



**NATIONAL INFRASTRUCTURE INSTITUTE
CENTER FOR INFRASTRUCTURE EXPERTISE (NI²CIE)**

**CANADA – UNITED STATES CARGO SECURITY PROJECT
OPERATION SAFE COMMERCE - NORTHEAST**

Intelligent Container Interoperability

2005

NOTE

The NI² Center for Infrastructure Expertise is a not-for-profit applied research organization dedicated to improving the management and protection of the built infrastructure in the United States. The Center is funded through a grant from the U.S. Department of Commerce National Institute of Standards and Technology (NIST). This survey is funded through a grant from Small Business Administration.

Executive Summary

The National Infrastructure Institute Center for Infrastructure Expertise's (NI² CIE) recent project explored public safety benefits when commercial off the shelf (COTS) geo-position tracking technology was applied to cargo container transportation. NI² CIE applied COTS geo-position tracking technology to simulated over-road transports and their containerized cargoes. During live field tests instrumented container geo-position data was linked with different types of first responder networks and emergency notification systems. NI² CIE demonstrated that containers instrumented with geo-position technology improved emergency responders' reaction time. NI² CIE's test results also illustrated how geo-position tracking technology enabled first responders' capability to prevent cargo containers from being used as terrorist weapons. However, these tests also showed that geo-position tracking technology is not a container industry standard, nor are there pre-established interoperability protocols effectively linking commercial transportation operators with first responders. Therefore, NI² CIE supports additional intelligent container development, including possible container and commercial trucking standards that require geo-position tracking systems. NI²-CIE also recommends improved interoperability between the trucking industry and first responders.

Table of Contents

1. Introduction and Background	7
2. Objectives	7
3. Methodology and Test Details	7
4. Emergency Notifications Systems Analysis and Research	8
4.1. RISS/ATIX	8
4.2. National Response Center	9
4.3. Emergency 911	11
4.4. Enhanced 911	11
4.5. States' Anti Terrorism Hotlines	12
5. Additional Research	12
6. Recommendations	13

List of Appendices

Appendix 1.....	14
Appendix 2.....	18
Appendix 3.....	21
Appendix 4.....	24
Appendix 5.....	28

List of Key Terms

ATIX	Automated Trusted Information Exchange
COTS	Commercial Off the Shelf
DHS	Department of Homeland Security
EOP	Emergency Operation Plan
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
GPS	Global Positioning System
HSPD	Homeland Security Presidential Directive
ICS	Incident Command Systems
MOU	Memorandum of Understanding
NI ² CIE	National Infrastructure Institute Center for Infrastructure Expertise
NIMS	National Incident Management System
NRC	National Response Center
NRP	National Response Plan
RISS	Regional Information Sharing Systems
UASI	Urban Area Security Initiative

1. Introduction and Background

NI² CIE tested existing local, state and federal emergency notification networks to identify the most effective method to link first responder agencies with instrumented cargo container geo-position data. NI² CIE performed comparative analysis on the capability of the following U.S. federal, state and local emergency notification and information collection systems to assimilate instrumented container data and quickly alert first responders about a geo-position anomaly:

- (1) Regional Information Sharing Systems/Automated Trusted Information Exchange (RISS/ATIX);
- (2) The National Response Center;
- (3) Emergency 911;
- (4) Enhanced 911, and;
- (5) State Anti-Terrorism Phone Numbers.

2. Objectives

(a) Confirm how law enforcement, fire service and hazardous material emergency response agencies are to be alerted when an intermodal container has been hijacked for the purpose of executing a terrorist attack.

(b) Evaluate the most rapid and effective emergency notification system to mobilize local, state and federal emergency responders to prevent and/or preempt a potential terrorist attack.

3. Methodology, Tests and Scenario Details

1. Identify potential partners from the domestic over-road cargo container transportation industry and emergency responder agencies.
2. Select at least one commercially available off the shelf (COTS) intermodal cargo container tracking device, see **Appendix 1**.

3. Apply COTS to an intermodal cargo container or a transport carrier, and transmit the container's and/or truck's geo-position to a secure web interface where the information can be analyzed by a Logistics Manager.
4. Determine whether or not emergency responders should receive an alert directly from the COTS device or from an individual responsible for analyzing data.
5. Evaluate pre-existing communication systems for emergency notification and response.

NI² CIE conducted two live tests. The scenario for these tests involved a simulated hijacked transport truck and container, whose hazardous material cargo could be easily converted into a potential terrorist weapon. The scenario included the transport changing directions, violating its geo-fence¹ and presenting a potential terrorist threat to the city of Boston, MA. The simulated transport was outfitted with COTS geo-position tracking technology and transmitted in real time all geo-position data to a secure web site. During the scenario, the Logistics Manager would have to monitor the secure web site for geo-fence violations. If the Logistics Manager was to detect a geo-fence violation, he would attempt to contact the transport driver by cellular phone. If Logistics Manager was unable to contact the driver he would become suspicious of a potential terrorist threat. According to company protocol, the Logistics Manager would have to notify authorities for the purpose of initiating an emergency response. To view the complete scenario, refer to **Appendix 2**.

