

REDACTED AND UNCLASSIFIED



# **THE FEDERAL BUREAU OF INVESTIGATION'S EFFORTS TO PROTECT THE NATION'S SEAPORTS**

U.S. Department of Justice  
Office of the Inspector General  
Audit Division

Audit Report 06-26  
March 2006

REDACTED AND UNCLASSIFIED

# **THE FEDERAL BUREAU OF INVESTIGATION'S EFFORTS TO PROTECT THE NATION'S SEAPORTS**

## **Executive Summary**

The nation's seaports and related maritime activities are widely recognized as being vulnerable to acts of terrorism. The consequences of a maritime-based terrorist attack are potentially devastating to both the economy and to public safety. The United States has more than 360 seaports, and 95 percent of overseas trade flows through these ports or inland waterways. Further, seaports are often located near major population centers and hazardous fuel or chemical storage facilities that may provide attractive terrorist targets. According to the National Commission on Terrorist Attacks Upon the United States (9/11 Commission), the risk of maritime terrorism is equal to or greater than the risk of terrorism involving civilian aviation. Although the United States has placed much attention on better securing civilian aviation since 2001, seaports remain largely at risk.

The protection of U.S. seaports is a shared responsibility among the Department of Homeland Security's (DHS) U.S. Coast Guard and U.S. Customs and Border Protection (CBP), and the Federal Bureau of Investigation (FBI). The Coast Guard has primary responsibility for the physical protection of the nation's seaports, and it has law enforcement authority in the maritime domain. CBP enforces import and export laws and regulations and bears primary responsibility for cargo inspections at seaports. The FBI, as the lead federal agency for preventing and investigating terrorism, has an overarching role in helping to secure the nation's seaports. The FBI's responsibilities are part intelligence and part law enforcement, including assessing the threat of maritime-based terrorism; gathering, analyzing, and sharing information on maritime threats; and maintaining well-prepared tactical capabilities to prevent or respond to maritime-based terrorism. Unless incident command and other coordination issues are resolved in advance and response scenarios are exercised, the overlapping nature of the FBI's and the Coast Guard's responsibilities in the maritime domain may result in confusion and interagency conflict with the FBI in the event of a maritime incident. CBP's more discrete responsibilities do not present as much likelihood for conflict.

A 1979 memorandum of understanding (MOU) between the FBI and the Coast Guard acknowledges their overlapping jurisdiction and the need for cooperation and coordination in the maritime domain. After the September 11 terrorist attacks, the Maritime Transportation Security Act of 2002 increased the Coast Guard's responsibility in maritime terrorism prevention and response. In addition, the National Strategy for Maritime Security, developed by an interagency committee and issued in September 2005, attempts to align federal government maritime security programs into a comprehensive national effort involving federal, state, local, and private sector entities. Eight plans support the National Strategy for Maritime Security. One of the plans is the Maritime Operational Threat Response (MOTR) plan, which was issued in October 2005. The MOTR describes the U.S. government's plan to respond to terrorist threats in the maritime domain, including the roles of various federal agencies, protocols for lead and supporting agencies, and the need for additional planning. The MOTR assigned the DHS, implemented through the Coast Guard, lead agency responsibility for interdicting maritime threats where it operates and assigned the Department of Justice (DOJ), through the FBI, lead agency responsibility for investigating maritime threats and incidents. However, both the FBI and the Coast Guard have jurisdiction to interdict maritime threats, and the MOTR did not resolve potential conflict between the two agencies in incident command and response.

The DOJ Office of the Inspector General (OIG) initiated this audit to examine the FBI's seaport security efforts. We reviewed the FBI's roles and responsibilities for preventing and responding to terrorist attacks in the maritime domain, and the extent and effectiveness of the FBI's interagency coordination and cooperation. To accomplish these overall objectives, we examined the FBI's: (1) initiatives to prevent maritime terrorism, including coordination with the Coast Guard and other agencies; (2) capability to respond to maritime incidents; and (3) efforts to assess the maritime terrorism threat.

Our audit found that over the past 3 years the FBI has taken steps to enhance its capability to identify, prevent, and respond to terrorist attacks in the maritime domain, including seaports. Among the positive steps the FBI has taken to enhance seaport and maritime security are:

REDACTED AND UNCLASSIFIED

- creating Maritime Liaison Agents (MLA) at FBI field offices and assigning these agents responsibility for coordinating with the FBI's maritime partners, including the Coast Guard and CBP;
- establishing a Maritime Security Program at FBI headquarters to oversee the MLAs and centralize the FBI's maritime efforts;
- improving the FBI's ability to respond to a maritime terrorism threat or incident, including creating enhanced maritime Special Weapons and Tactics (SWAT) teams located in the field offices closest to the Coast Guard's counterterrorism response teams;
- providing maritime-related intelligence to other intelligence and law enforcement agencies; and
- establishing a database, the Guardian Threat Tracking System, to collect information on terrorist threats and suspicious incidents at seaports and elsewhere and manage follow-up action on these threats and incidents.

However, we believe the FBI needs to take additional steps to improve its capability to deal with the threat of maritime terrorism by:

- resolving potential incident command, coordination, and response issues that could arise from confusion about the respective roles of the FBI and the Coast Guard;
- improving the collection and dissemination of lessons learned and best practices from maritime counterterrorism exercises;
- allocating FBI resources according to the threat and risk of maritime terrorism relative to other threats against other critical infrastructures such as aviation;
- ensuring that all FBI field offices use the Guardian database to enter and maintain data on threats and suspicious incidents at seaports and elsewhere; and
- improving maritime-related intelligence gathering and dissemination.

## **Maritime Initiatives**

The FBI established its MLA program in 2004 as a result of a joint FBI and Coast Guard investigation into the threat posed by divers and combat swimmers. MLAs are assigned to most of the FBI's 56 field offices and are the most visible and active FBI resource dedicated to preventing maritime terrorism. There are 73 MLAs, about two-thirds of whom are FBI agents and one-third are other agency personnel assigned to the FBI's Joint Terrorism Task Forces. MLAs are primarily responsible for coordinating with other entities who share responsibility for security at the nation's ports, thereby facilitating the sharing of information on threats and security measures. According to FBI Counterterrorism Division (CTD) managers, MLAs should be maritime experts with the knowledge and relationships to significantly assist the FBI in resolving any terrorist threat or event that may occur at local seaports.

However, we found that the FBI does not always assign MLAs according to the threat and risk of a terrorist attack on a given seaport. An analysis performed by the DHS for its Port Security Grant program suggests that 24 FBI field offices are responsible for helping protect over 80 percent of the seaports facing the greatest risk of a terrorist attack. But because the FBI assigns MLAs without assessing the threat and risk of terrorists attacking or using a particular seaport for an attack, MLAs are not necessarily assigned to the most critical ports. Instead, we found that FBI field offices with multiple vital ports may have only one MLA, while other FBI field offices with only minor maritime activity may have multiple MLAs. For example, one FBI field office has six significant ports in its territory but only one MLA. In contrast, another FBI field office has no strategic ports in its area but five MLAs. Furthermore, the FBI does not track the amount of time MLAs or other agents or analysts spend on maritime terrorism. Such tracking would help the FBI determine where its maritime activity is occurring, how much time is being spent on specific activities such as interagency training or coordination with Coast Guard-sponsored Area Maritime Security Committees (AMSC), and where additional resources should be deployed.<sup>1</sup>

---

<sup>1</sup> AMSCs, mandated by the Maritime Transportation Security Act, are comprised of federal, state, and local agencies as well as representatives of the shipping and port communities. Each committee is charged with assessing its port's vulnerabilities and developing plans to meet security requirements.

In July 2005, during the course of our audit, the CTD created a Maritime Security Program, which now has responsibility for the MLA program. The Maritime Security Program is intended to be the focal point for the FBI's maritime efforts, including carrying out the FBI's responsibilities under the National Strategy for Maritime Security and the strategy's eight implementing plans. Because the Maritime Security Program is a recent initiative, we could not fully assess its impact. It has, however, already changed the MLA program by asking all field offices with MLAs to name an FBI special agent as the field office's lead MLA. In addition, the Maritime Security Program plans to visit 30 percent of the nation's major transportation hubs, metropolitan areas with both a major seaport and major airport. The purpose of the visits is to learn about the vulnerabilities of seaports, the activities of the MLAs, how to improve guidance to the MLAs, and how to better focus the Maritime Security Program. We view this as an indication that the FBI is beginning to consider the threat and risk of maritime terrorism in conducting its Maritime Security Program.

The Maritime Security Program has also announced 13 objectives for fiscal year (FY) 2006, many of which we believe will be beneficial and help focus the FBI's efforts at preventing maritime terrorism. However, we are concerned that these objectives are not described in a way that will allow the program to assess progress toward meeting its goals. In addition, the objectives do not include critical needs such as maritime threat assessments and the identification of informants who can provide information on maritime threats.

### **Maritime Response Capabilities**

The response to terrorist threats or incidents in the maritime domain presents unique challenges to the FBI and other responders. The FBI has several tactical assault options for maritime situations and also the capability to deal with maritime-based weapons of mass destruction (WMD) through:

- field office SWAT teams, including 14 teams with some additional maritime training;
- the Hostage Rescue Team (HRT), which has specialized training and equipment and is able to assault and take control of a ship whether it is docked or underway; and

## REDACTED AND UNCLASSIFIED

- the Hazardous Devices Response Unit, with capabilities to deal with terrorist attacks using chemical, biological, radiological, or nuclear weapons — including a WMD aboard a ship.

The Coast Guard has significant responsibilities for enforcing laws in the maritime domain, a role that received an added counterterrorism component with the passage of the Maritime Transportation Security Act in 2002. This Act required the Coast Guard to create Maritime Safety and Security Teams (MSST) capable of rapidly responding to threats of maritime terrorism. The Coast Guard has 13 MSSTs nation-wide. At the same time, the FBI created enhanced maritime SWAT teams to enable it to work better with the Coast Guard's MSSTs. Nearly all of the FBI's teams are located in the FBI field office closest to an MSST.

### *Overlapping Responsibilities*

Officials at the FBI and the Coast Guard agreed that the Maritime Transportation Security Act created overlapping responsibilities between the agencies. This overlap has the potential to confuse the respective responses of the FBI and the Coast Guard to a maritime-based terrorism incident. For example, the FBI officials with whom we spoke were unsure of MSST capabilities and were concerned that these Coast Guard tactical teams might duplicate the FBI's HRT and SWAT teams. Based on our discussions with FBI personnel, we believe the HRT has unique capabilities to board, assault, and take control of a ship whether it is docked or underway. Prior to the release of the Maritime Operational Threat Response plan, officials from both the FBI and the Coast Guard agreed that the MOTR should resolve jurisdictional issues. However, the MOTR issued in October 2005 is an interim plan, which FBI officials say does not clearly delineate the respective roles of the Coast Guard and the FBI. In our opinion, a lack of jurisdictional clarity in the MOTR could hinder the ability of the FBI and the Coast Guard to coordinate an effective response to a terrorist threat or incident in the maritime domain. Specifically, we are concerned about how confusion over authorities will affect the two agencies' ability to establish a clear and effective incident command structure. While a final MOTR plan may resolve the problem of overlapping roles, we believe the FBI should propose an MOU to the Coast Guard and conduct joint exercises with the Coast Guard to resolve any coordination or incident command issues.

Compared to the FBI-Coast Guard relationship, the relationship between the FBI and CBP is better defined given the more distinctive roles of each agency. The FBI, for example, does not have a direct role in cargo inspection. Consequently, the coordination required between the two agencies centers on intelligence sharing and notification in the event of a threat or incident.

