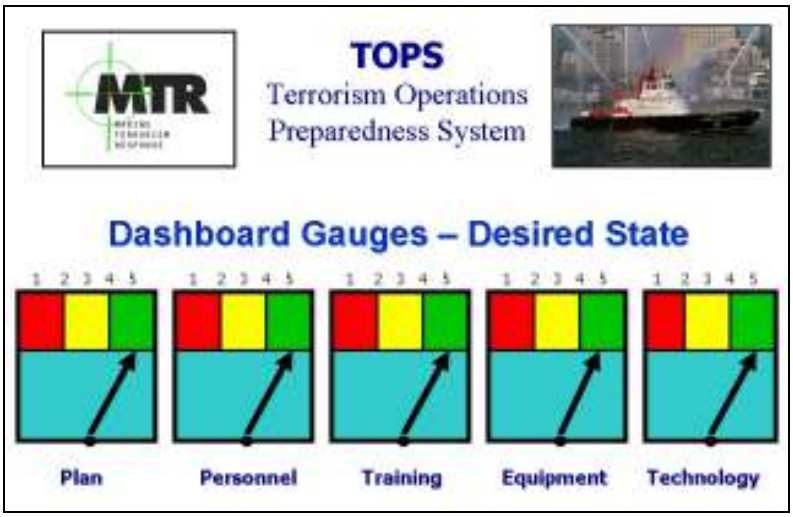


Figure A-2—TOPS Dashboard Gauges

The rating scale from 1 to 5 for all categories represents attainment of the following number of "key readiness factors":

- 1: Red: One or none of the five "Readiness" components has been addressed.
- 2: Red/Yellow: Two of the five components addressed.
- 3: Yellow: Three of the five components addressed.
- 4: Yellow/Green: Four of the five components addressed.
- 5: Green: All of the five components addressed.

Technology Readiness Factors: The factors in determining the level of Technology readiness are:

- A technological "needs assessment" has been conducted based on the technological tools available and identified the additional tools needed to enhance emergency response.
- A technology enhanced "notification system" is in place, updated and operational.
- Interoperable communications systems are procured and available.
- The technological tools available include computers and required software, a secure, password protected MTR Network is available, real time tracking systems procured and available and technology "ready kits" comprised of computers, servers, wireless cards and other items are prepared and ready for deployment to command centers.
- Technical assist teams and documentation teams are trained and available to set up, operate, maintain and service the technological tools.

6. Technology Checklist

The following Technology checklist is also provided in other Sections of the MTR Plan to assist planners determine that the technology components of a response are considered and addressed in the course of carrying out a response.

Technology Checklist

- ☐ Assign person to identify and employ available technology tools that address resource tracking, notifications and web information exchange.
- ☐ Ensure initial information notice prepared for automated notification and update system(s) and provide redundancy through multiple means of broadcast.
- ☐ Ensure process is in place and personnel tasked to provide updated information on the MTR Network, web based information exchange system.
- ☐ Determine persons, agencies and organizations that should have access to the information system(s) and provide passwords and training. Advise authorized users/groups of the system availability and alternate methods of communication.
- ☐ Identify resources where automated tracking is available and ensure that data is incorporated into master tracking system.
- ☐ Identify resources that should be tracked to enhance response efforts and locate and deploy portable transponders.
- ☐ Assign personnel to ensure data such as photos, charts, status reports and contact lists are incorporated into the information exchange system in a timely manner.

SECTION B – HARDWARE AND SOFTWARE

1. Overview

To support the technological demands of an effective MTR, a wide range of hardware and software is required. The hardware/software needed to operate an Automated Secure Resource Tracking System (ASRTS is addressed later in this Plan. Communications are addressed in Volume I and II of the Plan. This section addresses the other hardware and software needed to support an MTR Network and specifically addresses what was developed in support of the national MTR project that is available to other response entities.

2. Components of MTR Technology System

The components of an MTR Technology System are the various software and hardware provided to address the needs of first responders. These will normally include the following:

a. **Deployable "Ready Kits"** with:

- Portable Computers
- Wireless and Ethernet connectivity systems (i.e. cellular, WiFi and hard wire internet access)
- Scanners for transforming documents (ICS forms) and graphics into digital format for entry into the MTR Network
- Digital cameras
- Presentation display (computer display projectors and large plasma display screens)
- Software Systems (MTR Network, Basic internet, word processing, spreadsheet and scanning and photo processing software)

b. MTR Software

The MTR Network was developed as a collection of online applications hosted on a web server under the domain **"**marineresponse.org.**"** The application was built upon Microsoft's Internet Information Server (IIS) and SQL Server 2000 and utilizes third-party components readily available to web developers including a 128-bit SSL server certificate. While each port / jurisdictional area will need to review their unique security requirements, in its basic format, the application is light on system requirements and may be run from any current web server supporting Microsoft's IIS 5 (or greater) and SQL Server 2000 (or greater).

The core MTR network was built as a fully functional model system running two (2) Windows 2000 servers: one running IIS 5 and the other SQL Server 2000. The hardware used to host this system is commensurate with any modern web server and security patches are applied regularly per industry best practices. In addition, these servers are mirrored at two remote locations to avoid loss should one datacenter become unavailable.

For the purpose of supporting MTR Exercises, the Incident Management Shell (Web EOC) was leased from Emergency Services Integrators (ESI) on an application service provider agreement. ESI-911 hosted the application on their servers allowing the MTR project to evaluate the benefits of Web EOC without a significant outlay of capital.

As the MTR network is internet based, clients may vary; however minimum requirements include: Microsoft Office (Word + Excel) used for creating and reading of content; Internet Explorer 5.5 (or greater) with Adobe Acrobat Reader and Autodesk MapGuide Viewer plug-ins installed; and image editing software for the processing of images (optional).

SECTION C – PUBLIC MTR WEB SITE

1. Overview

A public, regionally focused, web accessed component of the MTR Network is a valuable tool for sharing information with the various responders and the commercial and private members of the maritime community that play a vital role in the response to maritime incidents. The efficient deployment of commercial resources (e.g., tugs, barges, oil spill response vessels, chemical response, salvage equipment, personnel, subject matter experts, etc.) can best be accomplished through the timely dissemination of information. The "public site" in this context provides both an open access section and a password protected area that provides a level of security for the more sensitive information provided on the site. The public site is an ancillary web component of MTR that is always operational and used to broker information in contrast to the MTR Network, which normally is activated and accessed when a response is initiated.

2. Components

For the ODP (Office of Domestic Preparedness) funded MTR Project, the public site was developed to inform and educate interested citizens, including the regional response and maritime community, as well as those from the national response and maritime community who were involved in the MTR Project. The site was also used to disseminate MTR Project information. It was hosted under the domain "marineresponse.org" and served also as an entry point to the secure network. It provided limited information about the project in the open access section (e.g., overview and meetings) and more comprehensive and sensitive information in the password protected section (e.g., meeting minutes, member names or MTR project participants, points of contacts, and copies of the various plans to facilitate easy access and downloading as needed).

The MTR public site display shown in the below graphics provides a template for developing a public access site to support the regional response communities.