The scenario included having the transport truck and container cross state lines, involving several jurisdictions.

¹ A feature that stores geographic boundary information on the geo-tracking device. When a stored boundary is violated, the COTS will notify the user by having an alarm sent to their email, facsimile, phone, or pager. A geo-fence may also be plotted on an electronic map and when a container violates the geo-fence boundary an alarm is sent alerting the user about the incident.

4. Emergency Notification Systems Analysis and Research

NI² CIE identified five separate emergency notification systems. Because of concern about false alarms when using “Emergency 911” or “Enhanced 911” neither was used during the real-time tests. Real-time tests were conducted using RISS/ATIX and the National Response Center. NI² CIE’s research of the limitations and capabilities of Emergency 911 and Enhanced 911 involved a site visit to the Enhanced 911 control center and a detailed interview with an Enhanced 911 watch supervisor. Additional interviews were also conducted with various New England States’ Anti-Terrorism Hotlines.

4.1. RISS/ATIX: During the initial test the Logistics Manager used the RISS/ATIX secure email platform to notify emergency responders about the container emergency. Officials responsible for critical infrastructure, law enforcement, fire services, emergency management, public health, environmental protection, and utility services routinely access RISS/ATIX. Governmental and non-governmental organizations responsible for all hazards-incidents are included on the RISS/ATIX platform, where a secure means to disseminate national security information is provided. RISS/ATIX is a U.S. Department of Justice single-source communications network, where criminal intelligence information is shared with various U.S. and Canadian emergency responder agencies.

The RISS/ATIX secure email system proved to be a valuable information exchange tool for notifying emergency responders about a potential container-based terrorist attack. Emergency responder organizations were able to acknowledge receipt of the original message and confirmed that they were taking appropriate action. The Logistics Manager sent an email from the secure web-site and attached copies of the in-container geo-position data (latitude, longitude), commercial transport’s over-road speed and frequency of geo-position data transmissions. The RISS/ATIX link demonstrated potential as a tool to enable a quick emergency response during a real hi-jacking.

Presently, RISS/ATIX is not designed for emergent notifications. RISS/ATIX was useful for assimilating and sharing incident data with local, state and federal emergency

responders. However, because RISS/ATIX is currently a passive notification system requiring emergency responders to actively monitor the RISS/ATIX web-based network, there is the distinct possibility that emergency notifications would not be received in a timely manner. In order to consider using RISS/ATIX as the platform linking commercial transport operators and instrumented container owners with emergency responders, RISS/ATIX would have to be re-designed to include emergency notification functionality.

4.2. National Response Center (NRC): During the second test, the Logistics Manager reported the potential hi-jacking incident to the National Response Center (NRC). Sixteen federal agencies and/or cabinet level departments comprise the NRC: U.S. Environmental Protection Agency; U.S. Coast Guard; U.S. Department of Agriculture; U.S. Department of Commerce; U.S. Department of Defense; U.S. Department of Energy; U.S. Department of Health and Human Services; U.S. Department of Interior; U.S. Department of Justice; U.S. Department of Labor; U.S. Department of Transportation; U.S. Department of Treasury; Federal Emergency Management Agency; U.S. General Services Administration; U.S. Nuclear Regulatory Commission; and U.S. Department of State. The NRC can be reached at 800-424-8802. The NRC was originally created to provide a national notification center for oil spills and hazardous substance releases. However, since the events of September 11, 2001, the NRC increased its services to address all emergency situations, including terror related incidents. As found on the NRC's web-site, it is promoted as the "one call does it call" (for all hazards and all emergencies). The NRC was established as the emergency notification aspect of the National Response Plan. The National Response Plan depicts coordination of response resources from various levels of government and from agencies with overlapping jurisdictions. The National Response Plan also established the National Incident Management System (NIMS), which describes how incidents of national significance are to be managed. For more detailed information about NIMS, please see **Appendix 3.**

The National Response Center's 800-424-8802 emergency phone number was an extremely capable tool for notifying federal emergency responders about a potential commercial transport hi-jacking and terrorist event. The Logistics Manager identified the threat, called the NRC and was immediately transferred to a live watch. The Logistics Manager was required to answer questions about the potential terrorist attack. Once the Logistics Manager's report was completed the NRC watch-stander sent a comprehensive alert to the nearest Environmental Protection Agency (EPA) office, the nearest FBI field office and various state government officials. Within a few minutes, the Logistics Manager also received a copy of the official incident report.