### *Lesson Learned*

Exercises, whether operational or incident command exercises, can provide valuable lessons and identify best practices for improving future response capabilities. FBI policy requires the preparation and dissemination of after-action reports following exercises and major operations. However, the FBI was unable to provide after-action reports for most maritime exercises, and we concluded that reports were not prepared for all exercises. During FYs 2002 through 2005, the FBI prepared reports for 6 of 19 maritime-related exercises or incidents. Most of these six involved interagency exercises with the Coast Guard and other elements of the DHS, such as CBP. We reviewed the FBI's after-action reports and found that most raised concerns about interagency incident response in the following areas: communication, adequacy or coordination of resources, command and control coordination, and jurisdiction or authority. According to an acting unit chief in the FBI's Critical Incident Response Group, the FBI has not systematically reviewed these after-action reports to identify and disseminate the lessons learned from these exercises. Due to the critical need for the FBI to resolve any jurisdictional, communications, or incident command and response issues, we believe the FBI should prepare after-action reports and take action on the lessons learned from all interagency and FBI maritime terrorism exercises.

### **Scope of the Maritime Threat**

The FBI faces a difficult challenge in trying to cover all likely terrorist tactics and targets given the many types of infrastructure in the United States and the huge number of potential targets. Although the FBI has conducted general terrorist threat assessments, it has neither conducted nor reviewed a threat assessment that indicates where seaports and the maritime domain rank among the tactics and likely targets of terrorists. Assessing the maritime threat would be useful not only to define the nature, likelihood, and severity of the threat compared to other threats but also to allow FBI managers and others to make informed decisions about resource allocation.



## REDACTED AND UNCLASSIFIED

In reviewing the FBI's maritime-related intelligence reports over the 4 years since the 9/11 terrorist attacks, we found that the FBI tended to focus on just two potential tactics: attacks by scuba divers or combat swimmers and infiltration of the United States by various maritime methods. We are concerned that the FBI may not be devoting its intelligence resources to assessing high-risk maritime areas. For example, although terrorists have indicated a strong desire to use a WMD and vessels can be used to transport a WMD for detonation in a port or elsewhere, none of the FBI's intelligence reports assessed the threat and risk of terrorists smuggling a WMD in a shipping container aboard a cargo ship.

The FBI's Directorate of Intelligence establishes requirements for meeting the FBI's intelligence needs but does not follow up to ensure that the FBI's operational divisions and field offices are working to address these requirements concerning maritime or other threats. Therefore, intelligence questions about terrorists' maritime intentions and plans may go unanswered. Further, the FBI does not correlate its list of intelligence requirements with its intelligence reports. This lack of linkage hampers the FBI from readily identifying those intelligence reports that answer intelligence questions about maritime terrorism. Consequently, the FBI might have intelligence about maritime terrorism that is not easily located within the intelligence reports. However, we found that the Directorate of Intelligence is aware of these shortcomings and has several initiatives ongoing to ensure that the FBI addresses its intelligence-gathering requirements in the maritime domain and other areas.

The FBI has not collected complete data on the number of suspicious activities or terrorist threats involving seaports. However, using a database called the Guardian Threat Tracking System (Guardian), the FBI appears to be making significant progress in identifying, tracking, and internally sharing information on maritime and other terrorist threats and suspicious incidents. However, Guardian cannot be easily searched to identify trends in maritime-related suspicious activities or threats, and the FBI has not ensured that FBI offices comply with directives concerning the use of Guardian and the need to document the resolution of all incidents entered in Guardian. The number of Guardian entries varies greatly by field office, with two field offices accounting for 21 percent of the entries made by field offices. Also, as of August 2005, Guardian contained about 6,000 entries that showed no outcome of any follow-up or

investigation. According to FBI officials, a new version of Guardian, scheduled to be deployed in March 2006, will enhance the FBI's ability to search the database for maritime-related incidents. But the success of Guardian and the FBI's ability to identify trends in suspicious incidents, including maritime-related incidents, is highly dependent on field agents using the system as required.

Through our review of the FBI's maritime-related intelligence reports, we identified useful initiatives at the FBI's Chicago, Newark, and Seattle field offices. Chicago and Newark issue intelligence bulletins discussing maritime-related incidents to other federal, state, and local law enforcement agencies. A Seattle intelligence assessment used a weighted ranking system to evaluate whether a given maritime-related suspicious incident was indicative of pre-operational planning for a terrorist attack. We believe that the FBI should consider making greater use of these initiatives.

### **Conclusions and Recommendations**

The FBI faces a difficult task in protecting the nation from all potential terrorist targets and methods, and seaports are just one type of critical infrastructure that requires protection. Yet due to the vulnerability of seaports and maritime activities to a terrorist attack, the FBI has a responsibility to not only provide the resources needed to ensure an adequate response capability and intelligence gathering and sharing, but also to contribute to an effective, coordinated government response to any maritime-related terrorist threat. The FBI recognizes the general threat of maritime-based terrorism due to the inherent vulnerability of seaports, and it has established a Maritime Security Program, assigned MLAs to many FBI field offices to coordinate with other agencies involved in securing the nation's seaports (although the FBI should ensure that MLAs are assigned to the higher-risk locations), participates in Coast Guard-sponsored AMSCs, and has trained and equipped tactical assault forces and hazardous materials experts that can operate in the maritime domain.

To ensure an effective federal government response to maritime terrorism, the overlapping responsibilities, jurisdictions, and capabilities of the FBI and the Coast Guard need to be sorted out before an incident occurs and not during an incident. Unfortunately, the MTSA and the MOTR plan have not eliminated the potential for interagency conflict and confusion in the event of a terrorist incident at a seaport or elsewhere in the maritime domain. The shared

## REDACTED AND UNCLASSIFIED

responsibility among the FBI, Coast Guard, and to a lesser extent CBP, to ensure the safety of U.S. seaports requires the FBI to update the 1979 MOU or otherwise come to agreement with the Coast Guard on each agency's respective roles and authorities.

Once such agreement is reached on incident command and related issues, the FBI should emphasize leading or participating in more interagency maritime-related exercises involving likely terrorism scenarios. Such exercises are important to identify and resolve any problems or misunderstandings over jurisdiction, incident command, communications, tactical operations, or other matters that might impede the swift and effective resolution of a maritime terrorist incident. In addition, the FBI should ensure that it gleans lessons learned and best practices from all interagency maritime-related exercises to help resolve any disputes, confusion, or communications problems and improve its response capabilities.

The FBI has not specifically assessed the threat and risk of terrorism at U.S. seaports, although it is addressing aspects of seaport security in its intelligence gathering and reporting activities. However, in addition to assessing the threat and risk of maritime-based terrorism, the FBI's Directorate of Intelligence should better track how the FBI's field offices are addressing the FBI's intelligence collection requirements pertaining to seaport security. The FBI is in the process of enhancing the search capabilities of its Guardian threat-monitoring database used to identify and track threats and suspicious activities, including those at seaports. However, the FBI needs to ensure that the database is more universally applied throughout FBI field offices and that the entries receive prompt follow-up or investigation.

In our report, we make 18 recommendations to the FBI to help enhance the FBI's contributions to the security of U.S. seaports. Among our recommendations are that the FBI:

- resolve potential role and incident command conflicts in the event of a maritime terrorist incident through joint exercises and, if necessary, a revised and broadened MOU with the Coast Guard;
- ensure that the Maritime Security Program has measurable objectives;

REDACTED AND UNCLASSIFIED

- assign MLAs based on an assessment of the threat and risk of a terrorist attack to critical seaports;
- prepare after-action reports after all maritime-related exercises and use the reports to identify and disseminate lessons learned and best practices;
- assess the threat and risk of maritime terrorism compared to other terrorist threats;
- focus intelligence reporting to more comprehensively address potential maritime-related terrorist targets and methods; and
- monitor the progress of operating divisions and field offices in answering intelligence collection requirements pertaining to seaports and maritime terrorism.

**TABLE OF CONTENTS**

INTRODUCTION ..... 1  
    Background..... 1  
    Authorities ..... 2  
    Prior Reports ..... 8

FINDINGS AND RECOMMENDATIONS..... 12

Finding 1: Maritime Initiatives ..... 12  
    Organization and Resources ..... 13  
    Maritime Liaison Agent Program ..... 13  
    MLA Program Not Risk-Based ..... 16  
    Some Risk Data Is Available ..... 18  
    FBI Does Not Measure Efforts to Prevent Maritime Terrorism ..... 19  
    Maritime Security Program..... 23  
    Conclusion ..... 26  
    Recommendations ..... 26

Finding 2: Maritime Response Capability ..... 28  
    Field Office SWAT Teams ..... 28  
    Hostage Rescue Team ..... 31  
    Hazardous Devices Response Unit..... 33  
    Capability-Based Planning ..... 36  
    Maritime Operational Threat Response Plan..... 38  
    Exercises and Responses ..... 42  
    Conclusion ..... 46  
    Recommendations ..... 47

Finding 3: Scope of the Maritime Threat..... 48  
    Comprehensive Assessment of the Threat..... 49  
    Intelligence Requirements..... 58  
    Data on the Number of Maritime Threats ..... 63  
    Conclusion ..... 72  
    Recommendations ..... 72

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS..... 74

STATEMENT ON INTERNAL CONTROLS..... 75

APPENDIX I: OBJECTIVES, SCOPE, AND METHODOLOGY..... 77

APPENDIX II: FIELD OFFICE GUARDIAN ENTRIES, 30-DAY PERIOD  
    ENDING MARCH 28, 2005..... 79

REDACTED AND UNCLASSIFIED

APPENDIX III: MARITIME ACTIVITY AND RISK OF MARITIME  
TERRORISM CONCENTRATED IN THE TERRITORY OF  
24 FBI FIELD OFFICES ..... 81

APPENDIX IV: ACRONYMS ..... 82

APPENDIX V: FEDERAL BUREAU OF INVESTIGATIONS RESPONSE TO  
THE DRAFT REPORT ..... 83

APPENDIX VI: OFFICE OF THE INSPECTOR GENERAL, AUDIT DIVISION  
ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO  
CLOSE REPORT ..... 99

## **INTRODUCTION**

### **Background**

U.S. seaports import and export cargo worth hundreds of billions of dollars each year. With more than 360 ports, the nation's port system stretches along 95,000 miles of coastline. Over 95 percent of the nation's overseas trade flows through seaports and inland waterways, and the U.S. economy is highly dependent on an efficient transfer of goods flowing into and out of these gateways.

The U.S. seaport system is complex, with each port having its own geography, infrastructure, and mix of cargo and passengers. Ports handle various bulk cargo, oil, liquefied natural gas, and other goods; serve as passenger terminals for ferries and cruise lines; and house or are adjacent to critical infrastructures such as chemical storage facilities, oil refineries and tanks, and rail yards. Ports also host naval bases and vessels.

Because of the maritime domain's open nature and economic and military significance, it is an attractive target for exploitation and disruption by terrorists. Seaports are susceptible to terrorists because their facilities contain critical infrastructure, are sprawling and exposed, are accessible by water and land, are often close to crowded metropolitan areas, and are interwoven with complex transportation networks.

Consequently, seaports are vulnerable to a variety of terrorist attacks. For instance, cargo containers are a potential conduit for terrorists to smuggle a weapon of mass destruction (WMD) or other dangerous materials into the country. Also, ports often contain many potential targets such as military vessels and bases, cruise ships, passenger ferries, terminals, factories, office buildings, power plants, refineries, and other critical infrastructures. In January 2004 testimony before Congress, a Federal Bureau of Investigation (FBI) Counterterrorism Division (CTD) official recognized ports' vulnerability to cargo thefts and smugglers of drugs, aliens, and weapons. He stated that terrorist organizations have studied the practices of traditional smuggling operations and are looking to exploit any weaknesses in the country's port security system. He also said that access into and around U.S. port facilities is difficult to secure without closing access to legitimate business and recreational port traffic.

While no port-related terrorist attacks have occurred in the United States, a large-scale maritime attack could cause mass casualties and economic disruption. Internationally, terrorists attacked the USS *Cole* and the French tanker *Limburg* and have attempted other attacks on maritime targets, thus illustrating terrorist groups' interest in exploiting the vulnerability of the maritime domain.

## **Authorities**

The FBI derives its roles and responsibilities for preventing and responding to maritime-related terrorist attacks against the United States from a series of statutes and directives. The U.S. Coast Guard also has law enforcement authority in the maritime domain and, according to the Maritime Transportation Security Act (MTSA), is the lead federal agency responsible for seaport security. U.S. Customs and Border Protection (CBP), part of the Department of Homeland Security (DHS), is responsible for preventing terrorists from using cargo containers to smuggle personnel or a WMD into the United States.