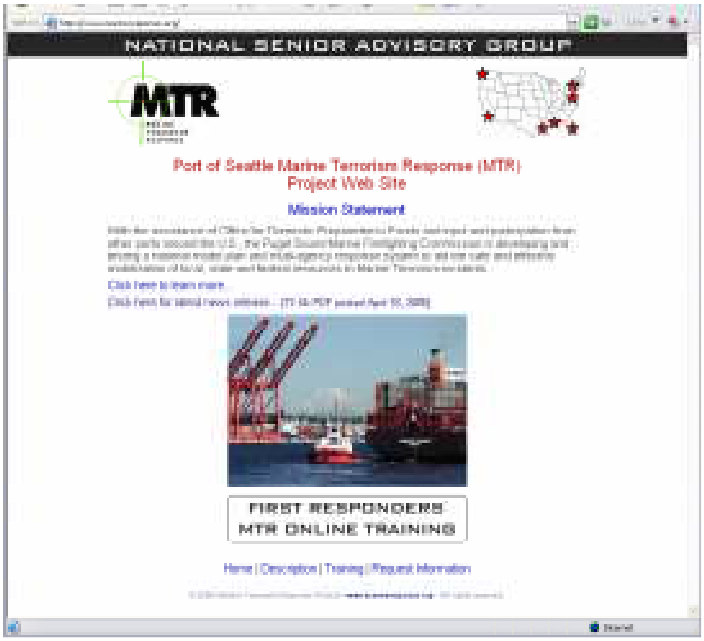


Figure C-1 – Public MTR Site General Information Page

Figure C-2 – Public MTR Site General Information Page

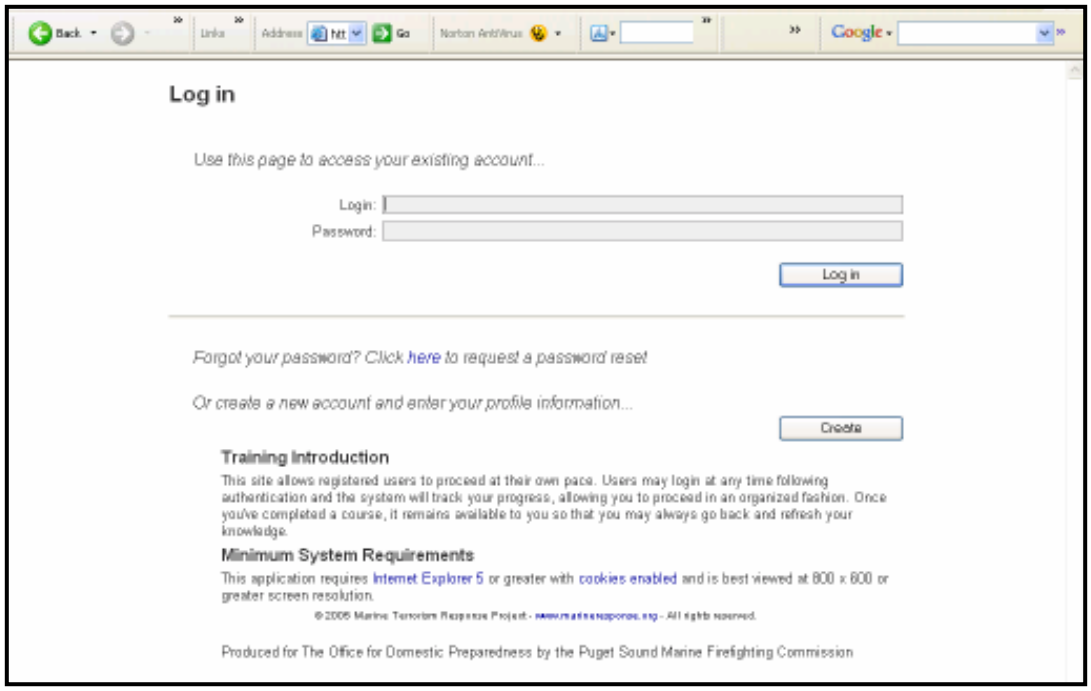


Figure C-3 – Information and Access to Web Based MTR Training

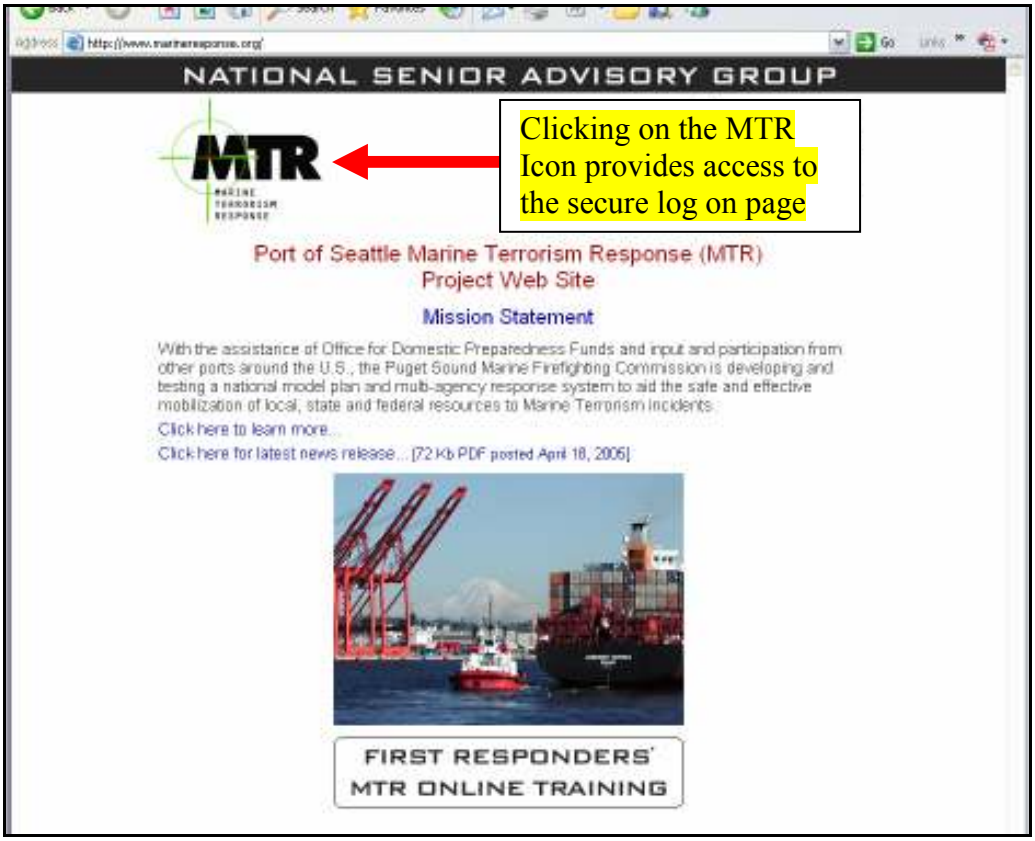


Figure C-4 –Access to Secure Section of Public MTR Web Site

Figure C-5–Access to Secure Section of Public MTR Web Site

Figure C-6–Secure section of regional Public MTR Web Site
Access to MTR Plans and other documents

SECTION D – SECURE NETWORK

1. Overview

The MTR Network was built as an extensible shell with additional applications and third-party solutions linked to it. As a result, port response communities wishing to implement elements of the system may pick and choose those components that meet their unique requirements or implement the entire system.

The MTR Network has the capability to manage users, restricting access to certain areas of the site by individual, group, or global policies. Credentialing of users presents a significant challenge for system administrators. To minimize administrative duties, the MTR Network was designed to allow users to gain access to the system via self-enrollment, response to an invitation to enroll, or be bulk enrolled by a system administrator or department Chief.

Upon creation of a new account, notifications are sent to department and system administrators, credentials are checked and valid users are approved or denied access. Participating agencies may be allowed to self-manage users or be restricted based upon design criteria.

Once credentials have been verified and authenticated, a system administrator grants the user access with varying permissions. Roles and groups determine access to the secure areas of the site. User types are predefined and configurable. Roles range from authenticated guests (lowest permissions) to system administrators. Authenticated guests are allowed access to non-restricted courses in the training site only while system administrators are granted full access to all areas of the site. Intermediate roles allow for the sub-management of the individual components and include:

- Chief / Operations Chief
- Training Officer
- Author
- Publisher
- Records Manager
- Agency Manager
- Report Reader
- Resource Owner
- Resource User
- Incident Command
- Press

It is important the network incorporate Information Security best practices to safeguard proprietary information. In real-world application, the MTR Network may handle critical and sensitive information, which needs to be safeguarded and protected from compromise or unauthorized access. In addition to organic information assurance features found in most networked software environments (encryption, passwords, role-based access), ports / jurisdictional authorities deploying an Incident Management System should strongly consider the use of third-party solutions for secure handling of Electronic Data Interchange (EDI) from remote networks / locations. These systems may utilize Public Key Infrastructure PKI or other credentialing technologies to authenticate users on the network. For a listing of solutions please refer to the VeriSign website www.verisign.com under the heading “Security.”

2. Online Plan Repository

The MTR Network Online Plan Repository is a secure area of the MTR public site used to communicate project status with the Senior Advisory Group and other stakeholders throughout the lifecycle of the project. In addition to providing access to the MTR Plan, progress reports and links to other relevant information was provided through this feature. As noted in the previous section of this Plan, the access to the more sensitive sections of the public MTR site was accessed through a user name and password.

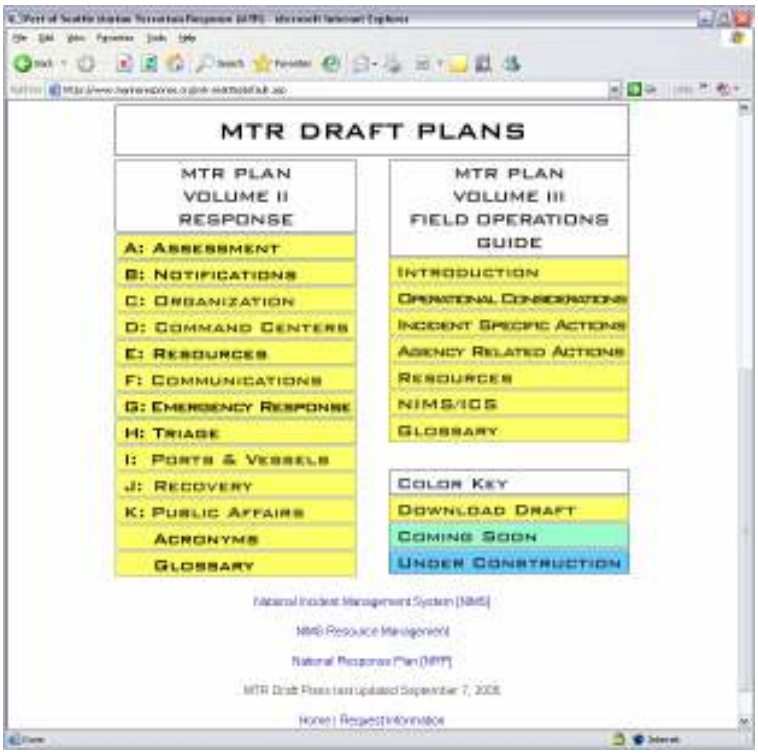


Figure D-1 – MTR Network online plan repository

3. MTR Library

The MTR Library is an online document management system that allows content to be posted via a form-based interface, restricted to specific users or groups. This module is rule-based and may be configured to restrict file types, file size and user permissions. In collaboration mode, the Library module allows authorized users interactive access to original documents enabling collaboration across long distances with informed decisions and fast responses while reducing document handling and distribution costs. When ready to publish, authors / publishers may auto-generate PDF documents for final deployment to general users.

Figure D-2 – MTR Network add document form

4. MTR Learning Management System

As part of the Port of Seattle's MTR grant, the Puget Sound Marine Firefighting Commission (PSMFC) was tasked with developing training programs for first responders. This training was designed to enhance the capabilities and safety of land-based responders who may be called upon to respond to marine fire and life safety incidents, including acts of terrorism. A combination of web-based training (WBT) and instructor-led training (ILT) was chosen to prepare responders for weapons of mass destruction (WMD) and other events that may occur on the nation's waterways. This training also effectively met the competencies outlined in the ODP Emergency Responder Guidelines at the awareness, performance and planning / management levels. The training developed is accessible and flexible enough to meet demands of a response community with a dynamic schedule and is managed / deployed via the MTR Learning Management System (LMS).

The MTR WBT deployed via the LMS follows the recommendations outlined in the ODP Strategy for Blended Learning Instructional Systems Design (ISD) process for course analysis, design, development, implementation and evaluation (ADDIE model) and utilizes the web-based style guide and industry best-practices in development of the WBT delivery application or LMS. This tool provides self-paced, interactive learning and allows the reallocation of critical trainers from the classroom to the hands-on skills teaching area and may be utilized by other Ports. ILT is utilized to complement the MTR WBT and reinforce synthesis and evaluation learning objectives through experiential, hands-on, simulation-based training. Course materials for ILT may be utilized by other ports in their training efforts. In the initial phase of the MTR project, the following courses were developed and deployed via this online system:

- The Marine Environment for First Responders: Awareness
- Marine Terrorism Response (Firefighter): Awareness
- The Marine Environment for First Responders: Performance Defensive
- The Marine Environment for First Responders: Performance Offensive

These courses were designed to supplement live-fire ILT conducted at the Washington State Patrol Fire Training Academy, located at North Bend, Washington and also a planning / management level course designed for those officers who can expect to be the initial Incident Commanders at a marine fire and life safety event. The latter ILT was conducted at the Seattle NOAA facility aboard the NOAA Ship McArthur.

The LMS application is described in greater detail in Section E: Learning Management System.

5. Resource Inventory Management

Working in coordination with the National Incident Management System (NIMS) Integration Center, the MTR Project team has developed a NIMS compliant database and online forms to inventory a sample of the response resources located within the Puget Sound marine area. New resource Category/Kind/Types were developed for marine specific resources/response units using the methodology in use at the NIMS Integration Center. Best practices for mobilizing resources and real-time tracking of resource units were identified.

The resource inventory management system is described in greater detail in Section G.

6. Incident Management Shell

For a Full Scale Exercise, MTR utilized WebEOC by Emergency Services Integrators (ESI) as the Incident Management shell. WebEOC is designed to deliver features for the planning and management of real-time incident and event information and utilizes a control panel that can launch status boards, maps and links to other applications and sites. This application was selected as it is widely utilized throughout Washington State public agencies and was leased on an application service provider basis hosted by ESI. This arrangement allowed the MTR project to evaluate the plan using a system employed by local agencies without investing in a complete system nor exposing State or local jurisdictional systems during the exercise.