The NRC was very capable of providing emergent notification and initiating the mobilization of multi-jurisdictional emergency responders. The watch-stander quickly took pertinent information about the incident, put it into a report format and sent it via facsimile to applicable emergency responders. NRC points of contact are located in every state, and they are automatically notified when an emergency occurs. Notifications are sent using facsimile, phone or email. The receiving agency chooses the notification format. All completed incident reports are published on the NRC website for public review. However, terrorist related reports, actual or test, are not published because of the sensitive nature of the information. To view the report obtained during the second test see **Appendix 4**.

NI²-CIE's comparative analysis illustrated that the NRC needs to improve its capability to notify and mobilize applicable municipal emergency responders. The NRC had a database of in-state emergency responders; however, personnel seemed unfamiliar about each specific states' in-state emergency notification system. For instance, NRC watch-standers successfully accessed the State of New Hampshire's Office of Emergency Services, including New Hampshire's Enhanced 911. However, the NRC watch-stander was uncertain about what happened once the Enhanced 911 notification was executed. Moreover, NI² CIE's research found that neither the public nor the commercial transport industry easily recognized the NRC for the purpose of reporting a potential terrorist

incident. For a print-out documenting the National Response Center's contacts by topic, see **Appendix 5**.

4.3. Emergency 911: Emergency 911 was identified as a viable system for notifying emergency responders about an actual or imminent terrorist emergency. Emergency 911 covers 96% of the U.S., most of Canada and it is the public's most recognized emergency notification phone number in America. However, Emergency 911 has limitations as a national system to effectively alert emergency responders from multiple jurisdictions. Cargo supply chains using intermodal cargo transportation, in most cases, either cross several states and/or international borders. Therefore, Emergency 911, which is generally designed for in-state notifications, does not lend itself as a national notification system for domestic transportation of intermodal cargo.

4.4. Enhanced 911: New Hampshire and Rhode Island use enhanced 911 to mobilize in-state emergency responders. Enhanced 911 distinguished itself from Emergency 911 because of its capability to identify the caller's location. NI² CIE conducted a site visit at the State of New Hampshire's emergency operations center and interviewed the on-watch supervisor. NI²-CIE's research found that Enhanced 911 was capable of dispatching multiple emergency units and could effectively alert officials in bordering states. However, Enhanced 911 watch-standers were found to have limited authority to quickly escalate a terrorist incident of national significance to the federal level. NI² CIE's research showed that the Enhanced 911 protocol required the watch-stander to notify their supervisor and their supervisor had to notify either the Director or the Assistant Director. The Director or the Assistant Director held absolute authority to escalate the incident to the national level by either activating the state's emergency response plan or notifying their direct contacts at the federal level. It seemed perplexing that the protocol to elevate potential terrorist incidents of national significance did not reference the National Response Plan / National Response Center.

4.5. States' Anti-Terrorism Hotlines: NI² CIE researched states' anti-terrorism hotlines as potential methods for alerting emergency responders. The U.S. Department of

Homeland Security provided most states with funding to establish and maintain toll free terrorist hotlines. Citizens call terrorist hotlines to report suspected terrorist-related activities and behaviors. In general, phone numbers were found on state governments' official websites. States not having a terrorist hotline instructed their citizens to call Emergency 911. State terrorism phone numbers offer state-to-state connectivity; citizens from one state can directly access a terrorist hotline in another state. State terrorism hotlines were dedicated solely to terrorism issues, in contrast to Emergency or Enhanced 911, which are dedicated to all emergencies. However, state terrorist hotlines appear to be predominately used for intelligence gathering and not emergency response. Although states' anti-terrorism hotlines do not provide emergency notifications as one of their services, every call is to be investigated. This practice, though admirable, creates potential public and transport industry confusion as to the preferred protocol for elevating a terrorist incident of national significance, and the capability to execute an effective (quick) multi-agency response.

5. Additional Research

NI² CIE conducted additional research by interviewing emergency managers from several tractor trailer transportation companies located in the United States and Canada in order to gain a perspective from the transport industry. The purpose of these interviews was to learn about these companies' emergency response protocols for a potential hi-jacking incident. Overwhelmingly, transport companies place an operational priority on cargo integrity. All polled transport companies use GPS tracking devices to continuously monitor their trucks and cargo. However, companies place concern on knowing where their cargo is at anytime and forecasting exactly what time it will be at its intended destination.

One company's Safety Manager stated that his company has invested in commercially available geo-position tracking, panic alarm and remote engine shutoff devices. However, the company decided neither to activate the panic alarm nor the remote engine shutoff options because they were concerned with false alarms and human error. When asked about the company's protocols for a potential hi-jacking and terrorist incident,

paraphrasing the Safety Manager's response, "I would call Emergency 911". He further stated, "I am not aware of the National Response Center, but a national system would be useful when reporting an incident that covers more than one state".