### *FBI General Authority*

The FBI's general law enforcement authority comes from 28 U.S.C. § 533, which grants the Attorney General the authority to appoint officials to detect and prosecute crimes against the United States. That statute recognizes the need for the FBI to work with other federal law enforcement agencies that may also have concurrent authorities for crimes the FBI may investigate. In implementing this statutory mandate, the Attorney General made this concurrent authority clear by promulgating 28 C.F.R. § 0.85 instructing the Director of the FBI to "Investigate violations of the laws, including the criminal drug laws, of the United States and collect evidence in cases in which the United States is or may be a party in interest, except in cases in which such responsibility is by statute or otherwise exclusively assigned to another investigative agency."



REDACTED AND UNCLASSIFIED

The FBI's statutory jurisdiction includes the "special maritime and territorial jurisdiction" defined in 18 U.S.C. § 7:

*The high seas, any other waters within the admiralty and maritime jurisdiction of the United States and out of the jurisdiction of any particular State, and any vessel belonging in whole or in part to the United States or any citizen thereof, or to any corporation created by or under the laws of the United States, or of any State, Territory, District, or possession thereof, when such vessel is within the admiralty and maritime jurisdiction of the United States and out of the jurisdiction of any particular State ....*

This jurisdictional definition applies to both terrorism-related crimes as well as any other criminal offense in Title 18 U.S.C. that specifically applies to the "special maritime and territorial jurisdiction of the United States."

*FBI Authority for Investigating Terrorism*

In addition to the FBI's general authority to investigate federal crimes, 18 U.S.C. § 2332b (f), "Acts of Terrorism Transcending National Boundaries," gives the Attorney General lead investigative authority over terrorist crimes, as follows: "In addition to any other investigative authority with respect to violations of this title, the Attorney General shall have primary investigative responsibility for all federal crimes of terrorism ..."

The definition of Federal Crimes of Terrorism, 18 U.S.C. § 2332, lists several violations within the maritime domain in which the FBI has primacy, including:

- 18 U.S.C. § 2280 — violence against maritime navigation covering the hijacking, damage/destruction, or other violence aboard a vessel that endangers the safe navigation of that vessel,
- 18 U.S.C. § 2281 — violence against maritime fixed platforms,

REDACTED AND UNCLASSIFIED

- 18 U.S.C. § 1363 — damage to buildings or property within the special maritime and territorial jurisdiction of the United States,
- 18 U.S.C. § 81 — arson within the special maritime and territorial jurisdiction, and
- 18 U.S.C. § 2332f — bombings of places of public use, government facilities, public transportation systems and infrastructure facilities including waterways.

In 28 C.F.R. § 0.85, the Attorney General made the FBI's role in investigating terrorism clear, including those situations which may involve concurrent authority, by instructing the Director of the FBI to:

*Exercise Lead Agency responsibility in investigating all crimes for which it has primary or concurrent jurisdiction and which involve terrorist activities or acts in preparation of terrorist activities within the statutory jurisdiction of the United States. Within the United States, this would include the collection, coordination, analysis, management and dissemination of intelligence and criminal information as appropriate. If another Federal agency identifies an individual who is engaged in terrorist activities or in acts in preparation of terrorist activities, that agency is requested to promptly notify the FBI. Terrorism includes the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.*

Presidential Decision Directives (PDD) 39 and 62 reaffirm the existing statutory responsibilities for counterterrorism assigned to the FBI. In June 1995, 2 months after the bombing of the Murrah Federal Building, in Oklahoma City, the President issued PDD 39 to clarify U.S. counterterrorism policies. The PDD requires that "the Secretaries of State, Defense, Treasury, Energy and Transportation, the Attorney General, the Director of Central Intelligence and the Director, FBI shall ensure that their organizations' counterterrorism capabilities within their present areas of responsibility are well managed, funded, and exercised."

REDACTED AND UNCLASSIFIED

The PDD also directs that certain federal agencies, including the FBI take measures to:

- reduce vulnerabilities and prevent and deter terrorist acts before they occur;
- respond to terrorist acts that do occur (crisis management) and apprehend and punish terrorists; and
- manage the consequences of terrorist acts.

The strategy outlined in PDD 39 incorporates the need to address terrorists' potential use of WMD across the three elements listed above. PDD 39 gives the FBI responsibility for reducing the United States' vulnerability to terrorism through an expanded program of counterterrorism and gives the FBI lead federal agency responsibility for crisis response and crisis management in the event of a terrorist attack on U.S. soil. Specifically, the FBI leads the operational response to a terrorist attack while performing law enforcement and investigative efforts to deter, preempt, apprehend, and prosecute terrorists.

In May 1998, the President issued PDD 62, which reaffirms the FBI's lead agency role in crisis management for terrorist events occurring domestically and clarifies or establishes various agencies' roles in the overall federal counterterrorism strategy.

*United States Coast Guard*

According to 14 U.S.C. § 2, the Coast Guard "shall enforce or assist in the enforcement of all applicable federal laws on, under, or over the high seas and waters subject to the jurisdiction of the United States," thereby granting the Coast Guard concurrent authority over maritime matters with other federal agencies.

The safety and protection of U.S. ports, waterways, and marine environment are governed by Title 33 of the U.S. Code. As provided by 33 U.S.C. § 1226 and § 1227, the Coast Guard has concurrent authority to prevent, respond to, or investigate an act of terrorism within its jurisdiction.

## REDACTED AND UNCLASSIFIED

The FBI and Coast Guard entered into several memoranda of understanding (MOU) and other agreements, in which both federal agencies acknowledge their concurrent jurisdiction and the need for cooperation and coordination in the maritime domain. Most recently, in 1979 the FBI Director and the Coast Guard Commandant signed an MOU agreeing to a policy of mutual assistance in support of FBI and Coast Guard operations to counteract terrorist activities in the maritime environment. According to the MOU, the FBI:

- maintains a large number of strategically located Special Weapons and Tactics (SWAT) teams;
- has personnel trained to act as negotiators in dealing with terrorists' demands; and
- can use SWAT teams to suppress terrorists' actions during direct confrontation scenarios.

The Coast Guard:

- maintains and operates a large number of strategically located floating units, aircraft, vehicles, and shore stations; and
- has trained personnel to react to law enforcement activities in a maritime environment.

This MOU was intended to eliminate delays in response time to terrorist activities and encourage procedures and contingency plans to combat terrorist activities in the maritime domain.

### *United States Customs and Border Protection*

The Department of Homeland Security's CBP, which enforces import and export laws and regulations, also has responsibilities for preventing terrorists and WMD from entering the United States. Specifically, CBP is responsible for preventing terrorists from exploiting vulnerabilities caused by the movement of millions of oceangoing containers. Because approximately nine million of these cargo containers arrive at U.S. seaports every year, it is not feasible for CBP inspectors to physically inspect each container. Instead, CBP inspectors, both at overseas and U.S. seaports, assess the risk of each

container to determine which containers will undergo inspections. For those containers determined to be high-risk, CBP inspectors perform a non-intrusive examination, an intrusive inspection, or a combination of both. A non-intrusive examination may include one or more of the following techniques: use of an x-ray or gamma ray machine to identify anomalies in a container's contents, radiation detectors to identify illegitimate radioactive material, and canine search for narcotics or explosives. An intrusive inspection generally involves a partial or total removal of a container's contents.

*Recent Legislation and Directives*

Since the attacks of September 11, 2001, the federal government has been attempting to strengthen U.S. transportation and critical infrastructure security weaknesses. Seaports have been widely recognized as a critical vulnerability in the nation's defense against terrorism.

In November 2002, Congress passed the Maritime Transportation Security Act, which mandated an increase in the Coast Guard's responsibility in maritime terrorism prevention and response. The MTSA also requires the Secretary of Homeland Security, through the Coast Guard, to conduct a detailed vulnerability assessment of port facilities and vessels that may be involved in a transportation security incident. The vulnerability assessment must include the identification and evaluation of critical assets and infrastructures, identification of the threats to those assets and infrastructures, and identification of weaknesses in areas such as physical security, structural integrity, and contingency response.

The MTSA also requires that the Coast Guard develop a National Maritime Transportation Security Plan for deterring and responding to a transportation security incident at U.S. ports. This plan must identify: assignments of duties and responsibilities among responding federal, state, and local agencies; security resources; emergency procedures; and ranking of critical infrastructure.

The MTSA also directed the Coast Guard to create Maritime Safety and Security Teams (MSSTs) capable of rapidly responding to maritime terrorism threats to U.S. waters and ports. MSSTs are required to have the ability to conduct high-speed intercepts; board, search, and seize any harmful article in a vessel or port; and assist

REDACTED AND UNCLASSIFIED

with vulnerability assessments of facilities. The MSSTs are directed to coordinate their activities with other responding agencies.

On December 21, 2004, the President Issued National Security Presidential Directive 41/Homeland Security Presidential Directive 13, entitled "Maritime Security Policy," outlining a policy to fully coordinate and integrate government-wide efforts to protect U.S. interests in the maritime domain. The directive requires the Secretaries of Defense and Homeland Security to jointly lead the interagency effort by drafting an overarching maritime domain strategy called the National Strategy for Maritime Security along with eight supporting plans.

The National Strategy for Maritime Security, issued in September 2005, attempts to align federal government maritime security programs into a comprehensive national effort involving federal, state, local, and private sector entities. The eight supporting plans address the specific threats and challenges of the maritime environment. One supporting plan, the October 2005 Maritime Operational Threat Response (MOTR) plan, details federal agencies' protocols in responding to various maritime terrorism threats or incidents. The MOTR describes the U.S. government's plan to respond to terrorist threats in the maritime domain, including the roles of the different federal agencies, protocols for lead and supporting agencies, and the need for additional planning. It calls for operating plans outlining how each lead agency will fulfill its responsibilities. The MOTR endorses capability-based planning, calling for all plans to assess the capabilities needed to meet the plan's requirements and identify any gaps. [REDACTED]

**Prior Reports**

The Department of Justice (DOJ) Office of the Inspector General (OIG) and the Government Accountability Office (GAO) have conducted several audits that are relevant to our review of the FBI's maritime terrorism efforts.

REDACTED AND UNCLASSIFIED

*Department of Justice OIG*

Since 2002, the OIG has published several reports discussing FBI counterterrorism programs and initiatives.

In September 2002, the OIG issued Audit Report 02-38, *A Review of the Federal Bureau of Investigation's Counterterrorism Program: Threat Assessment, Strategic Planning, and Resource Management*, which reviewed aspects of the FBI's management of its counterterrorism resources. This report found that the FBI had not performed a comprehensive assessment of the terrorist threat facing the United States and that the FBI has adequately established strategic priorities or effectively allocated resources to its counterterrorism program. The report made 14 recommendations to the FBI, including:

- prepare an authoritative written national-level threat and risk assessment of terrorism with a predictive and strategic view, including the potential use of WMD;
- develop criteria for evaluating and prioritizing incoming threat information for analysis, and establish a protocol to guide the distribution of threat information; and
- issue a policy on and develop a system for capturing and disseminating lessons learned from counterterrorism incidents, operations, and exercises.

In December 2003, the OIG issued Audit Report 04-10, *The Federal Bureau of Investigation's Efforts to Improve the Sharing of Intelligence and Other Information*. The focus of this audit was to identify and evaluate corrective actions taken by the FBI to improve the sharing of intelligence and other information since the September 11, 2001, terrorist attacks. The OIG made six recommendations to improve the FBI's ability to provide useful information within the FBI and to other federal, state, and local agencies. One recommendation stated the FBI should use its Concepts of Operations as a framework to establish a written policy and procedures for information sharing, including what types of information should be shared with specific parties, and under what circumstances.