Resource Tracking provided by the Maritime Information Service of North America's (MISNA) Automated Secure Vessel Tracking System (ASVTS) was incorporated into the shell. The tracking system used AIS (Automatic Identification System) for vessels so equipped and satellite tracking devices on certain vessels and vehicles. More information regarding this system is provided in Section H of this Volume of the MTR Plan and at www.asvts.org. This application provided real-time tracking of assets that was incorporated in the MTR Network display system.

SECTION E – WEB BASED TRAINING/LEARNING MANAGEMENT SYSTEM

1. Overview

The MTR Learning Management System (training module) utilizes web-based training (WBT) and allows for large numbers or first responders to be trained in a cost effective manner, freeing resources for scenario-based / instructor-led training (ILT). The MTR plan recognizes the need to deliver relevant, fact-based training that is national in scope but also somewhat geographically specific. Recognizing that the driving factor in many public response agencies is funding, the MTR training committee devised a delivery vehicle for training that could be accessed easily by all participating agencies, was easy to maintain and required little training to deploy or use.

2. Components of Learning Management System

The MTR LMS module is built on Microsoft's IIS using Active Server Pages (ASP) to interface with a SQL Server database. The LMS uses a form-based interface and allows for the full management of all aspects of WBT deployment without special tools or knowledge. The following screens demonstrate the LMS in its core deployment.

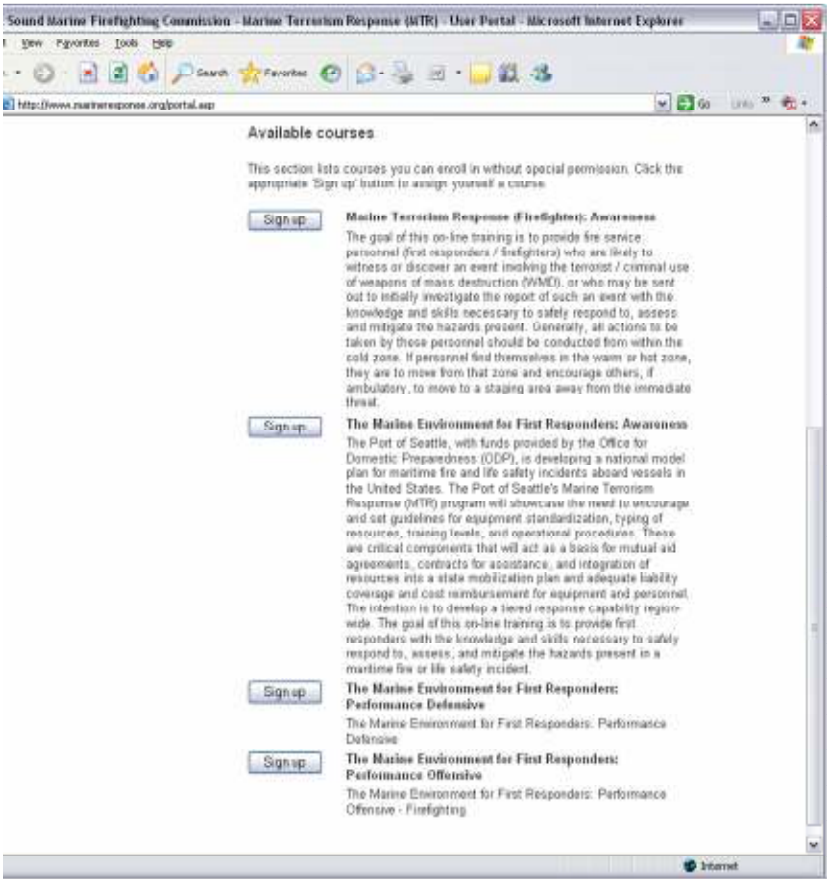


Figure E-1 – MTR LMS self-enrollment page for available courseware

The LMS module, like other MTR modules, is rule-based and may be configured to permit users to self-manage which allows self-assigning, or it may be training officer-driven which requires an invitation to enroll and instructor-determined due dates. In either mode, the authenticated end users are allowed to progress at their own pace and are alerted to progress status, deadlines, or expiring certifications (when enabled).

Figure E-2 – MTR LMS typical course display page

User progress is tracked allowing for them to proceed at their own pace. Quizzes are used to reinforce course content as the user progresses with immediate feedback following the quiz: user score and correct answers (when questions are missed). The application randomizes quiz and exam questions and answers presenting each user with a unique examination. Must-ask questions may be implemented for critical material; however, if implemented, the user must answer these questions correctly to pass the exam. For those who do not pass the first time, the application may be configured to allow users to reset their own exams once before requiring training officer / administrator intervention.

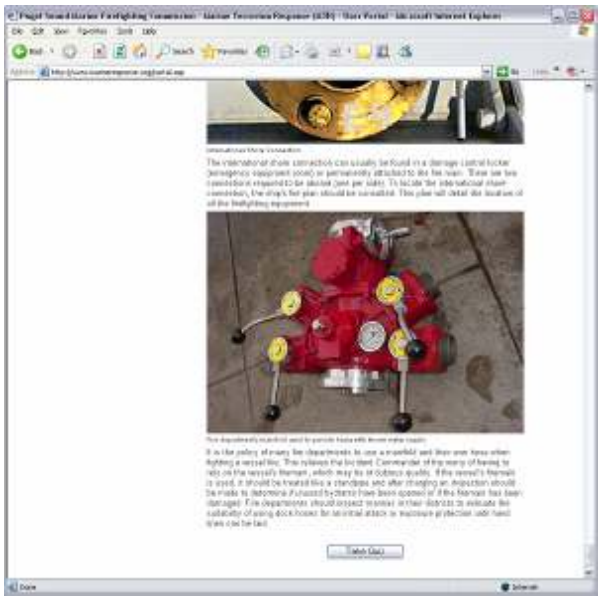


Figure E-3 – MTR LMS end of chapter – take quiz

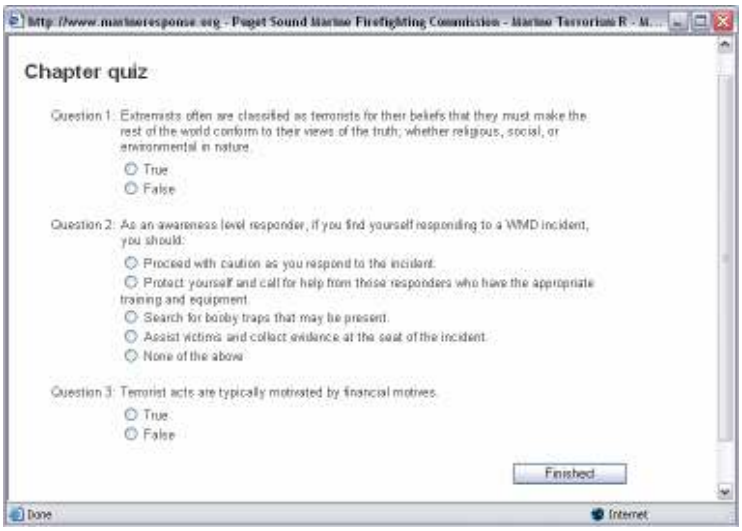


Figure E-4 – MTR LMS typical quiz

Figure E-5 – MTR LMS training alerts, progress, and courses

The application may be configured to allow users to print their own certificates following the successful completion of online courses (optional) or the training officer may print these certificates from the LMS reporting tools, sign and distribute to course participants.

Figure E-6 – MTR LMS user-generated Certificate of Completion

Courses may be assigned using the MTR LMS "Assign Training" function. When enabled, this allows training officers or department Chiefs to assign training to a group of individuals, assign a completion date and a course contact. When utilizing this mode, the system notifies end users via email and alert messages on their welcome screens.

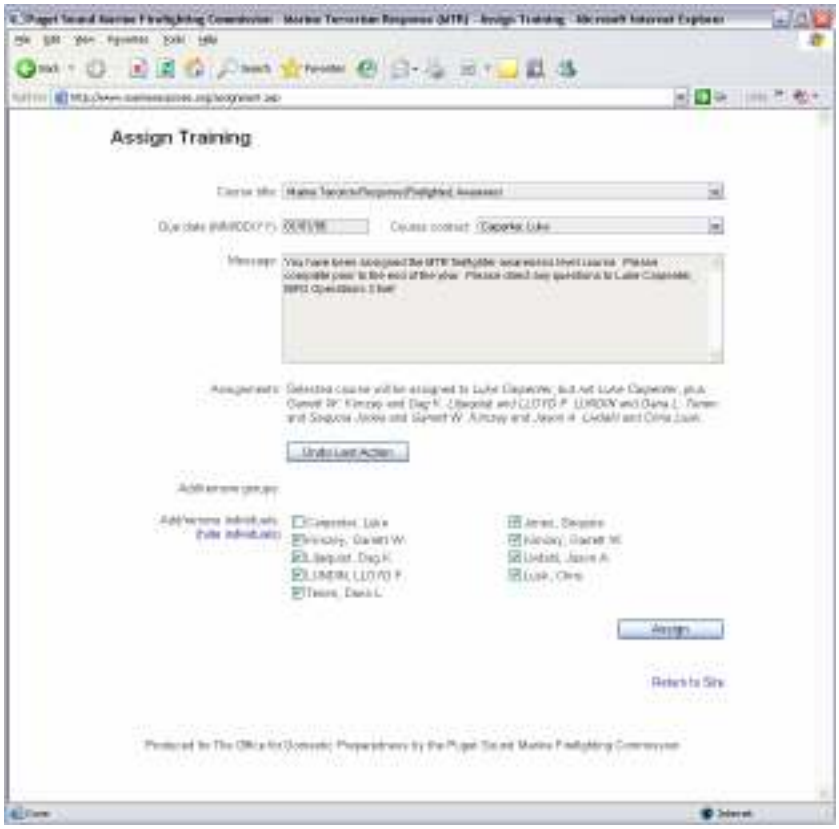


Figure E-7 – MTR LMS training officer's assign training screen

Courses are entered into the LMS using a form-based interface by either authors or publishers. Authors have rights to enter content; however, only publishers may actually publish courses. No special programming skills or applications are required to upload content. Images are automatically resized and optimized for web display and content styles are linked to an agency style sheet for a standard presentation.