NI² CIE's research identified that a majority of the polled U.S. transport companies were unaware of the National Response Center and none of the Canadian carriers were aware of the National Response Center. Many transport companies did not have in-place protocols addressing a potential terrorist hi-jacking.

To improve first responder capabilities to thwart a potential terrorist attack, NI² CIE's research identified a need for emergency notification centers and anti-terrorism information collection centers to have a greater understanding of each others' roles and responsibilities. Moreover, the U.S. Department of Homeland Security needs to educate the public and transport industry about the preferred emergency notification protocol for a potential terrorist incident of national significance.

6. Recommendations

The use of COTS geo-positioning technology within the container transportation industry will greatly aid emergency responders in their capability to thwart a terrorist attack by way of a hi-jacked or rouge cargo container and transport. NI² CIE found that there is a need for industry standards requiring the implementation of geo-position tracking technology, especially for over-road transportation of intermodal cargo containers. Test results revealed that geo-position tracking information maybe relayed to emergency responders. However, it is recommended that protocols governing the interoperability between the cargo container transportation industry and emergency responders be developed to foster a public safety culture to prevent potential terrorist attacks.

The use of geo-position tracking technology and the creation of strict protocols governing the interoperability between the transportation industry and emergency responders will;

- (a) improve anti-terrorism information sharing between the transportation industry and

emergency responders; and, (b) improve the capability to effectively mobilize response resources from various levels of government to prevent a potential terrorist attack.

Appendix 1

The GlobalTrak combines all the technology needed for global asset tracking and reporting as well as SSAS compliance for today's and future regulations

GlobaFone's partner Applied Satellite Engineering has researched the trends in the maritime industry to not only meet the Ships Security Alert System (SSAS) regulations, but to make an end-to-end solution for possible policies to come.

Monitor the transportation of your land or ocean fleet via the Internet using Iridium's truly Global all-digital satellite technology. Experience secure real-time tracking of your assets through your home or office computer.

In addition, use the Iridium network and GlobalTrak to make and log voice calls on board. An analog phone/pbx interface, crew PIN, and downloadable crew call log make the GlobalTrak the perfect crew voice telephone solution for your vessel.

GlobalTrak shown with optional battery back-up.



Feature Highlights	Hardware Highlights
<ul style="list-style-type: none"> GPS Tracking capability Capable of simultaneous emergency alert while phone in use Built-in crew calling, including unique caller ID codes and call history access "Smart Dialing" recognizes country codes, dismissing the need for the '+' or '00' Voice communication made available with optional analog phone or Iridium handset 	<ul style="list-style-type: none"> RJ11 Analog Phone/ PBX Jack RJ45 for external sensor/switch input RJ45 DSC Bus (for Handset/SIM Reader) 2.5 mm Headset Jack DB9 Data Port DC Inlet Jack Panic Button input Battery back-up (optional)

GlobalTrak

Web Based Interface via Ontec Tracking:

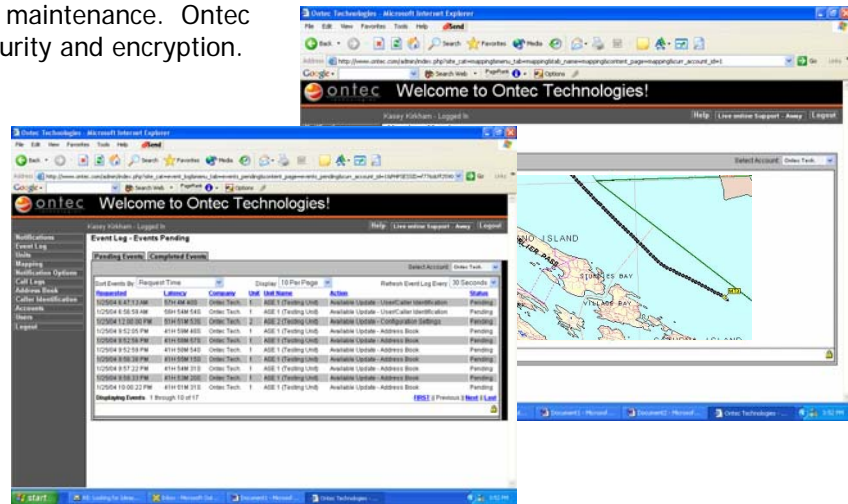
Ontec's Tracking provides complete interaction with GlobalTrak, giving users global access from any web interface. No software to install and no maintenance. Ontec ensures secure access using the strongest possible online security and encryption.