In June 2005, the OIG issued Audit Report 05-27, *Review of the Terrorist Screening Center (TSC)*. The TSC was created to consolidate government watch lists of suspected terrorists, and the FBI was designated as the lead agency responsible for administering the TSC. The OIG report provided 40 recommendations to the TSC to strengthen its operations. The OIG report highlighted the TSC's need to create formal plans for automating greater outreach of threat information to particular target organizations and industries. For instance, the TSC should have a targeted maritime group with key government and private stakeholders. The OIG identified weaknesses in the consolidated watch list in the completeness and accuracy of data, and recommended that the TSC develop procedures to regularly review and test the information contained in the terrorist screening data base.

In addition, the OIG concluded that the management of the TSC call center and its staff needed improvement. The OIG recommended that the TSC establish protocols for the proper entry and review of data in the Encounter Management database and develop an automated method for flagging records in the database that require follow-up action. Likewise, the TSC needed to establish an automated method for entering call data and sharing this data with the FBI's Counterterrorism (CT) Watch to eliminate redundancy and reduce the time it takes for CT Watch to receive the data.

#### *Government Accountability Office*

The GAO has also conducted reviews of the FBI, with several reports recommending the FBI initiate risk-management techniques and performance measures.

Since 1998, the GAO has consistently advocated the use of risk-management techniques to allocate the nation's counterterrorism resources.<sup>2</sup> In 1999, the GAO further recommended that the FBI conduct a national-level assessment to combat terrorism.<sup>3</sup>

---

<sup>2</sup> Government Accountability Office. *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments* (GAO/NSIAD-98-74), April 9, 1998.

<sup>3</sup> Government Accountability Office. *Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks* (GAO/NSIAD-99-163), September 14, 1999.



In January 2005, the GAO issued *Homeland Security: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security*, which analyzes government-wide challenges in implementing counterterrorism and homeland security strategies. The report recognized that improving risk-management methods for resource allocation and investments is a challenge facing all federal departments with homeland security missions. A risk-management approach entails a continuous process of managing risk through a series of actions, including setting strategic goals and objectives, assessing risk, evaluating alternatives, selecting initiatives to undertake, and implementing and monitoring those initiatives. The report also discusses a second government-wide challenge, developing adequate performance measures for homeland security initiatives.

## FINDINGS AND RECOMMENDATIONS

### Finding 1: Maritime Initiatives

Maritime Liaison Agents (MLA), assigned to 31 of the FBI's 56 field offices and 12 of its resident agency offices, are the most visible FBI resource dedicated to maritime terrorism. MLAs are primarily responsible for coordinating with other organizations who share responsibility for security at the nation's ports, to facilitate the sharing of information on threats and security measures. However, because the MLA program is not risk-based, MLAs are not necessarily assigned to the most critical ports. As a result, field offices with multiple vital ports have only one MLA while other field offices with only minor maritime activity have multiple MLAs. The FBI's case classification system does not allow it to measure the amount of time MLAs or other agents or analysts spend preventing or investigating maritime terrorism, including related categories such as time spent on training or participating in Coast Guard-sponsored Area Maritime Security Committees (AMSC).<sup>4</sup>

Shortly after our audit began in May 2005, the CTD created a Maritime Security Program and transferred the MLA program into it. The Maritime Security Program is intended to be the focal point for the FBI's maritime efforts and is charged with coordinating the FBI's obligations and responsibilities under the National Strategy for Maritime Security and the strategy's eight implementing plans. The Maritime Security Program has 13 objectives for fiscal year (FY) 2006, many of which we believe will be beneficial and help focus the FBI's maritime-terrorism efforts. However, we are concerned that the objectives do not include critical areas such as the development of informants and threat assessments.

---

<sup>4</sup> AMSCs, mandated by the Maritime Transportation Security Act, are comprised of federal, state, and local agencies as well as representatives of the shipping and port communities. Each committee is charged with assessing its port's vulnerabilities and developing plans to meet security requirements.

## **Organization and Resources**

The FBI's CTD has primary responsibility for preventing terrorist attacks and investigating acts of terrorism after they occur. The FBI does not measure the amount of resources it devotes to preventing and investigating maritime terrorism, and there is no single entity within the CTD that is responsible for the maritime terrorism portfolio. The most visible resource dedicated to maritime terrorism is the CTD's MLA program. Other FBI components that play a major role in fighting maritime terrorism include the National Joint Terrorism Task Force (NJTTF), the CT Watch, the WMD/Countermeasures Unit, and the Special Events Management Unit.

### **Maritime Liaison Agent Program**

The FBI's NJTTF created the MLA program in 2004 as a result of Operation Dive Shop, a joint FBI-Coast Guard project in 2002 that investigated and analyzed the potential terrorist threat posed by divers and combat swimmers. The CTD's WMD/Domestic Terrorism Operations Section, which managed the FBI's involvement in the project, found that few of the FBI's local Joint Terrorism Task Forces (JTTFs) had personnel who were either trained in the maritime trade or had established regular and effective relationships with the FBI's partners at ports in their territory. This section suggested that the JTTFs designate personnel to act as liaisons with law enforcement and non-law enforcement personnel at seaports.

In response to the suggestion from the WMD/Domestic Terrorism Operations Section, the NJTTF reviewed the FBI's efforts to prevent terrorism in the maritime domain and found the following.

- Some field offices with major ports (Baltimore, Long Beach, and Miami, for example) had personnel knowledgeable about the maritime domain and had used them to establish good relationships with relevant agencies in their ports.
- Some JTTFs had personnel qualified to act as liaisons to the maritime community, but many JTTFs were not using them for that purpose.
- Many FBI special agents in charge were participating in port security committees.

## REDACTED AND UNCLASSIFIED

- The FBI did not have any training for agents who worked at seaports or special agents in charge who participated in port security committees.

The MLA program formally began in July 2004 when the NJTTF sent an electronic communication (EC) to all field offices requesting that those field offices with major waterways in their territory name personnel to be assigned to the MLA program. In the EC announcing the MLA program, the NJTTF outlined the need for the program, its goal, its anticipated results, and an MLA's duties. The NJTTF stated that it had determined that the "maritime threat and terrorism-related intelligence could best be coordinated and disseminated to concerned entities through the adoption of the MLA program." The NJTTF also said the program's goal was to enhance the security of the maritime environment through increased interaction between MLAs and the FBI's maritime partners. The NJTTF envisioned that this increased interaction would "decrease response time to actionable intelligence and operational tasking by capitalizing on matured relationships."

According to the July 2004 EC, the new MLAs were to work full- or part-time to establish and maintain relationships with representatives of "maritime institutions" in their respective geographical areas. MLAs were to be in regular contact with maritime specialists at the NJTTF to allow for increased information sharing. By centralizing the FBI's maritime counterterrorism efforts, the NJTTF believed that it would create consistency in MLA job responsibilities, training, and reporting procedures. With the help of field offices that had already established maritime programs, the NJTTF identified the following MLA duties.

- Contact each of the entities below and identify a point of contact for security matters.
  - Area Maritime Security Committee
  - Anti-Terrorism Advisory Council
  - Coast Guard Investigative Service
  - Coast Guard Captain of the Port or Group Commander
  - Coast Guard Marine Safety Office
  - Coast Guard Field Intelligence Support Team
  - CBP — Operations
  - CBP — Intelligence

## REDACTED AND UNCLASSIFIED

- County/Local Emergency Operations
  - Ferry Security Director
  - Fire Department
  - Harbor Master
  - Harbor Patrol/Police
  - Regional Office of U.S. Immigration and Customs Enforcement
  - Local Police with Maritime Authority
  - Port Engineers
  - Passenger Ship Terminal Security
  - Regional Office of Navy Criminal Investigative Service
  - State Homeland Security Advisor
  - State Natural Resource/Fish and Game Police
  - State/Local Pilots Association
  - Significant Industry, including petrochemical industry
  - Regional Office of the Transportation Security Administration
  - U.S. Army Corps of Engineers, Homeland Security Regional Office
  - U.S. Attorneys Office
  - U.S. Park Police
  - Waterfront Commission
- Identify locations where secure databases may be accessed.
  - Establish 24-hour emergency contact lists for maritime resources, contacts, and agencies.
  - Research establishing e-mail groups to facilitate information sharing between maritime liaisons.
  - Review existing maritime initiatives for potential enhancements.<sup>5</sup>

The CTD managers with whom we spoke agreed that MLAs should not be involved with port security activities such as enforcing regulations. MLAs should establish relationships in their ports that allow the FBI to immediately receive and transmit information concerning ports, merchants, vessels, and cruise lines. However, the MLA position is broader than that of a liaison: an MLA should be the

---

<sup>5</sup> The NJTTF was to use this information to identify and disseminate best practices.

FBI field office's maritime expert. According to a CTD Deputy Assistant Director, this expertise, coupled with knowledge of the local port, should provide each field office with "situational awareness." Regardless of whatever event happens at a port, an MLA should know the port's procedures, protocols, and schedules and have relationships with key organizations to aid the FBI in resolving the event. In our judgment, the CTD managers' understanding of the role of the MLA is significantly more encompassing and outcome-based than the duties outlined in official guidance.

### **MLA Program Not Risk-Based**

Prior to developing the requirements for the MLA program, the NJTTF did not perform or review a risk assessment to identify the level of resources each field office, including resident agencies, should devote to maritime issues. Instead, each field office was given the discretion to:

- define major waterways in its territory;
- name one MLA for its entire territory, regardless of the number or size of the ports; and
- determine whether its MLA(s) would be full- or part-time.

In recent years, audit organizations, Congress (most recently through the Intelligence Reform and Terrorism Prevention Act of 2004), the Executive Branch through presidential directives, and the 9/11 Commission have required or advocated that federal agencies with homeland security responsibilities employ a risk-management approach to help ensure that finite resources are allocated to those programs and critical geographic areas where they will have the most impact. Without a risk-management approach, there is limited assurance that programs designed to combat terrorism are properly prioritized and focused. Applying risk-management techniques to the FBI's counterterrorism program can help assure it allocates resources effectively and efficiently to counter terrorist threats.

According to the GAO, risk assessment is a critical element of risk management. A risk assessment helps managers identify and evaluate potential risks so that countermeasures can be designed and implemented to prevent or mitigate the effects of the risks. Risk

## REDACTED AND UNCLASSIFIED

assessments can be qualitative or quantitative. Regardless, they determine the likelihood of an adverse event occurring and the severity of the consequences. When applied to counterterrorism, risk assessments often involve three elements: threat, criticality, and vulnerability.<sup>6</sup>

- A threat assessment identifies and evaluates potential threats on the basis of factors such as capabilities, intentions, and past activities.
- A criticality or consequence assessment evaluates and prioritizes assets and functions in terms of specific criteria, such as their importance to public safety and the economy as a basis for identifying which structures or processes are relatively more important to protect from attack.
- A vulnerability assessment identifies weaknesses that may be exploited by identified threats and suggests options to address those weaknesses.

A risk assessment would be useful in determining the amount of resources the FBI should devote to maritime terrorism and where it should locate those resources. However, the FBI has not conducted a risk assessment and therefore does not know whether it has allocated its resources in a manner that will achieve the MLA program's objectives.

As of October 2005, field office managers in 43 of the FBI's 56 field offices had named MLAs either at their field office, one or more of their resident agencies, or both. Because the MLA program is not risk-based, some offices with several significant ports in their territory have named only one MLA, and offices with no strategic ports have named multiple MLAs. For example, the New Orleans field office, with only one MLA, has six significant ports in its territory. In comparison, the Louisville field office has no strategic ports in its area but designated five MLAs, two in the field office, and one each in three of its resident agencies.

---

<sup>6</sup> Testimony before the Senate Committee on Commerce, Science, and Transportation. *Transportation Security: Systematic Planning Needed to Optimize Resources* (GAO-05-357T), February 15, 2005.