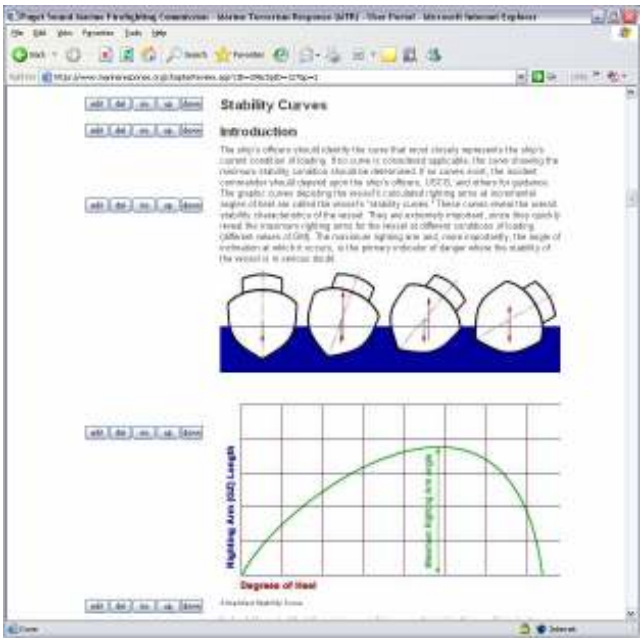


Figure E-8 – MTR Network author courseware screen

Courses are best thought of as containers to hold data: course, chapter, content. Using this system, authors enter the chapter titles and descriptions and then populate the chapters with content. Content is presented to the end user using a pre-determined cascading style sheet (CSS) and the author may alter this presentation during the creation process. Images may be incorporated into the course as content. This process is handled automatically and uploads and resizes the images to fit within the LMS template.

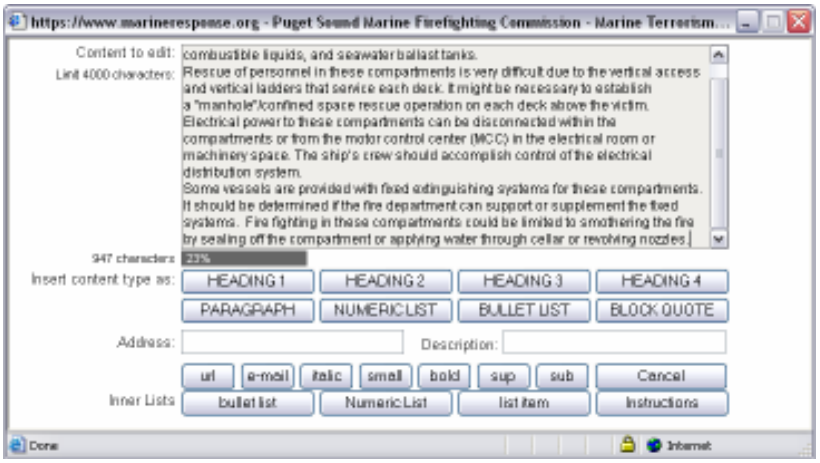


Figure E-9 – MTR LMS edit content courseware screen

Documents are maintained in the MTR Library and may be associated with individual courses or left as general documents. When associated with a course, these may be inserted as supporting materials with a hyperlink, associated with an individual chapter or a course in general. These documents may include manufacturer's literature for the use of specialized equipment, student worksheets, or any other material an author wishes to include.

Quizzes and exams are another type of specialize content. Each quiz / exam question may have one correct and up to 4 alternate (incorrect) answers associated with it. When a user subscribes to a course, a random exam is generated for them, where each chapter pulls a publisher-determined number of questions, including must-ask, randomizing both the order of the questions and display of the answers allowing each user to be presented with a unique examination.

Figure E-10 – MTR LMS exam questions are randomized by the module

When taking an examination, the window is presented full-screen and focus is set to the displaying window. As the intended audience is composed of first responders, examinations may be paused and resumed allowing for incident response mid-exam. If a user fails to log off, the exam is set to pause automatically with current progress recorded following 5 minutes (default) of system inactivity.

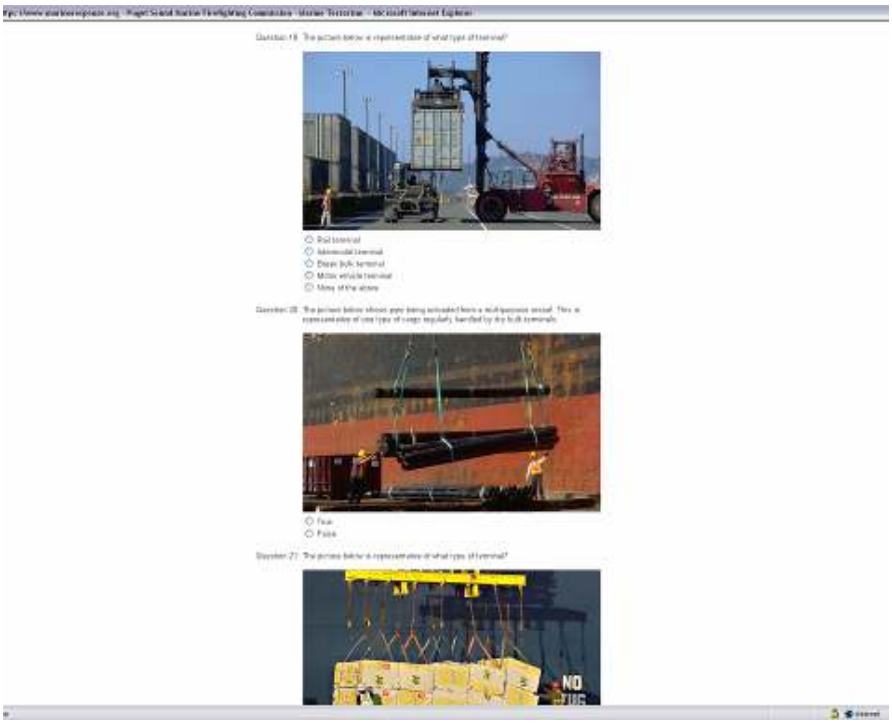


Figure E-11 – MTR LMS exam presented full-screen with randomized questions and answers

The system is configured to allow training officers and supervisors quick access to user progress. Course results are displayed with exam scores and may be expanded to show specific responses to questions missed. In addition, green, yellow and red icons are used for graphical representation. Exams may be reset for those who fail to meet the standard and certificates may be generated for passing students.

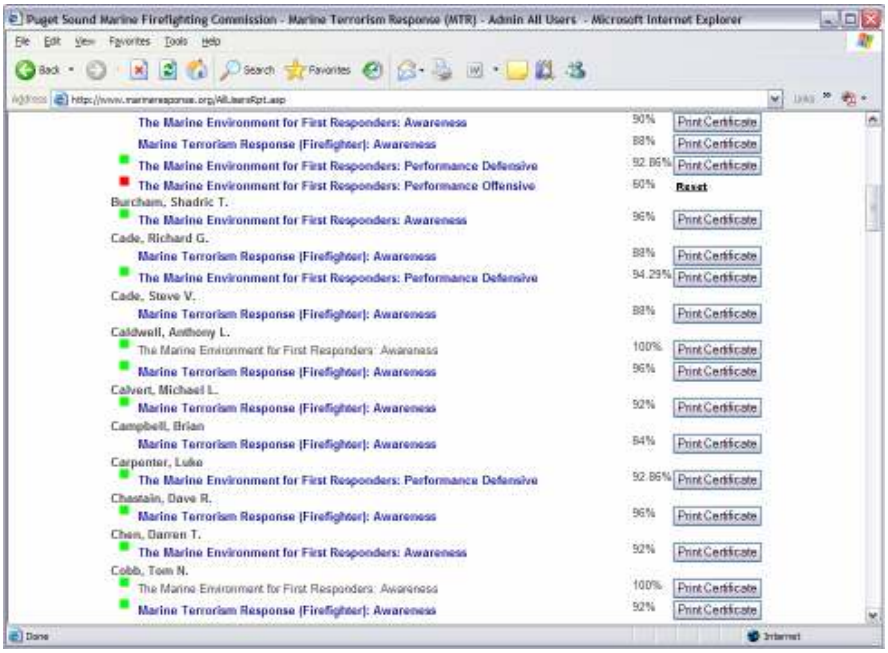


Figure E-12 – MTR LMS typical user's report

SECTION F – NOTIFICATION SYSTEM

1. Overview

The application of internet technology can dramatically improve the efficiency and timeliness of the various notifications that must be made to aid the response to terrorist or other maritime incidents.

The tiering of notifications is addressed in Volumes I and II of the Plan, as well as listings of various points of contact. Additionally, response notifications also need to be addressed expeditiously, such as the attainment of elevated MARSEC levels by ports, facilities and vessels when the Coast Guard directs increase security due to a TSI (Transportation Security Incident).

The initial notification of responders and involved parties can best be accomplished through automated call out systems supported by a web information system that can provide amplifying and updated information (i.e., MTR Network) as well as track the status of notifications made and actions taken, i.e., mobilized equipment, increased MARSEC level, etc. Such automated notification systems can be a component of the MTR Network or an independent system.

2. Components of a Notification System

To accomplish the above, as notification system should include the following capabilities to aid the rapid dissemination of information to a large number of response entities. The information provided in this "Notification Site" should be less comprehensive than the MTR Network, but easier to access.

a. **Notification Data Base:** An updated, comprehensive call out/notification data base with various means of contacting individuals and there alternates needs to be provided. The data base should also prioritize the sequencing of various notifications.

b. **Software**: There are some COTS software solutions such as PIERS, that provide the capability of automatically sending messages and tracking acknowledgments graphically to track the notification process.

c. **Information Site**: An internet accessed web site location should be set up and updated to provide current information on the incident to the parties that are notified. Information at this site should include as appropriate the following:

- Description of incident(s)
- Assistance Requested
- Location of Command Posts
- Contact numbers and e-mail addresses

d. **Ability to Receive Information**: Where the maritime community is tasked with increasing MARSEC levels, the system should have an ability to receive reports back and display the status of notifications including message delivered and action taken.

e. **Displays for the Notification System**: The below graphics provide examples of ways data can be presented to facilitate timely notifications and to monitor progress made in notifications and tracking the attainment of elevated MARSEC levels at facilities.