Highlights of this service include:

- Alarm and alert notification via email, fax, and pager
- Unit event logging and settings
- GPS listing and mapping
- Single or fleet unit configuration
- View call logs
- Remotely maintain unit address book, crew id codes, and tracking parameters

Personalized Options:

- Permission-based features and functionality
- Action logs track interaction with the application
- Branded experience with company's logo, color scheme and content



GlobaFone
80 Rochester Ave
Portsmouth, NH 03801
V.603.433.7232
F.603.436.8152
<http://globafone.com>



Globaltrak Interface Ports

Port	Function
RJ11 SLIC	Analog Phone, PBX Interface
DB-9 Data	RS-232C Computer Interface
2.5mm Audio Jack	Hands-free Headset Operation
RJ45 DSC Bus	SIM card reader, digital handset
RJ45 Expansion I/O	(3) 5V Logic Level Inputs, (3) Outputs
Power Input Jack	DC Voltage Input

GPS Specifications

Parameter	Value
Channels	12
Accuracy: Position	15 meters, 2D RMS 7 meters 2D RMS, WAAS corrected 1-5 meters, DGPS corrected
Velocity	0.1 meters/second
Time	1 microsecond synchronized to GPS time
Sample Rate	1 – TBD seconds (configurable)
Tracking Report Rate	Continuous, per minute, hourly, daily (configurable)

Mechanical Specifications

Parameter	Value
Dimensions	10.75 x 7.25 x 2.7 Inches
Weight	6.4 lbs
Mounting	Flange Mount

Iridium Antenna Specifications

Parameter	Value
Operating Temperature Range (without loss of function)	-40°C to +85°C
Measurement Frequency Range	1616 MHz to 1626.5 MHz
Return Loss (minimum)	9.5 dB (< 2:1 VSWR)
Gain (weighted average minimum)	0.0 dBic
Minimum 'Horizon' Gain	-2.0 dBic (82 degree conic average)
Nominal Impedance	50
Polarization	Right Hand Circular (RHCP)
Basic Pattern	Omnidirectional and Hemispherical

Note: The antenna cable used must insure a loss of < 3 dB and the minimum link margin of 12.1 dB must be maintained.

Electrical Specifications

Parameter	Value
Operating Voltage Range	10 to 32VDC Unregulated
Power Consumption	5 Watts Idle, 15 Watts Peak
Internal Battery Type	12V, 2.2AH Sealed Lead Acid
Battery Life (typical)	2 Hrs (Idle), 25 Minutes (Active)
Battery Charging Characteristics	Trickle Charge Method (15 Hrs to Full Charge)

Ship Security Alert System

Parameter	Value
Alarm Inputs	(3) Normally Closed
Test Button	(1)
Emergency Battery Backup	2 hours inactive / 25 minutes active
Qualifications	IEC 60495 (pending)
Emergency Position Transmission Rate	60 seconds
Emergency Communication Channel	SMS (leaves Voice channel available)

Environmental Specifications

Parameter	Value
Operating Temperature Range	0 to +70°C
Exposure	Dry, Protected Location per IEC 60945

Remote Control and Configuration

Parameter	Value
Remote Interface	TCP/IP, Web browser
Iridium Data Channel	RUDICS, SMS, SBD
Crew Call Logging	
Crew ID Combinations	65000 unique id codes
Log Size	500 calls
Log Download Rate	Hourly, daily, weekly
GPS	
Sample Rate	Continuous, 1 sec to 60 seconds
Transmit Sample Buffer Rate	Continuous, 1 – 59 minutes, hourly, or daily
Configuration Options	
Ringer	Base, Phone, Both
SmartDial	On/Off
Alarm Assigned Names	5-Characters Each

COTS/Hardware

GlobalTrak™ was chosen as the COTS. The **GlobalTrak™** device was provided to NI² CIE by **GlobaFone®** (www.globafone.com). **GlobalTrak™** provides global asset tracking and reporting by using the Iridium global all-digital satellite system provided by **Iridium Satellite LLC**. The Iridium system allows the user to track a shipment in real-time through a home or office computer via **Ontec Tracking™**. **Ontec Tracking™** is a web-based interface provided by **Ontec Technologies®**. **Ontec Tracking™** provides a complete interaction with the GlobalTrak device from any web interface, without software installation or maintenance.

GlobalTrak™ is a small device (10.75 x 7.25 x 2.7 inches, 6.4 lbs) that provides Global Positioning System (GPS) tracking, door intrusion detection and geo-fencing. The **GlobalTrak™** device can be mounted on a vehicle or on an intermodal cargo container. **GlobalTrak™** provides the following configurable tracking report rates: continuous, per minute, hourly or daily. The frequency at which the **GlobalTrak™** device sends a signal (ping), depends on how it is programmed. The ping is sent to the Iridium satellite. The satellite then sends a signal to the **Ontec Tracking™** system, which illustrates on a digital map the exact geo-position of the **GlobalTrak™** device.