Twelve of the remaining 13 field offices have not named MLAs because they determined they do not have any navigable waterways in their territory. We analyzed the territory of these 12 field offices and found that their maritime responsibilities vary from not having any ports to having significant ports. For example, we found that the Jackson, Mississippi, field office's territory includes three significant ports. In 2003, the Bureau of Transportation Statistics ranked Pascagoula, Mississippi, 17th among the nation's 361 ports in terms of the tonnage of products shipped. As the result of a risk-based assessment, in Mississippi the DHS selected Greenville, Pascagoula, and Vicksburg as 3 of the 66 ports eligible to apply for a 2005 Port Security Grant. The 13th field office, Milwaukee, did not respond to the EC asking field offices to name MLAs. However, the Port of Milwaukee met the DHS's risk-based criteria for eligibility to apply for a 2005 Port Security Grant.

### **Some Risk Data Is Available**

While the FBI did not base the MLA program on a risk assessment of the nation's ports, publicly available data provides some insight into which of the nation's ports face the greatest risk. For example, the Bureau of Transportation Statistics publishes data on the nation's largest seaports, both in terms of value and tonnage. Furthermore, in FY 2005, the DHS allowed only the most at-risk seaports to apply for Port Security Grants.<sup>7</sup> In that program, the DHS evaluated the nation's 129 largest-volume ports using the following risk formula: Risk = Consequence x Vulnerability x Threat.

The consequence risk factor considered the number of people, economic, and national security impacts, and port-specific considerations such as oil and hazardous materials. The vulnerability risk factor considered the following data: the distance from open water, the number of port calls, and the presence of tankers. Data for the threat risk factor included credible threats and incidents reported by the intelligence community, operational indicators such as less credible threats and incidents, and vessels of interest. Based on its

---

<sup>7</sup> According to the DHS, its FY 2005 Port Security Grants provided \$150 million to provide protection against small craft, underwater attacks and vehicle borne improvised explosive devices, enhanced explosives detection capabilities for the owners and operators of vehicle ferries and associated facilities, and facility security enhancements to the highest risk ports.



risk-based evaluation, the DHS identified 66 ports for eligibility in the 2005 Port Security Grant program.

Thirty-five FBI field offices have at least 1 port in their territory that is either a top 20 port by value or volume or was eligible to apply for a 2005 Port Security Grant. However, as shown in Appendix III, much of the maritime activity and risk of maritime terrorism is concentrated in the territory of 24 FBI field offices. Those 24 field offices are responsible for all of the top 20 ports and 83 percent of the port areas eligible to apply for FY 2005 Port Security Grants.

In our judgment, the FBI's resources should be focused on the areas that face the greatest risk of terrorist attack. Counterterrorism Division managers agreed that the MLA program should be strategically driven and said that resources should be allocated based on a port's law enforcement need, unique challenges and assets, and threat assessments.

### **FBI Does Not Measure Efforts to Prevent Maritime Terrorism**

The FBI does not have a method of tracking the amount of time its agents spend preventing or investigating maritime terrorism. Currently, under the FBI's case classification system, most MLA activities are designated as "Counterterrorism Preparedness – Other." This classification is not specific enough to allow managers of the FBI's maritime efforts to determine the amount of resources the FBI is spending maritime issues. For the FBI to implement a risk-based counterterrorism program, its managers must know the amount of resources it devotes to each type of its counterterrorism initiatives. According to NJTTF personnel responsible for the MLA program, the FBI should collect data on subcategories of the FBI's maritime efforts including the following.

- Attend Operational Maritime Training
- Conduct Operational Maritime Training/Presentation
- Positive Maritime-Related Terrorism Disseminated Within the FBI
- Positive Maritime-Related Terrorism Disseminated Outside the FBI

## REDACTED AND UNCLASSIFIED

- Participate as Member of an Area Maritime Security Working Group/Task Force
- Participate in Maritime Command Post/Major Case/Special Event
- Participate in Development of Maritime Operational Plan
- Participate in Maritime Field Training Exercise
- Participate in a Maritime Table Top Exercise
- Maritime Investigative/Response/Assistance Provided to Local/State/Federal Agency
- Tactical Maritime Response/Assistance Provided to Local/State/Federal Agency
- Maritime Counterterrorism Response/Preparedness Contact Developed
- Maritime-Related Liaison

We agree with the NJTTF about the FBI's need to collect data by subcategory. As part of our audit, we asked the FBI for data on many of these categories including: (1) training, (2) Area Maritime Security Committees, (3) maritime exercises, and (4) maritime responses. FBI officials could not provide this data and instead had to use other methods such as personal recollection to provide general answers to these questions. One method to measure the amount of resources devoted to maritime issues would be to create sub-classifications within the Counterterrorism Preparedness classification. These new classifications would also allow FBI personnel to record accomplishments that occur in the maritime domain.

### *Training*

While the FBI was not able to provide us with complete data on the training its MLAs or other personnel have attended, either as a student or instructor, the NJTTF provided a course to MLAs in 2004. According to FBI officials, the purpose of the course was to introduce new MLAs to issues specific to preventing terrorism at the nation's

seaports and to allow MLAs with maritime experience to discuss best practices. FBI officials said approximately 40 MLAs attended the 4-day class, which covered legal issues (including the Coast Guard's authority), port-related infrastructure, boarding procedures, and vessel safety. Personnel from the Coast Guard Investigative Service, which the FBI identified as the organization most capable to teach the course, taught most of the class. The NJTTF scheduled another training session for July 2005. However, this conference was cancelled when the CTD did not approve the necessary funding. The responsible CTD manager said requests for training throughout CTD exceeded the division's training budget, which was reduced by \$1 million as the result of reprogramming to help fund the development of the FBI's Sentinel case management system.

#### *Area Maritime Security Committees*

In written testimony for the Senate Judiciary Committee's Subcommittee on Terrorism, Technology, and Homeland Security on January 27, 2004, the FBI's Acting Assistant Director for Counterterrorism testified that the FBI is a full participant in the Coast Guard's Area Maritime Security Committees (AMSC). These committees, which were mandated by the Maritime Transportation Security Act, are comprised of federal, state, and local agencies as well as representatives of the shipping and port communities. Each committee is charged with assessing its port's vulnerabilities and developing plans to meet security requirements. The FBI's Acting Assistant Director for Counterterrorism further explained that AMSCs and their predecessor committees offered the FBI an opportunity to provide threat analysis and disseminate intelligence.

The CTD does not track field offices' participation in AMSCs or collect any data on FBI participation in AMSCs, so it does not know the amount of resources (in terms of hours) the FBI devotes to AMSCs. Participation in AMSCs is left to the discretion of field office managers. However, at our request the FBI collected data on the number, location, and position of its AMSC representatives. Twenty-six FBI field offices and 13 resident agencies reported having representatives on AMSCs.<sup>8</sup> The number of representatives and their position varies by field office. For example, the special agents in charge of three field

---

<sup>8</sup> Three offices that reported to the MLA coordinator at headquarters that they did not have any navigable waterways in their territory — Cincinnati, Indianapolis, and Jackson — reported having AMSC representatives.

offices — Mobile, San Diego, and San Francisco — reported participating in their local AMSCs. In comparison, the Chicago field office reported that its sole representative was a Coast Guard Investigative Service agent assigned to its JTTF. As shown in the following table, the majority of the FBI's 67 AMSC representatives are special agents or supervisory special agents.

**FBI Representation on  
Area Maritime Security Committees**

<b>Position</b>	<b>Number of Representatives</b>
Special Agent, including Supervisory Special Agent	47
Assistant Special Agent in Charge	6
Supervisory Senior Resident Agent	4
Intelligence Analyst, including Senior Intelligence Analyst	4
Special Agent in Charge	3
JTTF Agent	2
Computer Scientist	1
<b>Total</b>	<b>67</b>

Source: OIG analysis of FBI data

While AMSCs offer the FBI an opportunity to provide threat analysis and disseminate intelligence to maritime partners, participation in an AMSC is not one of the critical duties identified for MLAs. Instead, MLAs were directed to contact their AMSC and identify a point of contact for security matters. While AMSC participation is not required, we found that 25 of the 73 MLAs (34 percent) participate in an AMSC. Of those 25, 6 are on the executive committee or chair a subcommittee.

AMSCs vary widely in size, with some AMSCs having subcommittees and executive committees. According to January 2004 Coast Guard data, AMSCs ranged in size from 9 members and no subcommittees to 446 members including 9 subcommittees. The San Diego field office reported having the most AMSC representatives, seven, including representatives on the executive committee and three subcommittees. Of the 39 field offices and resident agencies that reported having AMSC representatives, 13 (33 percent) reported they

had a representative on an AMSC executive committee. These 13 offices reported having a total of 18 representatives, 39 percent of which were assistant special agents in charge or special agents in charge.

### **Maritime Security Program**

In July 2005, after our audit began, the FBI established a Maritime Security Program within the CTD's Special Events Management Unit and transferred responsibility for the management of the MLA program to the Maritime Security Program. CTD officials said the Maritime Security Program is modeled after the Special Events Management Unit's Civil Aviation Security Program, which was created in the 1990s and includes 530 airport liaison agents. The Civil Aviation Security Program offers a number of practices which may be transferable to the new Maritime Security Program:

- The Civil Aviation Security Program is risk-based according to FAA criteria, and Airport Liaison Agents are required at high-risk airports.
- The FBI participates in joint Transportation Security Administration/FBI threat and vulnerability assessments of individual airports.
- The Civil Aviation Security Program tracks aviation-related suspicious activity and disseminates the results within the FBI and intelligence partners.

Because the Maritime Security Program is a recent initiative, we could not fully assess its impact. We found that the goals and purposes of the Maritime Security Program are not yet clear. The CTD established the Maritime Security Program to coordinate the FBI's obligations and responsibilities under the National Strategy for Maritime Security. However, the Maritime Security Program's stated mission is much broader: prevent, disrupt and defeat terrorism directed against maritime targets and take a leadership role in counterterrorism preparedness by assisting federal, state, and local agencies responsible for maritime security.

According to an August 2005 EC outlining the Maritime Security Program's goals and objectives, the program aims to enhance the

## REDACTED AND UNCLASSIFIED

FBI's ability to prevent and disrupt terrorism by developing a detailed knowledge of operational and policy matters affecting seaports and the maritime domain. The Maritime Security Program plans to achieve this knowledge by developing informants, distributing intelligence, assisting in investigations, conducting threat and vulnerability assessments, and developing or enhancing relationships with law enforcement and intelligence partners. The Maritime Security Program established three goals, each with objectives intended to measure progress toward meeting the goal:

- utilize available resources to provide maximum assistance to the MLAs;
- identify, analyze, and disseminate information pertaining to maritime threats, vulnerabilities, and safety or security issues; and
- establish and maintain liaison with federal, state and local law enforcement, the intelligence community, and the maritime industry.

In addition to the 13 objectives supporting the program's 3 goals, the Maritime Security Program also developed 4 "recommended objectives" for FBI field offices. We believe the initiative behind several of the objectives shows that the FBI's maritime efforts are maturing. Specifically, during FY 2006 the Maritime Security Program plans to complete the transfer of the MLA program from the NJTTF to the Maritime Security Program, thereby placing all of the FBI's transportation-related counterterrorism programs in the same organizational unit. In addition, the MSP has recognized the general principals of risk management and has planned at least one future initiative accordingly. Based on a broad understanding of threat and criticality, the Maritime Security Program identified 10 major U.S. transportation hubs, metropolitan areas that contain both a major seaport and a major airport. The Maritime Security Program plans to visit 30 percent of these hubs in FY 2006. Each of these 10 hubs is in the territory of one of the 24 field offices listed in Appendix III.

The Maritime Security Program also plans to create a website on the FBI's Intranet, allowing the Maritime Security Program to disseminate intelligence, security directives, training materials, and points of contact. In addition, the Maritime Security Program plans to

review maritime-related suspicious activity reports and identify any trends that may be indicative of pre-operational planning. We believe the collection and analysis of suspicious activity reporting is a critical undertaking. Until the FBI's suspicious activity tracking system, discussed in Finding 3, has sufficient search capabilities to easily identify maritime-related threats and suspicious activity, it may be appropriate for the Maritime Security Program to review and report on such activity.