Figure F-1 – Notification tracking display

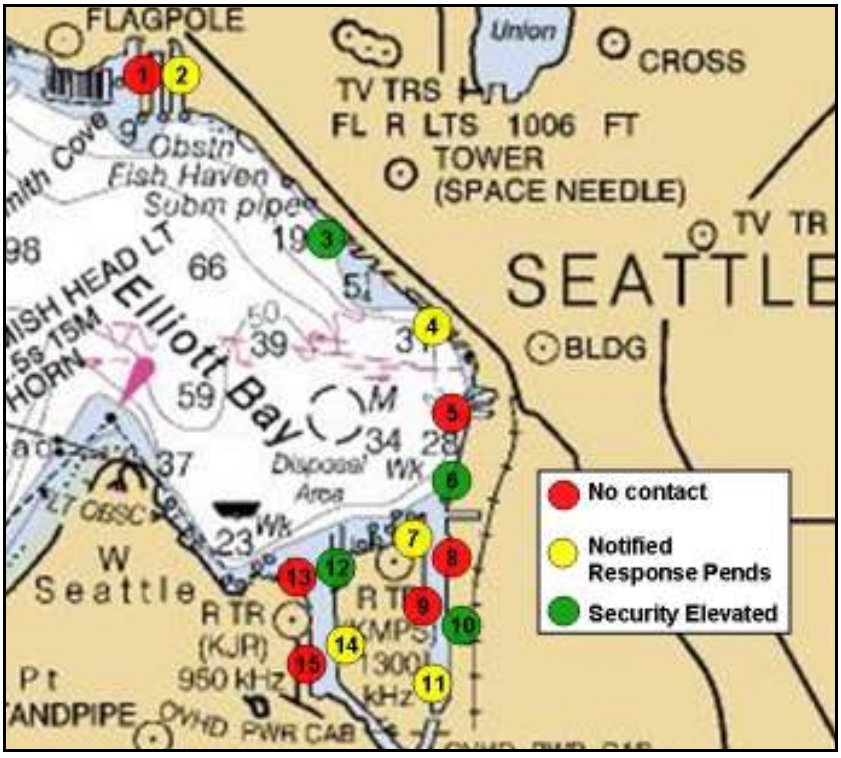


Figure F-2 – MARSEC attainment tracking display

SECTION G – RESOURCE INVENTORY MANAGEMENT

1. Overview

Working in coordination with the NIMS Integration Center, the MTR Project team developed a NIMS compliant database and online forms to inventory a sample of the response resources located within the Puget Sound marine area. New resource Category/Kind/Types were developed for marine specific resources/response units using the methodology in use at the NIMS Integration Center. Technology applications for mobilizing resources and real-time tracking of resource units were also identified and tested. A comprehensive, accurate, updated and accessible listing of resources is critical to carrying out an effective response and can best be achieved through the use of an internet based data base and entry system. The following screens demonstrate the basic interface for the Resource Inventory Management.

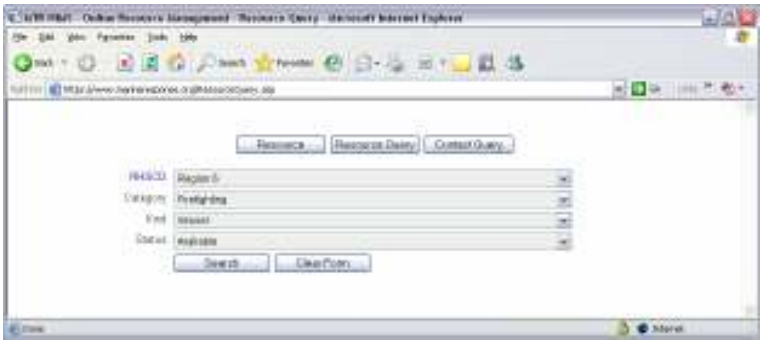


Figure G-1 – MTR Network resource query screen

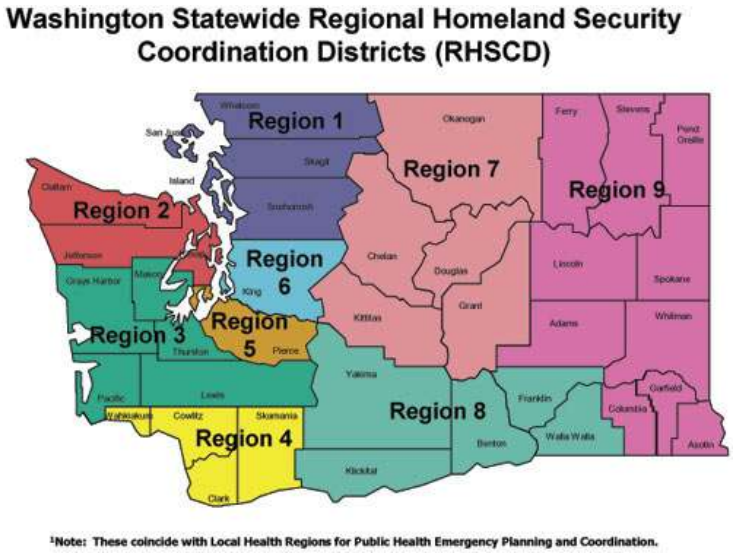


Figure G-2 – Washington State Regional Homeland Security Coordination District locations

The system is configured to allow resources to be associated with the Washington Statewide Regional Homeland Security Coordination Districts, agency or resource owner. This allows for mutual aid agreements to be established pre-incident and for Incident Commanders to gain a quick overview of assets available. The application is not designed

to track consumables; however EOC Logistics staff may access a list of contacts for procuring these materials. Like other MTR Network modules, resource owners may subscribe by invitation or self-enrollment. Once authenticated, resource owners manage their contact information and certify that their resources meet the NIMS Integration Center's minimum standards by category, kind and type. To encourage use of the system by commercial resource owners, these individuals are limited to access information associated with their assets solely and may not use the system to gain access to competitors' data.

Figure G-3 – MTR Network resource result screen – individual record

Figure G-4 – MTR Network edit resource record screen

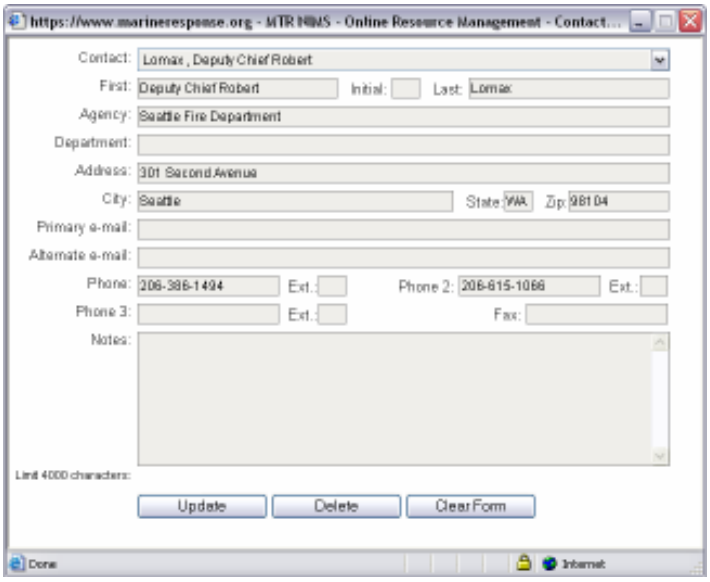


Figure G-5 – MTR Network edit contact record screen

As all resources are catalogued in a SQL database, Incident Commanders are able to get a clear picture of available resources immediately. While beyond the scope of this grant, the application may be integrated with Microsoft's Share Point Server for requesting resources by EOC personnel and then providing multiple communication channels to resource owners to gain access to available assets.

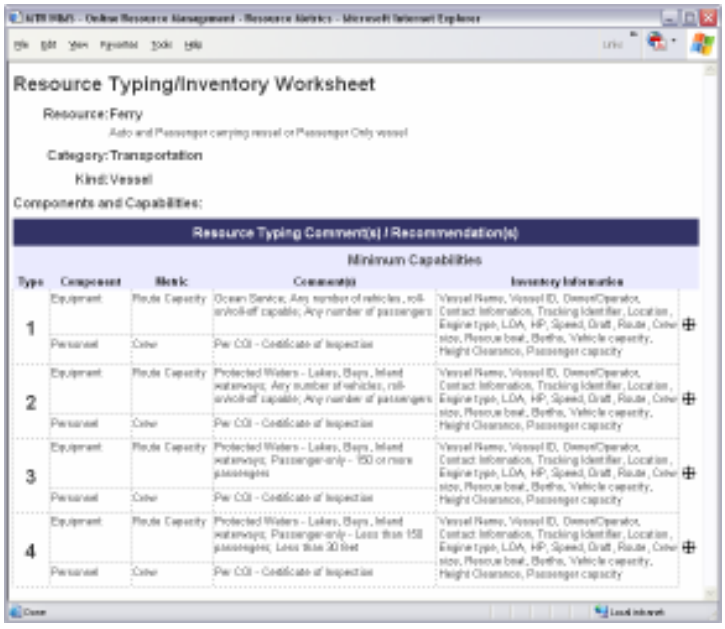


Figure G-6 – MTR Network Manage Resource Metrics

MTR has worked closely with the NIMS Integration Center to develop a tool based upon their current directives. New resources are added to the database using a form-based interface based upon the NIMS Integration model forms. Metrics are then added to define each type of resource.

SECTION H – RESOURCE TRACKING

1. Overview

Tracking the locations of major response equipment and resources can aid response efforts by ensuring the resources are proceeding to the reporting location, and best positioned to maximize the effectiveness in mitigating the impacts of a security incident(s) or other disaster(s).

There are several tracking systems coming on-line that may be used to track response vessels, vehicles and special teams. These include:

- Satellite transponders (universal coverage, limited blind spots, no shore infrastructure other than land earth station)
- AIS (Automatic Identification System) used by many commercial vessels. Requires shore stations.
- Cellular tracking phones and systems
- Other local systems

The challenge is bringing the various data streams provided by different tracking systems to one Situational Awareness display that can be shared with the response personnel at the various command posts and other locations through the internet.

The MTR Project field tested the Maritime Information Service of North America's (MISNA) Automated Secure Vessel Tracking System (ASVTS) that employs a secure, 128 bit encryption system to disseminate the data and display it on a Graphical User Interface (GUI).

2. Components of Automated Secure Resource Tracking System

The MTR project modified the tracking systems name to ASRTS (Automated Secure Resource Tracking System) to better represent the systems capabilities and functions.

The components of the system tested were:

- An open architecture data and software processing system that can process various satellite, cellular and AIS. The software system used is called SARS or Secure Asset Reporting System. More information can be obtained at www.sarsinc.com or by contacting the Maritime Information Services www.asvts.org.
- Globalstar Axxon Tracker simplex satellite tracking modems that can be programmed to provide position reports from every 15 minutes to longer periods The units are small, full self contained (battery, antenna, gps and transmitter) in a weather proof box that may be taped to the asset that needs to be tracked. The satellite comms cost be position report is approximately 10 cents.
- AIS transponders on commercial vessels. These were already installed on the vessels. Note: the units are costly and presently require some technical expertise to install. Class B transponders are expected to be available in 2006 that are inexpensive, battery operated and don't require installation. There are no fees for transmissions as they are over a VHF system, however, a receiving station must be in line of sight and tied into an internet system.

The below photos show a Globalstar satellite tracking device next to a cup of coffee to provide a size comparison, a display of the area transited by the barge on which the device was installed, and an ASRTS chart display of the vessel it tracked. These devices cost approximately $600 each.