NI² CIE chose **GlobalTrak™** as the COTS for the project because it was locally provided by **GlobaFone®**, which volunteered its time and resources to the two tests and provided knowledgeable customer service.

Appendix 2

Exercise Scenario

An intelligent cargo container is shipped to the United States from Europe via cargo ship. The intelligent container is equipped with a Commercial Off the Shelf (COTS) product(s) that has the ability to relay a data stream to a password protected website which can be manually or automatically reviewed. The COTS will allow the container to be globally tracked via Global Positioning System (GPS) signals. The COTS will also allow for the detection of unauthorized intrusion by using a magnetic door strip. All of the COTS data will be sent to the password protected website for review by the proper transport Logistics Manager to determine if there are any problems with the container.

The intelligent container is off-loaded at the port of Portland, ME onto a truck that is to deliver the container to a large retail store located in Bangor, ME. The truck will drive north on Interstate 95 (I95) to drop off the cargo. Therefore, a “geo-fence” will be set up on I95. A geo-fence is a predetermined location for which the truck can travel in without raising an alarm. If the truck leaves the geo-fence, data will be sent to the protected website and the consumer of the data will know that the truck has left its predetermined location. The geo fence for this example is highlighted below.



If the truck does not follow its predetermined course, the data being sent to the website will illustrate that the truck has left its geo-fence. If the magnetic strip that prevents unauthorized intrusion has been broken, a data signal will be sent to the website informing the trucking Logistics Manager that the container has been subjected to unauthorized intrusion. In the example below, the truck has broken its geo-fence and is heading south on Route 1 to Boston. The Logistics Manager will know that there is a security breach by reviewing the constant stream of live data being fed to the protected website.



Once the container violates its geo-fence, the Logistics Manager grows suspicious that the container transport might have been hijacked and could pose a serious danger to the public if used as a weapon. Attempts are made to contact the driver of the truck using cellular phone and VHF-FM radio but there is no response. After evaluating the situation and concluding that it is necessary to notify authorities, the Logistics Manager attempts to notify emergency responders. To contact and mobilize first responders, the Logistics Manager uses Regional Information Sharing Systems/Automated Information Exchange (RISS/ATIX) in the first test and the National Response Center in the second test.

Appendix 3

National Incident Management System

On February 28, 2003, President Bush issued Homeland Security Presidential Directive-5 (HSPD-5). HSPD-5 required the Secretary of Homeland Security to create the National Incident Management System (NIMS). NIMS provides a national framework for incident management and incident response for all levels of emergency response. NIMS enables the general public and first responders from the local, tribal, state and federal level to work under uniform guidelines in their response to domestic incidents. The aim of NIMS is to provide continuity in incident management, no matter the cause, size or difficulty of the situation.

The benefits of NIMS are as follows:

- Standardized organizational structures, processes and procedures;
- Standards for planning, training and exercising, and personnel qualification standards;
- Equipment acquisition and certification standards;
- Interoperable communications processes, procedures and systems;
- Information management systems; and
- Supporting technologies – voice and data communications systems, information systems, data display systems and specialized technologies.

<http://www.fema.gov/nims>

NIMS provides a comprehensive framework for the National Response Plan (NRP) of the United States. The NRP was created through coordination between local, tribal, state and federal agencies, nongovernmental organizations and private sector entities. The NRP applies to actual and potential incidents that would have a national impact on the United States. NIMS, combined with the NRP, provide the entire nation with a uniform way to plan, prevent, report and respond to emergencies both man made and natural. This is made possible by eliminating duplicate and cumbersome local, state and federal response plans and creating uniform guidelines across the board.

NIMS Compliance

The minimum requirements for NIMS compliance are drawn from the letter of the Secretary of Homeland Security to all of the state's Governors on September 8, 2004. State, local and tribal entities will need to accomplish these requirements during the fiscal year that ends on Sept. 30, 2005, if they want to become compliant with NIMS.