Lastly, the Maritime Security Program has asked field offices to name an FBI special agent or supervisory special agent as primary MLA. Currently, 32 percent of all MLAs are not FBI personnel but are personnel from other agencies assigned to one of the FBI's JTTFs. For example, 19 percent of MLAs are Coast Guard Investigative Service agents.

While we believe a number of the initiatives listed as objectives are positive developments, none of the objectives are phrased in a manner that allows the FBI to measure the outcome of its efforts. For example, one objective under the first goal is, "Develop and provide basic training and reference materials to assist the MLAs." This objective does not measure the output — the number of MLAs trained — or the outcome — the number of MLAs capable of effectively boarding a vessel.

While the CTD initiated the Maritime Security Program to coordinate the FBI's response to the National Strategy for Maritime Security, and the Maritime Security Program lists that role as an objective, we found that the Maritime Security Program has not reviewed the strategy's eight implementing plans to identify the FBI's responsibilities. Nor has the Maritime Security Program identified all of the FBI's representatives to the different working groups charged with implementing the plans.

According to Maritime Security Program planning documents, the Maritime Security Program will rely on the skills the FBI already has, including its ability to develop relationships with informants and other people who can provide substantive information to aid FBI investigations. The MSP plans to use this ability to develop sources of information to provide the FBI with a detailed knowledge of the operations at the nation's seaports. However, neither the Maritime Security Program's FY 2006 goals and objectives nor the critical duties

of an MLA include the need for the FBI to develop relationships with people who can inform the FBI about maritime operations. Also, the Maritime Security Program has not taken any steps to review the FBI's current human intelligence base to identify current informants who may be able to provide information on maritime terrorism.

The MLA program and the Maritime Security Program were both formed to aid in rapidly disseminating information. In our judgment, developing and maintaining a current roster of MLAs is vital to this capability. Responding to our request for a list of AMSC representatives, FBI field offices named seven personnel as MLAs that were not on the Maritime Security Program's latest list of MLAs.

### **Conclusion**

The FBI has limited resources, so it should ensure that the amount of resources devoted to maritime terrorism is measurable and allocated among its many counterterrorism programs according to threat and risk. Within the maritime arena, the FBI needs to ensure that ports facing the greatest risk receive the largest amount of resources. For example, the number of MLAs assigned to a field office or a resident agency should be proportionate to the risk of maritime terrorism faced by the ports in its territory.

The MLA position is relatively new and appears to be evolving. The recent transfer of the MLAs to the Maritime Security Program presents an opportunity for the FBI to reevaluate MLA roles and responsibilities. We believe that MLAs should focus on the FBI's strengths by recruiting informants and aiding in threat and vulnerability assessments. The FBI should ensure that the Maritime Security Program develops measurable annual objectives to allow it to assess the program's progress.

### **Recommendations**

We recommend that the FBI:

1. Ensure that MLA guidance is consistent with the actual role of MLAs.
2. Assign MLAs based on an assessment of the threat and risk of a terrorist attack to critical seaports.



REDACTED AND UNCLASSIFIED

3. Measure the amount of resources devoted to maritime efforts by establishing a maritime case classification under the general Counterterrorism Preparedness classification.
4. Require field offices to name at least one MLA to each AMSC.
5. Require field offices to immediately notify the Maritime Security Program of any MLA appointments or reassignments.
6. Ensure that the Maritime Security Program has measurable objectives.
7. Ensure that the Maritime Security Program's objectives include developing human intelligence.

**Finding 2: Maritime Response Capability**

Response to terrorist threats or incidents in the maritime domain presents unique challenges to the FBI and any other responding agency. FBI SWAT teams, Hostage Rescue Team (HRT), and Hazardous Devices Response Unit (HDRU) may all be involved in responding to a maritime-based terrorist attack. The Coast Guard also has significant responsibility for enforcing U.S. laws in the maritime domain, a role that received an added terrorism component with the passage of the Maritime Transportation Security Act of 2002. Officials at the FBI and the Coast Guard agreed that the Act may have created some overlapping responsibilities between the two agencies. Officials from both agencies also agreed that the Maritime Operational Threat Response (MOTR) plan, one of the plans supporting the implementation of the National Strategy for Maritime Security, should resolve any such issues. However, the MOTR issued in October 2005 is an interim plan, which FBI officials say does not clearly delineate the roles of the Coast Guard and the FBI and therefore raises concern about potential confusion over authorities and incident command in the event of a terrorist attack in the maritime domain.

**Field Office SWAT Teams**

Each of the FBI's 56 field offices has a SWAT team, and the teams receive basic training in areas that are useful for operating in the maritime domain including water safety, limited climbing techniques, and exposure to close quarters battle tactics. Some teams receive somewhat more training and equipment than others, but all have a limited maritime capability in comparison to the FBI's HRT, discussed in more detail below. In September 2005, in an effort to enhance joint FBI/Coast Guard tactical efforts, the FBI created 14 enhanced maritime SWAT teams, nearly all of which are located in the FBI field office closest to one of the Coast Guard's 13 Maritime Safety and Security Teams (MSST). The enhanced maritime SWAT teams are to receive additional maritime training and maritime equipment. The additional training will provide the 14 SWAT teams with a limited maritime capability for emergency purposes and allow those teams to work effectively with the MSSTs. The enhanced maritime training will focus primarily on water safety techniques and the unique aspects of tactical operations in the maritime arena.

Upon notification of an imminent maritime threat or incident, an FBI special agent in charge can dispatch a local field office's SWAT team. After responding to the incident, the SWAT team and FBI field office management will assess the situation and determine if they have the capability to deal with the threat. According to FBI officials, assaulting a vessel containing terrorists who oppose the boarding poses unique challenges for the assaulting force and most FBI SWAT teams do not have the capability to overcome these challenges. First, the team must board the vessel. Second, the team must navigate and fight its way to strategic locations on the vessel. According to officials of the FBI's Critical Incident Response Group (CIRG), most FBI SWAT teams do not possess the skills and equipment needed to accomplish these tasks.<sup>9</sup>

According to FBI officials, an FBI SWAT team has two methods of assaulting a ship that is docked. The assaulting team can either use the gang plank or "hook and climb," a technique in which a grappling hook attached to a flexible wire ladder is thrown onto the side of a ship and the assault team climbs the ladder to get on deck. The hook and climb method can also be used on vessels that are adrift. However, the SWAT team needs a boat to reach the target vessel. Under extreme circumstances, a SWAT team could use the hook and climb technique to assault a moving ship. Because the hook and climb technique requires a boat, 13 FBI field offices have obtained between one and four boats each. Without its own boats, these SWAT teams would have to rely on the Coast Guard for transport to an incident.

---

<sup>9</sup> The FBI formed the Critical Incident Response Group in 1994 to facilitate the FBI's rapid response to and management of crisis incidents.

## FBI SWAT Team Hooks and Climbs During an Exercise



Source: OIG photo

Some FBI officials have expressed concern about FBI SWAT teams' reliance on the Coast Guard for transport to an incident. Their concerns focused on the need for a SWAT team to practice as a unit, using the same boats and the same boat pilots it would use during an actual incident. FBI officials said that not all boats are suitable for a tactical assault. Ideally, assault boats are fast, are painted a plain color, and give the pilot an unobstructed view in all directions. For example, the Baltimore field office boat shown in the previous photograph has a top speed of 45 knots, is painted gray, and has an open cockpit.

However, the purchase and maintenance of boats is an expense that each field office must bear using its discretionary funds. Because field offices must bear the expense of any boat, there is no uniformity in the distribution of the boats, and there are no readiness standards to determine maintenance intervals. For example, the Baltimore field

office has three boats, all of which were provided at no cost from the Coast Guard, which was discarding them as surplus. During training we observed, the Baltimore boats had several mechanical problems. As a result, one boat could not run at full speed.

### **Hostage Rescue Team**

The FBI's HRT is the FBI's most capable and best-equipped counterterrorism team. The HRT is the FBI's only tactical team with full maritime capabilities. Created in 1982, the HRT is trained to rescue U.S. citizens or others who may be held illegally by a hostile force, either terrorist or criminal. In the years it has been operational, the HRT has never responded to an incident in the maritime domain. The HRT is a full-time assignment, its members are trained in the methods and tactics that will be used in responding to a terrorist incident in the maritime domain.

#### *HRT Capabilities*

The HRT's equipment and tactics are more advanced than the FBI's field office SWAT teams. The HRT's capabilities are also more advanced because its operators (assault and sniper teams) serve full-time and train daily. HRT operators are assigned to one of three teams, one of which is a designated maritime team. The three teams rotate through three 60-day cycles: training, operations, and support. During the training cycle, the team refreshes its skills and takes part in exercises. During the operations cycle, the team is available for deployment. During the support cycle, the team works on special projects and maintains the HRT's equipment.

One of the chief capabilities that distinguishes the HRT from the FBI's SWAT teams is its ability to "fast rope," a technique where the assault team rappels from a helicopter. This technique is particularly useful for assaulting a maritime target because it allows the FBI to rapidly place a team aboard either a stationary or moving vessel. However, this advanced skill requires great coordination between the helicopter pilots and the assault teams, thus making it practical only for a full-time team.

## The HRT Fast Roping During an Exercise



Source: OIG photo

In addition to fast roping, the HRT also possesses additional capabilities in the maritime domain, including advanced “breaching” capabilities — the ability to circumvent locked doors aboard a ship — and shipboarding capabilities. The HRT has three boats outfitted for maritime assaults, most of which have been upgraded since 2004. The HRT’s boats are similar in size to Baltimore’s boats, but their engines are twice as powerful.

The HRT also has a maritime team, which has additional maritime capabilities, including subsurface diving, closed-circuit diving (scuba gear that does not emit bubbles), and combat swimming. All operators on the maritime team are military trained in closed-circuit diving and combat swimming. In addition, the maritime team assault element has an operator who is qualified to pilot a freighter.

HRT officials said the team's ability to respond to a maritime incident is unparalleled in the federal law enforcement community because it trains nearly continuously with helicopter-based assaults in a variety of environments, including low light, no light, and onto oil rigs. HRT officials said that while the team may not constantly train directly in the maritime arena, it conducts exercises weekly that build the skills needed for the maritime environment, such as close-quarters battle, room entry, helicopter piloting, and fast roping. HRT officials do not believe there is a need to be on the water in order to prepare for incidents in the maritime domain. For example, they said that the same principals for close-quarters battle that apply on land also apply aboard a vessel at sea. HRT officials said that the biggest difference in a maritime assault, compared to land, is how the team is delivered to an incident. Once at the site, the team uses the same procedures and tactics it would on land.

In addition to training, the HRT also conducts research on targets of terrorist attacks and develops methods to overcome any challenges posed by these targets. For example, the HRT is constantly doing research on how aircraft and ship doors work and how they can most effectively be breached.

### **Hazardous Devices Response Unit**

Established in 2004, the FBI's Hazardous Devices Response Unit is responsible for successfully resolving an incident involving a WMD, including incidents that occur on board ships. The mission of the HDRU is to provide technical response teams to find the WMD device, gain access to the device, and diffuse it. Two FBI officials, the Director and the Executive Assistant Director for Counterterrorism and Counterintelligence, have the authority to order the HDRU to deploy.

The FBI's approach to WMD incidents is similar to its approach to other tactical responses: personnel from FBI field offices are the first responders, and national level assets respond only when the incident exceeds local response capabilities. The FBI's field offices have over 140 agents who have been trained as bomb technicians. These technicians are typically the FBI's first responder to any incident that may involve a WMD. If a bomb technician decides the incident exceeds local capabilities, the field office coordinates with FBI headquarters to arrange for the HDRU to deploy. Deployment of the HDRU may also be intelligence driven. If the FBI becomes aware of a

REDACTED AND UNCLASSIFIED

terrorist threat that may involve a WMD, the FBI coordinates with the National Security Council and the affected FBI field office to deploy the HDRU. Once a WMD incident is resolved, (that is, the device is rendered safe), teams from the Departments of Defense and Energy are responsible for disposing of the device.