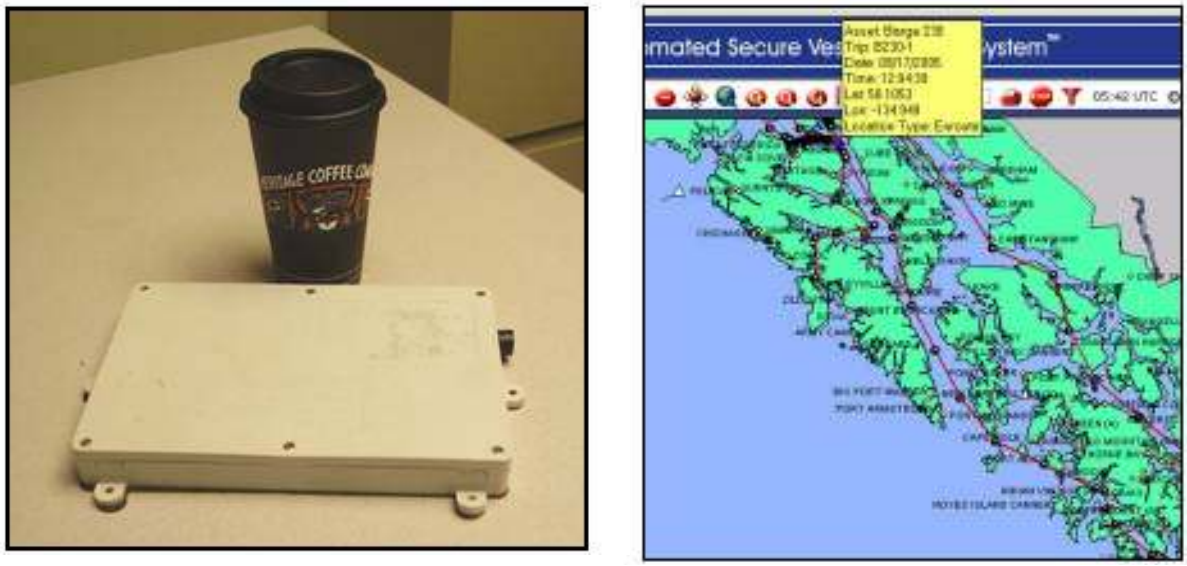


Figure H-1 – Tracking display and self contained satellite transponder

3. Tracking Displays

The following graphics show various resource tracking displays:

Figure H-2 – Vessels tracked with ASRTS

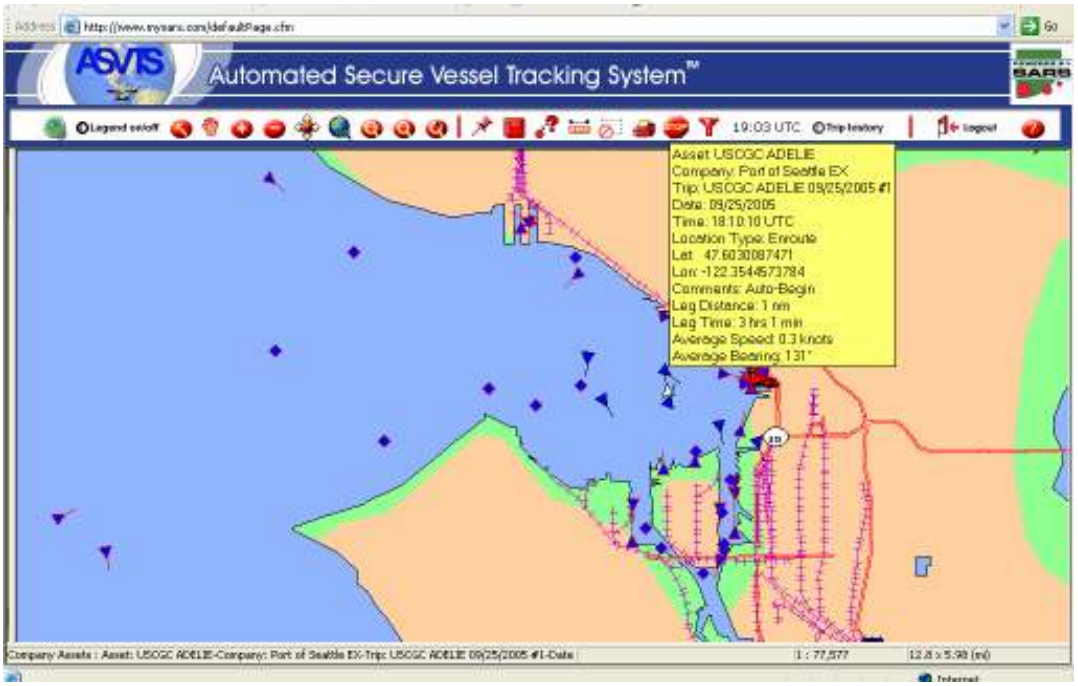


Figure H-3 – Display of various vessels involved in exercise

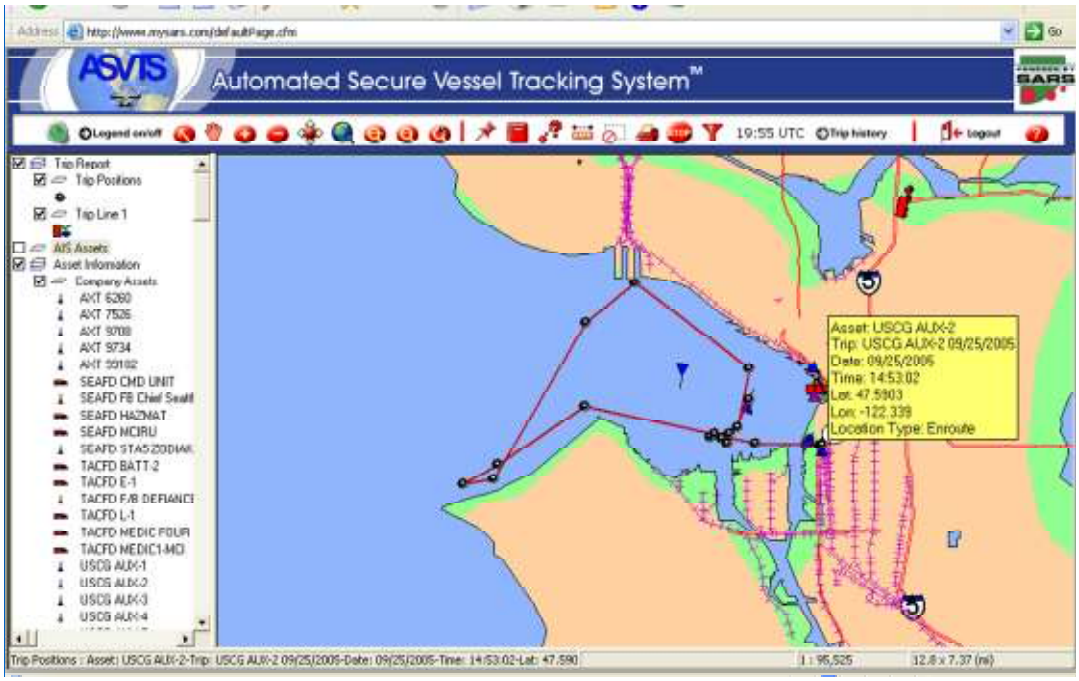


Figure H-4 – Trackline of Coast Guard patrol vessel

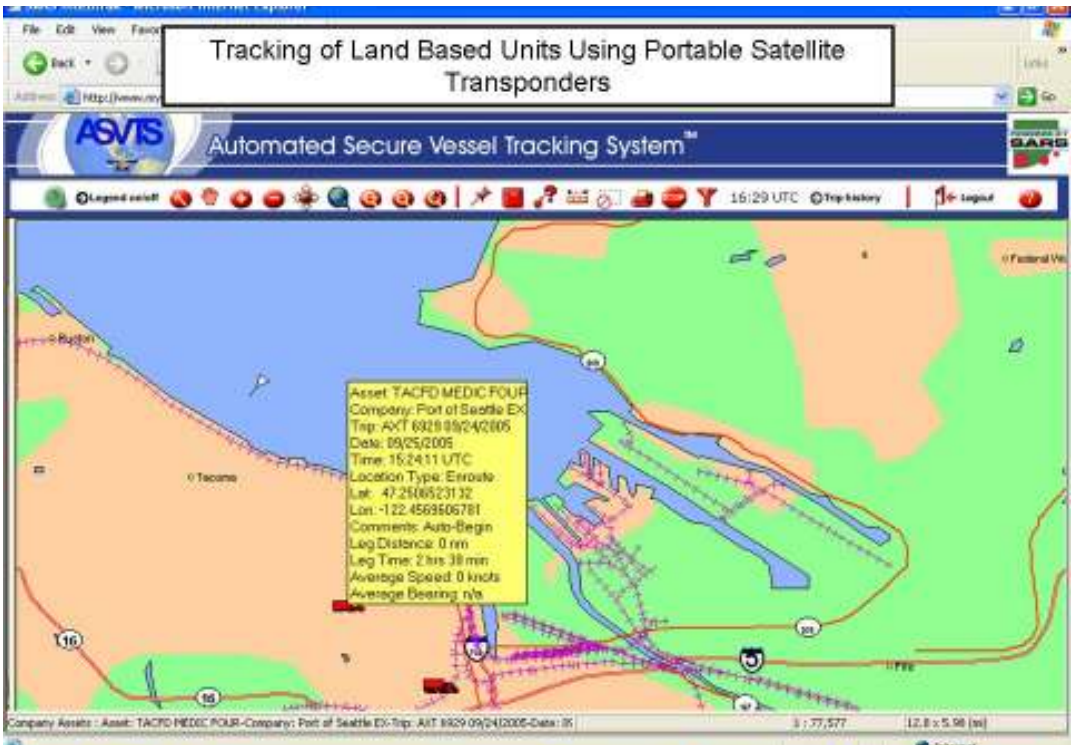


Figure H-5 – Tracking of land response resources

SECTION I – MTR NETWORK

1. Overview

Large scale, asymmetrical responses require the passing of large amounts of information to operations centers and field personnel and other command centers to facilitate coordinated and effective responses that mitigate impacts. ICS organizations are additionally so complex for large incidents that it is difficult to rapidly provide sufficiently large and well equipped command posts to accommodate all participants. Accordingly, the application of web and internet technology can allow response planners, coordinators and staff to participate from various locations and remain connected and having the requisite "situational awareness" to make informed decisions.

In real-world application, the MTR Network may handle critical and sensitive information, which needs to be safeguarded and protected from compromise or unauthorized access. In addition to organic information assurance features found in most networked software environments (encryption, passwords, role-based access) ports / jurisdictional authorities deploying an Incident Management System should strongly consider the use of third-party solutions for secure handling of Electronic Data Interchange (EDI) from remote networks / locations. These systems may utilize Public Key Infrastructure PKI or other credentialing technologies to authenticate users on the network. For a listing of solutions please refer to the VeriSign website www.verisign.com under the heading "Security."