State and territory level efforts to incorporate NIMS must include the following:

- **Incorporate NIMS into existing training programs and exercises**
- **Ensure that Federal preparedness funding (including DHS Homeland Security Grant Program, Urban Area Security Initiative (UASI) funds) support NIMS implementation at the State and local levels** (in accordance with the eligibility and allowable uses of the grants)

- **Incorporate NIMS into Emergency Operations Plans (EOP)**
- **Promote intrastate mutual aid agreements; Memorandums of Understanding (MOU).**
- **Coordinate and provide technical assistance to local entities regarding NIMS**
- **Use the Incident Command System (ICS)**

The State, local, territorial and tribal levels of emergency response must support NIMS implementation by doing the following;

- **Complete the NIMS Awareness Course: “National Incident Management System (NIMS), An Introduction” IS 700.** The IS 700 course explains the key aspects of NIMS, such as incident planning, principles and components. It can be found at <http://training.fema.gov/EMIWeb/IS/is700.asp>.
- **Formally recognize the NIMS and adopt the NIMS principles and policies.** Legislation should be established by states, territories, tribes and local entities to adopt the minimum NIMS standards. Formal language and templates for NIMS adoption will be provided by the NIMS Integration Center (NIC). The NIC provides oversight of the National Incident Management System. NIC supports both day to day maintenance and long-term system care.
- **Establish a NIMS baseline by determining which NIMS requirements your agency already meets.** This can be done by using the NIMS Capability Assessment Support Tool (NIMCAST), which is being developed by the NIC. The NIMCAST is an online self-assessment tool which States, territories, tribes, and local governments can use to evaluate their capabilities to respond to incidents. Information on NIMCAST can be found at <http://www.fema.gov/nimcast/index.jsp>.
- **Establish a timeframe and develop a strategy for full NIMS implementation.** States, territories, tribes, and local entities should achieve full NIMS implementation during fiscal year 2005.
- **Institutionalize the use of the Incident Command System (ICS).** If not already in use, State, territorial, tribal, and local entities must implement the ICS response system that is consistent with the Department of Homeland Security. In order to be compliant with NIMS, federal, state, local and tribal entities must implement ICS.

Funding

Federal preparedness funding will be available to those agencies that have met the minimum fiscal year 2005 compliance standards. All applicants must be able to certify in their fiscal year grant applications that they have met the fiscal year 2005 requirements.

Appendix 4

Fire Involved: NO Fire Extinguished: UNKNOWN
 INJURIES: Hospitalized: Empl/Crew: Passenger:
 FATALITIES: Empl/Crew: Passenger: Occupant:
 EVACUATIONS: Who Evacuated: Radius/Area:
 Damages:

Closure Type	Description of Closure	Hours Closed	Direction of Closure
Air:	N		
Road:	N		Major N Artery:
Waterway:	N		
Track:	N		

Passengers Transferred: UNKNOWN
 Media Interest: NONE Community Impact due to Material: NO

 REMEDIAL ACTIONS

TESTING THE LINKS BETWEEN 911 AND THE NRC
 Release Secured: UNKNOWN
 Release Rate:
 Estimated Release Duration:

 WEATHER

Weather: UNKNOWN, :F

 ADDITIONAL AGENCIES NOTIFIED

Federal:
 State/Local: 911
 State/Local On Scene:
 State Agency Number: NO REPORT #

 NOTIFICATIONS BY NRC

CHEM/BIO DEFENSE COMMAND (PRIMARY)
 11-AUG-05 12:39 (410)4362148
 CENTERS FOR DISEASE CONTROL (PRIMARY)
 11-AUG-05 12:42 (770)4887100 MR MILLER
 CG INVESTIGATIVE SERVICE HQ (PRIMARY)
 11-AUG-05 12:39 (202)4936607
 DOT INTERMODAL HAZ MAT PROGRAM (PRIMARY)
 11-AUG-05 12:43 (202)3668013 MS SPONAUGLE
 EPA HQ EMERGENCY OPERATIONS CENTER (PRIMARY)
 11-AUG-05 12:39 (202)5643850
 EPA OEM (PRIMARY)
 11-AUG-05 12:44 (202)5643850 MR BURGESS
 U.S. EPA I (PRIMARY)
 11-AUG-05 12:45 (617)7238928 MS PASQUERELLA
 FBI BOSTON FIELD OFC (PRIMARY)
 11-AUG-05 12:46 (617)7425533 MS MURPHY
 FBI STRATEGIC INFO OPERATIONS CNTR (PRIMARY)
 11-AUG-05 12:39 (202)3233300
 FEDERAL EMERGENCY MANAGEMENT AGENCY (PRIMARY)
 11-AUG-05 12:39 (800)6347084
 G-OPF FOLDER (PRIMARY)
 11-AUG-05 12:39 (202)2672100
 INFO ANALYSIS & INFRA PROTECTION (PRIMARY)

11-AUG-05 12:39
 NATIONAL INFRASTRUCTURE COORD CTR (INFRASTRUCTURE PROTECTION)
 11-AUG-05 12:39 (202)2829201
 NOAA- OR&R. ATTN: CDR BLAKE (PRIMARY)
 11-AUG-05 12:39 (202)2671321
 NATIONAL RESPONSE CENTER HQ (PRIMARY)
 11-AUG-05 12:39 (202)2672100
 DOT OFFICE OF INTEL AND SECURITY (PRIMARY)
 11-AUG-05 12:39 (202)3666525