Because Customs and Border Protection is responsible for inspecting cargo that enters the United States, its inspectors are often the first to encounter cargo that may potentially include a WMD. According to CBP and FBI officials, an alarm by a radiation sensor is the most common terrorism-related suspicious incident CBP inspectors encounter at seaports. CBP inspectors have been directed to resolve all radiation alarms. Often inspectors can resolve the alarms themselves by using a vessel's manifest and other shipping documents to identify legitimate cargo that emits radiation. If the inspectors cannot identify legitimate cargo that is the source of the radiation, they use other CBP resources to attempt to identify the radiation source. If these resources do not allow the inspectors to identify the source, the CBP contacts the FBI or the DHS, Immigration and Customs Enforcement. If CBP can exclude any potential link to terrorism or threat to the United States, it refers the incident to the Immigration and Customs Enforcement. However, if CBP cannot exclude terrorism, it contacts the FBI for assistance.

Both FBI and CBP officials had positive views about the two agencies' coordination in responding to potential WMD incidents at seaports. They said the coordination required between the two agencies centers on intelligence sharing and notification in the event of a threat or incidents. Officials from both agencies attributed the high level of coordination primarily to the distinct roles of the two agencies. Officials from both agencies agreed that CBP's role is primarily inspections and the FBI's is primarily investigation. CBP and FBI officials also agreed that the 31 CBP representatives in the FBI's JTTFs helped increase coordination at the local level. Officials from both agencies could not remember an incident in which there was any confusion about the role of the two agencies, nor could they recall any joint responses where there were any incident command conflicts between CBP and the FBI.

HDRU officials said the maritime domain presents unique challenges for resolving a potential WMD incident. Aside from the challenges of delivering the HDRU team and its equipment to a ship in



## REDACTED AND UNCLASSIFIED

open waters, HDRU officials said the logistics of searching a ship and the limitations of nuclear detection equipment were the two primary challenges.

Container ships are difficult to search. For example, in September 2002, the HDRU's predecessor responded to an incident aboard the container ship *Palermo Senator*. The Coast Guard had diverted the *Palermo Senator* to Elizabeth, New Jersey, after radiation was detected aboard the ship. The Coast Guard, the Port Authority of New York and New Jersey, the Department of Energy, and the FBI's Newark field office all responded to the incident. The National Security Council asked the Department of Defense to send a WMD team. The HDRU's assignment was to search the ship and identify the source of the radiation. Once inside the ship, the HDRU team found the vessel very difficult to search because there were 1,200 metal shipping containers stacked one on top of another, both above and below deck. The search took about a day, and the team did not find anything dangerous or locate the source of the radiation initially detected.

If the team would have located a radiation source deep within the stacks of containers, it would have been difficult for the team to access the problem container. Starting with the accessible container closest to the one emitting radioactivity, the team would have had to repeat the following process until it reached the target container: cut into the accessible side of the container, empty its contents, and cut out the opposite side. HDRU officials said they regularly practice cutting shipping containers to be ready for this type of emergency. Searching vessels is also difficult because many commonly shipped products, especially in large amounts, can give off radiation in detectable amounts. For example, large amounts of cocoa powder produce a detectable amount of radiation.

Nuclear detection equipment has limitations. The HDRU's equipment cannot detect every type of nuclear device that could be placed within a ship's cargo hold. Nuclear devices can be shielded in an effort to avoid detection, and thus the HDRU's detection equipment will not identify it. Even after a thorough search of a ship with its detection equipment, the HDRU cannot guarantee that a ship does not contain a nuclear device. This lack of certainty does not provide FBI managers or other responsible officials with much comfort. For example, during the *Palermo Senator* incident, the special agent in charge of the Newark field office wanted to be absolutely certain that

none of the containers on board the ship contained a nuclear device, but the HDRU could not give him that assurance. HDRU officials also said the only way to attain that certainty would be to open and inspect the contents of every container on the ship. HDRU officials said the most likely method for conducting such a search would involve using a crane to remove the containers and individually searching them. This method is time consuming, likely taking weeks to complete, and presents additional challenges. For example, officials are unlikely to want to keep a ship in port that is suspected of having a WMD aboard. It would take a second ship and special equipment to perform this kind of search at sea.

### **Capability-Based Planning**

The HRT has not fully assessed the capabilities it needs to counter threats or incidents in the maritime domain. The MOTR calls for the Departments of Defense, Homeland Security, and Justice to develop a plan to provide an immediate and "deliberate" response to maritime threats, including multiple simultaneous attacks. The FBI has not assessed the terrorism scenarios most likely to occur in the maritime domain or the required time for a tactical response to resolve those scenarios.



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

10 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

HRT's plans call for it to deploy on its own within a 600-mile radius of the National Capital Region. The HRT official said that the range of the current HRT helicopters is limited, which affects the range in which the team can self-deploy.

### **Maritime Operational Threat Response Plan**

The Maritime Operational Threat Response is one of eight implementing plans detailing how the U.S. government will develop the capabilities needed to fulfill the National Strategy for Maritime Security. The MOTR describes the government's plan to respond to terrorist threats in the maritime domain, including the roles of the different federal agencies, protocols for lead and supporting agencies, and the need for additional planning. It calls for specific operating plans outlining how lead agencies will fulfill their responsibilities. The MOTR endorses capability-based planning, calling for all plans to assess the capabilities needed to meet the plan's requirements and identify any gaps.

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



The plans are intended to ensure that MOTR agencies have the capability to operate as a team "against the spectrum of expected security threats." To achieve this, the MOTR calls for security forces to have a high degree of interoperability, reinforced by joint interagency training and exercises.

We believe that the MOTR's efforts to clearly delineate the roles of the FBI and the Coast Guard in responding to terrorist threats and incidents help meet an existing policy void. Officials at the FBI and the Coast Guard both agreed that the MTSA may have created some overlapping responsibilities. At the headquarters level, we found that the FBI and the Coast Guard both want the ability to respond to terrorist threats in the maritime arena. FBI officials said they were unsure of the MSSTs' mission and capabilities. They also said that planned enhancements to the Coast Guard's tactical capability are redundant and may result in reduced funding for the FBI, thereby weakening its currently tactical capabilities. We are also concerned that any competition for funding could erode interagency cooperation. We found indications that the relationship between the FBI and the Coast Guard may already be strained. Early in 2005, as part of its efforts to develop its tactical response teams, Coast Guard and FBI officials met, and the Coast Guard requested further information on the selection criteria the FBI uses for SWAT teams and the HRT. The FBI responded to the Coast Guard's written request by stating that that the FBI would not be able to assist the Coast Guard until the two agencies' roles in responding to terrorist threats and incidents had been clearly defined and "are not competing for the same resources."

The Coast Guard and the FBI also have different opinions about the level of cooperation between the two agencies at TOPOFF 3, a DHS-sponsored exercise to assess the nation's capacity for preparing for and responding to terrorist attacks involving WMD. HRT representatives said the exercise showed the two agencies' ability to respond in a coordinated fashion. The HRT took part in one of the incidents of the exercise, a scenario that called for the team to assault a 200-foot moving ferry off the coast of Connecticut. A boat and

helicopters were used to transport the team to the ferry. The Coast Guard supported the HRT in the TOPOFF 3 exercise by providing search and rescue services. According to FBI officials, the Coast Guard could not participate in the boarding because it has a very limited capability to perform boardings when its boarding team faces armed resistance. FBI officials also noted that the Coast Guard does not train its personnel to board vessels that are underway.

Coast Guard officials disagreed with the FBI's analysis of TOPOFF 3, saying that the FBI guarded its territory as the lead federal agency for terrorism. One of the Coast Guard's goals for TOPOFF 3 was to exercise its new tactical assault team, called an Enhanced Maritime Safety and Security Team. However, Coast Guard officials said the FBI repeatedly blocked the Coast Guard's efforts, saying the FBI was the lead federal agency in the scenarios developed. The Coast Guard ultimately changed the scenario to circumvent the FBI's lead federal agency role.

Prior to the release of the MOTR, officials from both the FBI and the Coast Guard agreed that the MOTR should resolve jurisdictional issues. However, the MOTR issued in October 2005 is an interim plan, which FBI officials say does not define the roles of the FBI and the Coast Guard as clearly as they would like. They said they will work with the interagency Maritime Security Working Group to ensure that the final version of the MOTR more clearly articulates the respective roles and authorities of each agency. The FBI is concerned that the final MOTR does not conflict with any of the FBI's statutory authorities.

We believe a lack of jurisdictional clarity could hinder the FBI's and the Coast Guard's ability to coordinate an effective response to a terrorist threat or incident in the maritime domain. Specifically, we are concerned about how confusion over authorities will affect the two agencies' ability to establish a clear and effective incident command structure. In our judgment, unless such differences over roles and authorities are resolved, the response to a maritime incident could be confused and potentially disastrous.

### **Exercises and Responses**

As with all terrorist incidents or responses to a terrorist threat, maritime incidents and responses require the effective cooperation and coordination of numerous federal, state, local, and private entities —



## REDACTED AND UNCLASSIFIED

issues that exercises and after-action reports are intended to identify. To measure the FBI's involvement in the maritime domain, we asked it to provide a list of maritime exercises in which its various units and field offices had participated between FYs 2002–2005 and the corresponding after-action reports. The FBI named nine maritime-related exercises it was involved in during the period, and we subsequently identified another five.

The FBI recognizes the value of after-action reports, calling them critical in identifying the areas of crisis management theory and practice that need improvement. After-action reports can provide important insight into the strengths and weaknesses in training and preparedness as well as assist the FBI in identifying and disseminating lessons learned and best practices. The FBI's Manual of Investigative Operations and Guidelines (MIOG) requires FBI divisions to write an after-action report following any exercise in which the division had a significant role in the planning and execution. The MIOG also requires an after-action report after large-scale crisis management operations. Neither of the terms "significant role" or "large-scale crisis" is defined. In addition, the MIOG does not set a due date for preparing an after-action report.

The MIOG directs that after-action reports include, at a minimum, a discussion of relevant issues of the following areas:

- command and control,
- operations,
- support,
- communications, both oral and written, and
- significant lessons learned.

The MIOG also requires each field office to submit an annual report every January 15 on the following crisis management activities that occurred during the previous calendar year:

- instances in which it activated the field office's crisis management team; and

## REDACTED AND UNCLASSIFIED

- significant lessons learned from exercises, special events, and operations, including supporting after-action reports.

Because the FBI's list of nine maritime exercises appeared to have been formulated through personal recollection, we believe it may have undercounted the number of maritime exercises in which it participated. To verify that the FBI had identified all of its maritime exercises, we asked for copies of the 56 field offices' annual crisis management annual reports for 2004. However, we were not able to use these reports to identify all of the maritime exercises because 20 percent of the FBI's field offices did not submit an annual crisis management report.

Of the 45 field offices that submitted the report, the FBI determined that 10 field offices reported on maritime exercises. Of those 10 offices, the FBI provided the after-action reports for only 2 offices.<sup>11</sup> Through the reports of those 10 offices, we identified an additional nine maritime-related exercises. In addition, we identified one incident in which the FBI prepared an after-action report. Of the 19 maritime-related exercises, special events, and operations, the FBI submitted FBI-authored after-action reports for only 6, and we concluded that reports were not prepared for the remaining 13.<sup>12</sup> Most of these six were joint exercises involving the FBI, the Coast Guard, and other elements of the DHS such as CBP.

Most of the issues identified in the nine after-action reports were operational rather than legal in nature. Seven of the nine after-action reports included an objective-by-objective assessment of the exercise or identified issues that emerged from the exercise, event, or response. For analytical purposes, we divided the operational issues identified in those seven after-action reports into four categories: communication, adequacy or coordination of resources, command and control coordination, and jurisdiction or authority.

- Five of the seven reports identified communication issues, including problems with radio and cellular phone

---

<sup>11</sup> The FBI also provided an after-action report for a maritime-related special event from a field office that did not submit the crisis management report.

<sup>12</sup> Multiple FBI entities prepared after-action reports for the Arctic Strike exercise and the search of the *Palermo Senator*, so the total number of after-action reports for the six exercises, special events, and incidents was nine.