The MTR project uses the commercially available WEB EOC program to support the MTR Network that was tested and demonstrated during table top and full scale exercises.

2. Components of MTR Network

The MTR Network should provide the following capabilities:

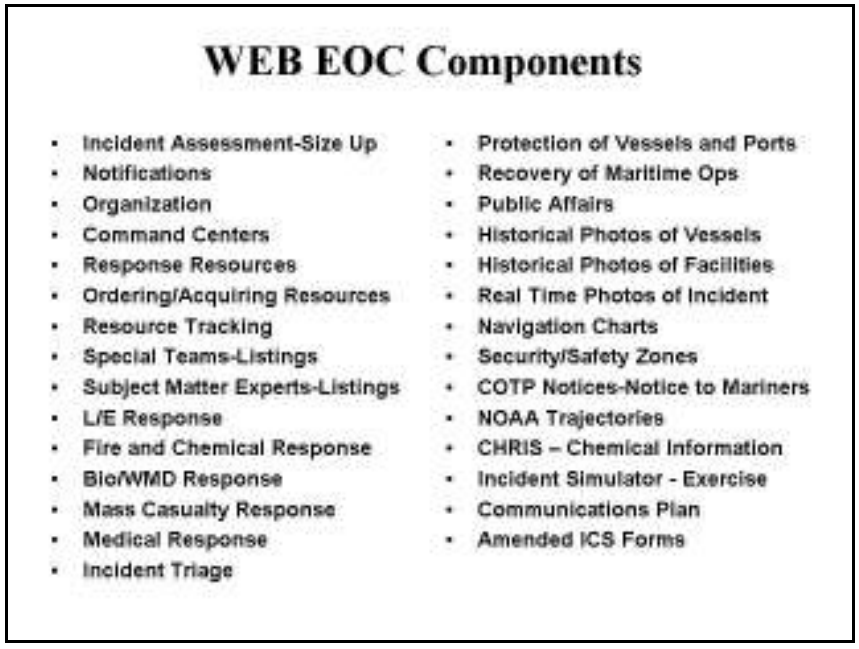
- Ability to incorporate, display and monitor input from multiple, geographically distributed locations in real time
- Provide current information on points of contact and response resources
- Display charts and photographs
- Display, allow entry and post ICS forms
- Display, allow entry, and post information on resources dispatched
- Incorporate real time resource tracking information
- Provide complete lifecycle support services
- Provide Standard Operating Procedures (SOP's) for end user reference and implementation
- Integrate SOP's (Standard Operating Plans), Response Plans, and Check Lists into the emergency management environment
- Incorporate Information Security best practices to safeguard proprietary organizational information.

For the Full Scale Exercise, MTR utilized WebEOC by Emergency Services Integrators (ESI) as the Incident Management shell. WebEOC is designed to deliver features for the planning and management of real-time incident and event information and utilizes a control panel that can launch status boards, maps and links to other applications and sites. This application was selected as it is widely utilized throughout Washington State public agencies

and was leased on an application service provider basis hosted by ESI. This arrangement allowed the MTR project to evaluate the plan using a system employed by local agencies without investing in a complete system or exposing State or local jurisdictional systems during the exercise. While WebEOC met the needs of the MTR project, other IM shells may be utilized with varying success and must be evaluated by the jurisdictional requirements. Other internet-based IM shells include:

- ETeam by NC4 Public Sector, LLC www.eteam.com
- Blue Emergency Management (Blue EM) by Blue292 www.blue292.com
- L-3 CRISIS by MPRI Ship Analytics www.shipanalytics.com
- OpsCenter by Alert Technologies Corp www.alerttech.com
- Ramsafe by Ramsafe Technologies www.ramsafe.com
- SoftRisk SQL by SoftRisk Techologies, Inc. www.softrisk.com

As a follow-on extension to this grant, MTR has plans for developing a basic IMS for distribution to other ports / jurisdictions. This system, Incident Management Shell, will be extensible and deployed in a unique configuration for each distribution to limit vulnerabilities introduced by highly-configurable systems designed to meet multiple needs.



3. ICS Forms, Charts and other Data

The MTR Network should have the capability to load and display modifiable charts, ICS forms, and photographs, diagrams, documents as well as link to other web sites that provide relevant information. The following graphics provide examples of how the information can be accessed and displayed in the MTR Network.