ADDITIONAL INFORMATION
 /////DRILL///// NO FURTHER INFORMATION GIVEN AT THIS TIME.

xxx END INCIDENT REPORT 768722 xxx
 Report any problems or Fax number changes by calling 1-800-424-8802
 PLEASE VISIT OUR WEB SITE AT <http://www.nrc.uscg.mil>
 xxxxxxxxxxxxxxxxxxxxxxxxxxxx THIS IS A DRILL
 xxxxxxxxxxxxxxxxxxxxxxxxxxxx
 THIS IS A DRILL xxxxxxxxxxxxxxxxxxxxxxxxxxxx
 xxxxxxxxxxxxxxxxxxxxxxxxxxxx THIS IS A DRILL
 xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Appendix 5

National Response Center Usage Statistics, 1997-2004

Fax and Email Notifications								
AGENCY	1997	1998	1999	2000	2001	2002	2003	2004
EPA	17,324	19,660	26,020	34,583	41,384	38,952	38,539	40,656
Coast Guard	12,975	13,815	14,524	16,211	18,654	18,005	19,231	24,374
Dept of Transportation	2,371	3,234	3,739	3,179	3,097	4,075	4,538	7,058
Department of Homeland Security	0	0	0	0	0	1,281	1,987	8,361
Department of Interior	13,342	12,311	12,967	12,194	19,622	21,183	14,100	4,503
Department of Health and Human Services	10,537	11,321	11,600	13,422	15,790	14,388	13,974	18,893
Federal Bureau of Investigation	5,723	5,853	2,193	703	447	6,816	491	2,233
National Transportation Safety Board	783	1,232	1,348	1,641	1,798	1,641	2,658	3,499
Nuclear Regulatory Commission	53	36	57	70	43	51	36	49
Department of Labor	52	90	139	230	190	114	82	72
National Oceanic and Atmospheric Administration	24,867	26,281	26,313	29,146	32,867	31,180	30,537	32,326
Department of Defense	2	68	147	122	124	463	3,525	5,184
Department of Energy	63	45	63	100	70	82	41	76
Chemical Safety Board	0	389	920	956	690	495	336	346
Department of State	0	1	6	2	10	10	3	25
Department of Agriculture	0	0	0	0	0	0	0	1
State Notifications	36,111	38,487	42,673	48,925	69,641	72,361	74,014	76,822
CHEMTREC	12	12	10	7	10	1	1	1
Other	789	575	971	2,025	3,957	5,024	1,207	1,116
Canada	0	0	0	0	0	0	0	9
Mexico	0	0	0	0	0	0	0	1,077
TOTAL NOTIFICATIONS	125,325	133,875	144,401	164,383	209,695	217,678	206,742	226,681
Incident Type, 1997-2004								
Incident Type	1997	1998	1999	2000	2001	2002	2003	2004
Fixed	10,388	10,961	11,230	11,813	12,441	11,917	11,972	12,972
Unknown Sheen	4,228	4,809	4,802	4,016	4,147	3,426	3,733	3,411
Vessel	3,778	3,886	3,877	3,945	4,378	3,919	3,961	4,385
Mobile	2,490	2,718	2,835	3,597	3,216	2,942	2,946	3,192
Pipeline	1,740	1,657	1,404	1,618	1,841	1,621	1,643	1,574
Platform	1,943	1,570	1,465	1,428	1,355	1,233	1,343	1,198
Storage Tank	0	0	0	1,379	3,140	3,044	2,809	2,838
Railroad Non-Release	586	823	1,049	1,335	1,235	1,124	1,173	1,476
Railroad	1,883	2,266	2,252	1,332	1,241	1,200	1,074	1,276
Continuous	170	304	376	938	238	393	462	112
Aircraft	207	181	241	248	297	278	262	277
Drill/Exercise	349	503	532	669	789	908	809	1,073
Unknown	14	3	52	84	0	0	0	0
Terrorist Non-Release	0	18	51	33	42	180	107	125
TOTAL INCIDENTS	27,776	29,699	30,166	32,435	34,360	32,185	32,294	33,909

Department of Homeland Security Notifications, 2003-2004		
UNIT	2003	2004
United States Coast Guard	19,241	24,374
Department of Homeland Security Coordination Center	1,746	2,142
Transportation Security Administration Operations Center	241	572
Transportation Security Administration Maritime and Land	0	1,091
National Infrastructure Coordination Center	389	1,103
Federal Emergency Management Agency	1,042	1,943
Federal Emergency Management Agency Region X	0	1,198
IAIP Watch	0	135
NIPC Watch and Warning Unit	0	167
TOTAL DHS NOTIFICATIONS	22,659	32,725