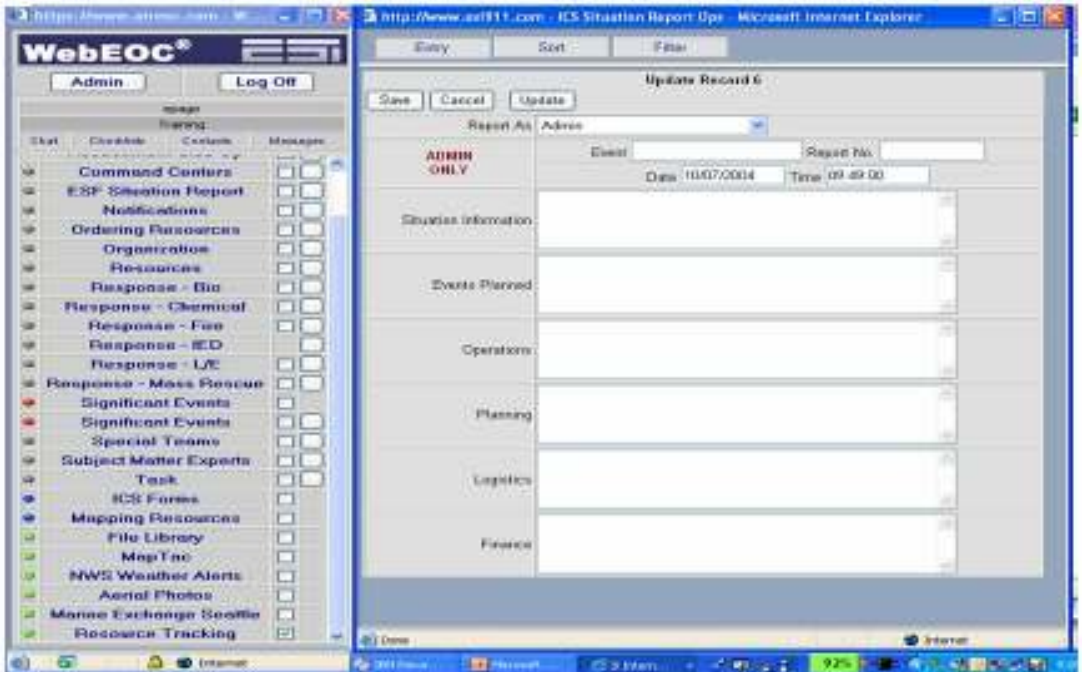


Figure I-1 – ICS Situation Report, Operations and Control Panel

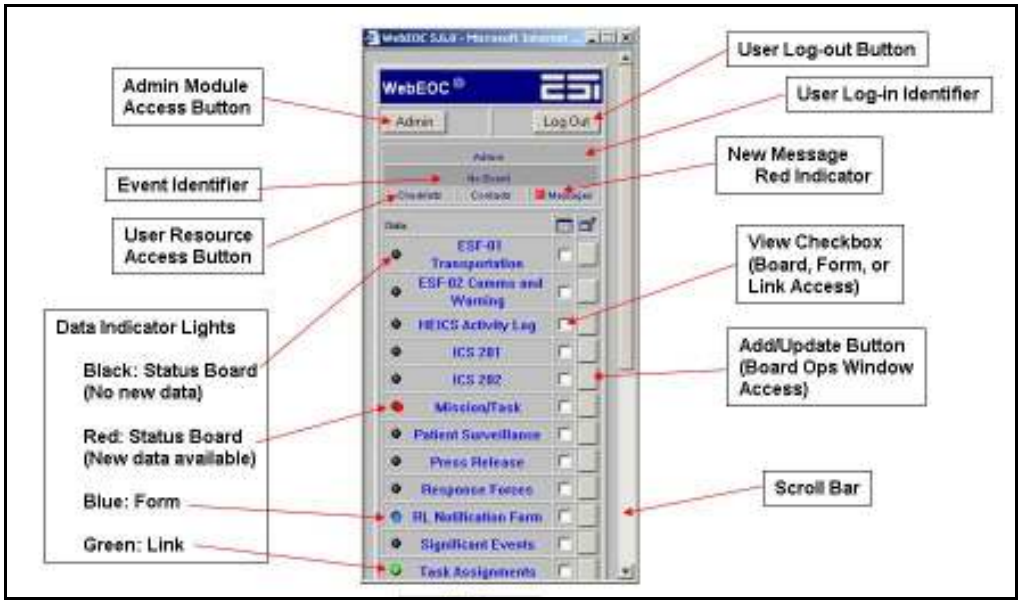


Figure I-2 – Control Panel

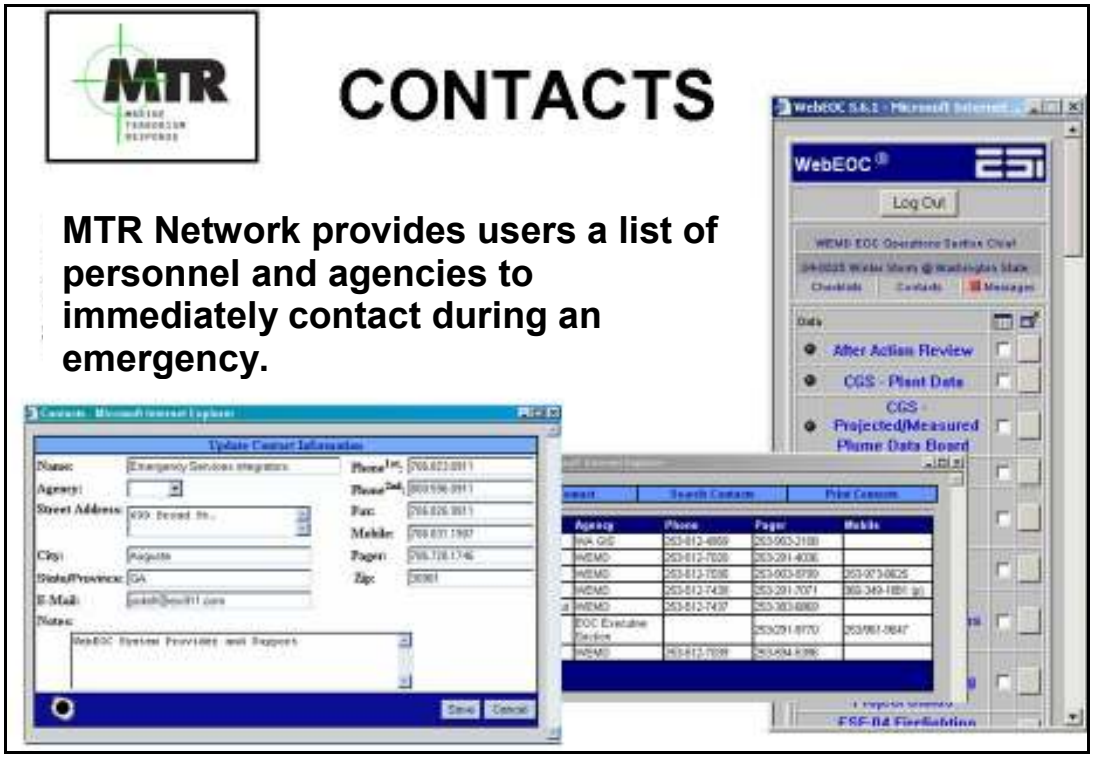


Figure I-3 – Contact listings

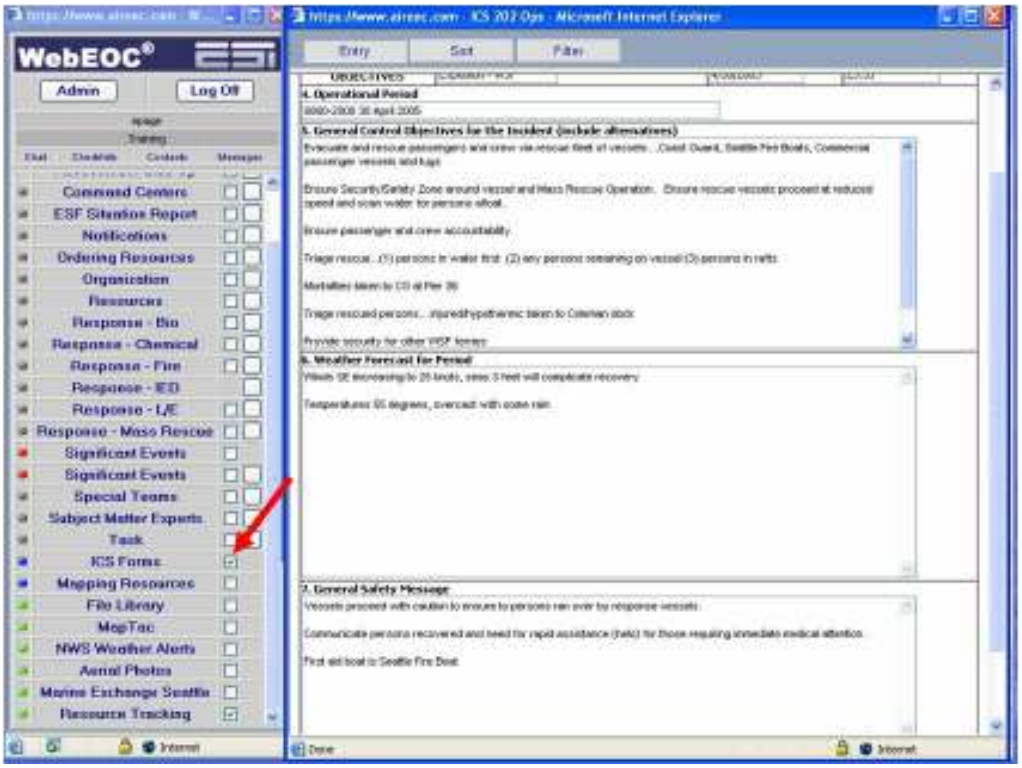


Figure I-4 – ICS Incident Action Plan

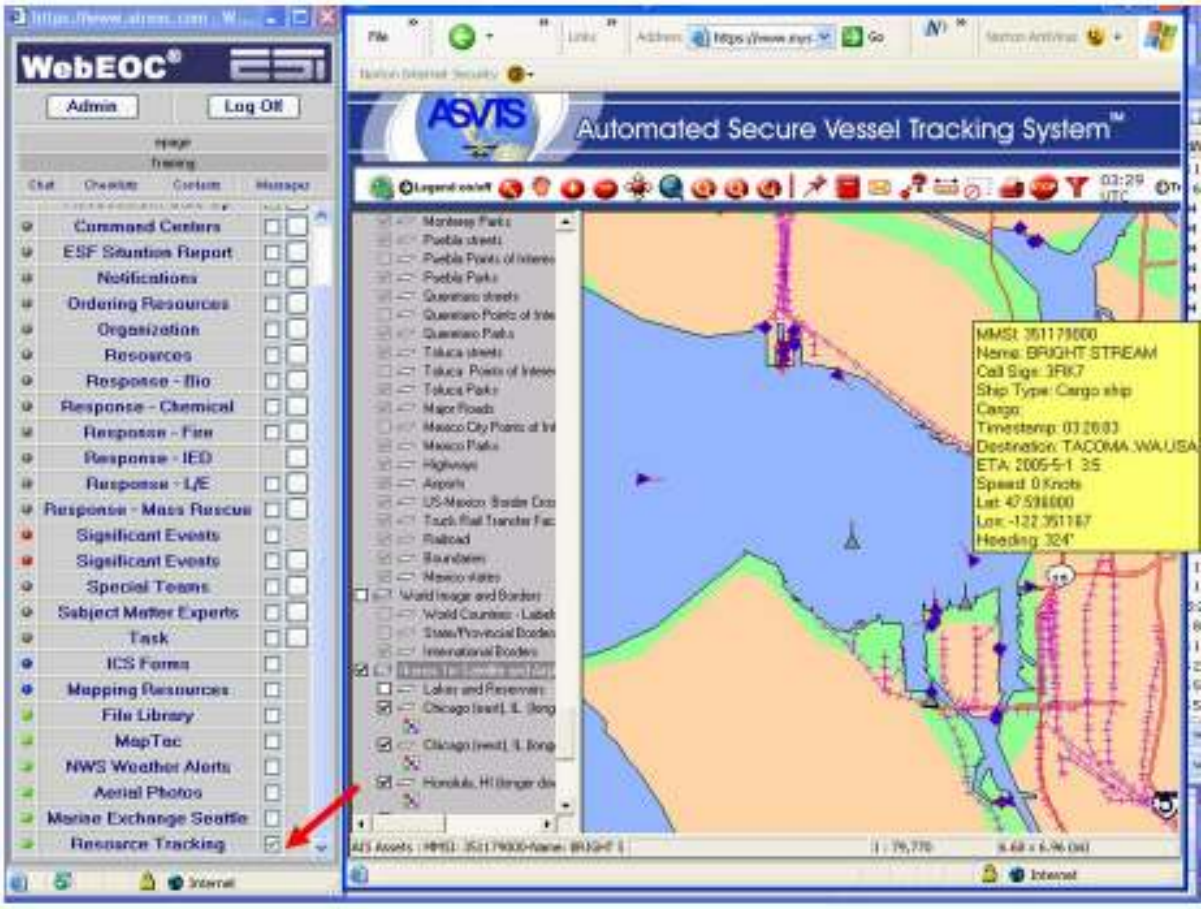


Figure I-5 – Resource Tracking Display on MTR Network

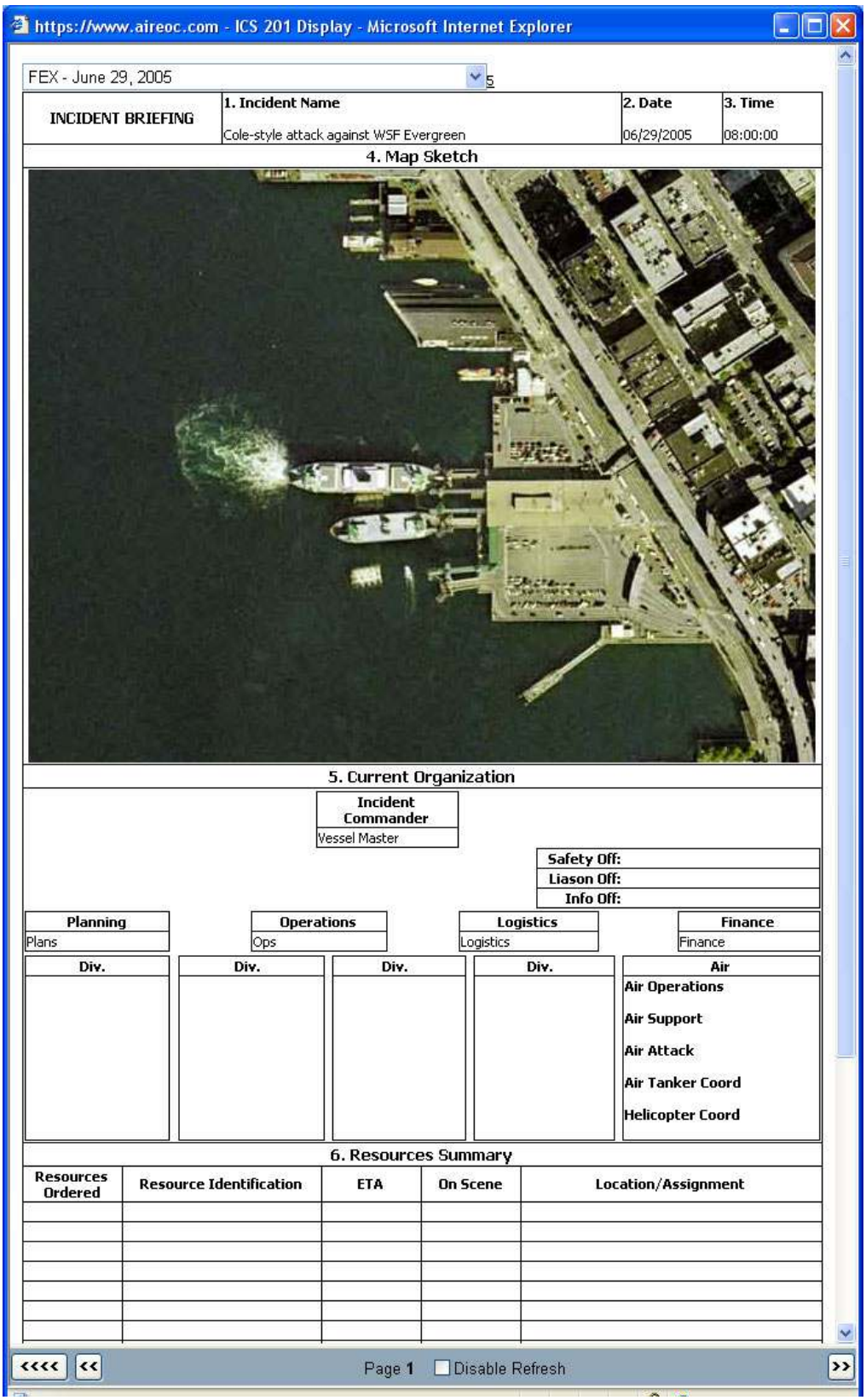


Figure I-6 – ICS Form integrated with photograph