## REDACTED AND UNCLASSIFIED

communications, and failure to share intelligence with tactical assault teams.

- Five of the seven reports raised concerns with the adequacy or coordination of resources, including too few SWAT and command center personnel, and interagency efforts to preserve evidence.
- Four of the seven reports voiced concerns to coordinate effectively in a command and control environment, most notably issues about the crisis response plan, such as personnel not being knowledgeable about the plan or the plan not covering key issues.
- Three of the seven reports discussed issues concerning jurisdictional authority, such as determining the federal agency with lead decision-making authority in an interagency response. Also, one after-action report indicated the Coast Guard participants were unclear about the FBI's authority to board a suspect vessel using a Coast Guard vessel.

The CIRG's Crisis Management Unit has not used the lessons learned cited in the field offices' critical incident annual reports to review FBI crisis management policies and practices and disseminate best practices to the field offices. Therefore, no maritime best practices have been disseminated. According to the acting unit chief of the Crisis Management Unit, the unit had not been able to conduct a comprehensive review of the after-action reports because the FBI does not have a standardized format for them, making a meaningful analysis difficult.

To address the lack of a standardized format, the Crisis Management Unit has undertaken a review of after-action report formats, both internally and externally. The Crisis Management Unit said it plans to obtain input from the field offices' Crisis Management Coordinators before deciding on the FBI's new after-action report format, which it intends to be Intranet-based.

In addition, the Special Agent Advisory Council has begun a "Lessons Learned Program," to synthesize and distribute best practices, thereby enhancing the FBI's operational effectiveness and saving lives, time, and money. This program has targeted after-action

reports as a primary source of potential lessons learned. The FBI plans to use an online database and search system, available free of charge from the U.S. Marine Corps, as a repository for materials containing lessons learned. Users will be able to search the repository and participate in forums on key topics.

## **Conclusion**

Given the somewhat limited and varying maritime capabilities of the FBI's field office SWAT teams, we believe the FBI should inventory these capabilities as part of the operations plan it must develop to support the implementation of the Maritime Operational Threat Response. To be useful, the operations plan should also examine high-risk scenarios, determine the required response time, and evaluate how FBI resources would address the scenarios. Since the timing of terrorist attacks is uncertain, the FBI and the Coast Guard should increase cooperation and coordination as soon as possible and not wait for the final version of the MOTR to resolve any concerns over the roles and authorities of each agency. We believe that the FBI should review its 1979 MOU with the Coast Guard to determine if it accurately reflects both agencies' understanding of the roles and responsibilities of each agency. If the two agencies find that the MOU does not accurately describe the current environment, they should replace it with a new one that more accurately reflects current roles and responsibilities. We also believe that additional joint FBI-Coast Guard exercises would help improve coordination between the two agencies and highlight any jurisdictional, communications, or incident command issues the two agencies need to resolve.

Complete and timely analyses of maritime exercises and incidents are important to identify and correct barriers to a successful response to a maritime terrorism threat or incident. The FBI's requirement that field offices submit annual critical incident reports is a positive step forward. However, we are concerned that the CIRG has not made it clear which incidents must be reported, developed a standard after-action report format, or determined a due date for after-action reports. All of these steps are necessary before the CIRG can provide meaningful feedback on the FBI's crisis management policies or disseminate lessons learned, including lessons learned in the maritime environment.

## **Recommendations**

We recommend that the FBI:

8. Ensure that the FBI's MOTR operations plan examines high-risk scenarios, determines the required response time, and evaluates how FBI resources would address the scenarios.
9. Establish a requirement for joint FBI/Coast Guard exercises in field offices assessed as having high-risk seaports.
10. Resolve potential role and incident command conflicts in the event of a maritime terrorist incident through joint exercises and, if necessary, a revised and broadened MOU with the Coast Guard.
11. Prepare after-action reports after all maritime-related exercises and use the reports to identify and disseminate lessons learned and best practices.
12. Ensure that all field offices submit critical incident reports to the CIRG by January 15 each year; require the FBI's Maritime Security Program, in consultation with the CIRG, to use the reports to conduct maritime-specific reviews of the FBI's crisis management policies and practices — including any requirements for field office crisis management plans — and to disseminate maritime-related lessons learned and best practices.

**Finding 3: Scope of the Maritime Threat**

The FBI has not performed a comprehensive written assessment of the risk of the terrorist threat facing the nation's 361 seaports, nor did it provide us with any assessment conducted by its intelligence community or law enforcement partners that it has relied upon in developing its maritime counterterrorism strategy. Such an assessment would be important in defining the nature, likelihood, and severity of the maritime threat. It would also allow FBI managers and others to make more informed choices about the resources needed for programs and initiatives aimed not only at combating the threat of terrorism at seaports and the maritime domain in general, but also directed at other critical infrastructures. Since 2003, the FBI has conducted an annual general assessment of the terrorist threat to the United States. As of January 2006, the 2005 assessment was in draft. However, neither the 2004 nor draft 2005 assessment ranked the various tactics and targets of terrorists, so FBI managers could not use the assessments to allocate relative resources to the various initiatives intended to prevent terrorism in these segments, including the maritime domain.

The FBI collects some information that may help it assess the potential scope of the maritime threat, including intelligence collection requirements, the number of disseminated FBI intelligence products, and the number of threats and reports of suspicious activity. The FBI has identified five intelligence collection requirements applicable to the maritime domain. However, it has not monitored its progress in addressing its maritime-related collections requirements. In the 4 years since the 9/11 terrorist attacks, the FBI has disseminated 38 maritime-related intelligence products to its intelligence and law enforcement partners. While the FBI has created the Guardian Threat Tracking System (Guardian) to manage the resolution of threats and suspicious incidents, this system is neither easily searchable nor a useful tool for identifying trends in types of incidents. As a result, during our audit the FBI could not identify the number of maritime-related threats from 2002 to the present.

## **Comprehensive Assessment of the Threat**

The FBI has not performed a comprehensive written assessment of the risk of the terrorist threat facing the United States' 361 seaports. Senior FBI officials with whom we spoke disagreed about the role of the FBI in assessing the terrorist threat faced by the nation's seaports. Some said such a threat assessment was the responsibility of the Department of Homeland Security and others said the FBI would conduct such an assessment as the Maritime Liaison Agent program, discussed in Finding 1, matures.

The 9/11 Commission has expressed concern both about the capabilities of the Transportation Security Administration (TSA) to perform comprehensive threat assessments and the need for the intelligence community to produce assessments that can guide the allocation of counterterrorism resources. Specifically, the 9/11 Commission Report discussed the TSA's failure to develop a strategic plan that analyzes assets, risks, costs, and benefits. In the absence of such a plan, the Commission said it was not convinced that the nation's transportation security resources are being allocated to the greatest risks, noting that "... opportunities to do harm are as great, or greater, in maritime or surface transportation" than they are in aviation. The Commission recommended that the federal government identify and evaluate the transportation assets that need to be protected and set risk-based priorities for defending those assets.

In 2004 congressional testimony, a 9/11 Commissioner stated that it is important for the intelligence community "to outline the risks, and to identify, to the extent that they can, the capabilities that they see on the part of terrorists. Had that been done prior to 9/11 — had there been a sweep, for example, of all of the intelligence that we had about the intentions and capabilities of terrorists to utilize airplanes as missiles — we could well have configured the way in which we defend ourselves more effectively."

The Commissioner also cited the need to assess the threat of maritime terrorism, "The same is true with respect to maritime security. We only have to look at the Cole. We know that terrorists, and al Qaeda in particular, have identified maritime avenues for threatening U.S. interests. The question is where do you rank these threats? Our intelligence community is assigned the task of identifying and ranking risk."

During that same hearing, another 9/11 Commissioner stated, "One of the frustrations in our investigation was as we looked and looked through the various agencies, we found no real overview, no strategic analysis that has been done as to relating the levels of risk from which you could plan and allocate a reasonable proportion of resources."

Although the FBI does not have a direct role securing seaports — for example, it is not the FBI's responsibility to ensure ports comply with federal security requirements — the FBI is the lead federal agency for preventing terrorism and responding to terrorist incidents. Because maritime transportation is vulnerable to terrorist attacks, the FBI devotes resources to the maritime domain. However, we believe that the amount of those resources should be threat and risk driven. While there is no clear directive for the FBI to conduct a comprehensive threat and risk assessment of maritime terrorism, we believe the FBI needs such an assessment either conducted by it or another agency in the intelligence community to guide its allocation of resources. During the course of this audit, the FBI did not provide us with any comprehensive assessment of the threat and risk of maritime terrorism or demonstrate to us that it used such an assessment to allocate resources to the maritime domain.

While the FBI has not conducted a comprehensive threat and risk assessment of maritime terrorism or the transportation sector in general, we examined the following FBI intelligence products, plans, and databases that could be used to help inform FBI managers about the level of risk of maritime terrorism and the resources dedicated to it:

- the FBI's annual comprehensive terrorism threat assessment, commonly referred to as the national threat assessment;
- maritime-related FBI intelligence products disseminated to the intelligence community;
- FBI intelligence collection guidance; and
- FBI data on terrorist threats and suspicious activity.



*National Threat Assessment*

In a 2002 audit of the FBI's counterterrorism program, the OIG found that the FBI had not conducted a comprehensive written assessment of the risk of the terrorist threat facing the United States. The FBI's efforts to conduct such an assessment, entitled *FBI Report on the Terrorist Threat to the United States and A Strategy for Prevention and Response* did not: (1) provide information to assist FBI management and other government managers in developing counterterrorism strategies and programs and allocating resources on a priority basis, (2) identify critical intelligence requirements, or (3) make recommendations to any level of FBI management. We noted that the lack of recommendations in the FBI's report underscored the fact that the report was not an assessment.<sup>13</sup> Because the FBI had not completed a systematic written assessment of the most likely terrorism scenarios — taking into account terrorist methods, capabilities, and intent — we expressed concern that it may not have fully identified the specific nature of the threat so that it could focus its attention and resources to prepare adequately and respond effectively. Further, we noted that determining what scenarios are most likely to occur in a comprehensive and more formal manner would better position the FBI to meet its new counterterrorism priority.

Since 2003, the FBI has conducted an annual assessment of the terrorist threat to the United States commonly referred to as the National Threat Assessment (NTA).<sup>14</sup> As of December 2005, the 2005 NTA was still in draft. The FBI's Deputy Assistant Director for Counterterrorism Analysis said the 2005 NTA had not been released because a National Intelligence Estimate with a similar scope was being prepared and the FBI wanted to ensure that the 2005 NTA was closely aligned with that document. However, we reviewed the 2004 and the draft 2005 NTA assessments and found that neither ranked the targets and tactics of terrorists. As a result, FBI managers could not use the assessments to allocate resources among the initiatives aimed at preventing terrorism in various critical infrastructures and segments of the economy, including the maritime domain.

---

<sup>13</sup> Federal Bureau of Investigation. *FBI Report on the Terrorist Threat to the United States and A Strategy for Prevention and Response*, August 2001.

<sup>14</sup> Federal Bureau of Investigation. *The Terrorist Threat to the US Homeland: An FBI Assessment*, April 2004.

However, the 2004 NTA includes an eight-page assessment of the tactical trends of al Qaeda and other extremists. This section of the assessment addresses five topics, including two specific types of targets: civil aviation and maritime. In addition, it makes the following observations and assessments about three tactical topics:

- Al Qaeda has shifted its attacks toward less-protected targets, because attacks against these soft targets require less logistical support and greater flexibility in target selection.
- Terrorists are constantly innovating, finding new ways to circumvent security measures, and build more threatening bombs.
- Terrorists are tenaciously pursuing chemical, biological, radiological, or nuclear weapons and may attempt to use them against the United States within the next 3 years.

The 2004 NTA's assessment of al Qaeda's maritime intent and capability is one of five topics discussed. It notes that al Qaeda has temporarily abstained from maritime attacks, and it attributes the lack of attacks to the arrest of key operatives. Based on suspicious activity reports and the vulnerability of ports, it concludes that al Qaeda will resume its maritime strategy. The NTA names vehicle-borne improvised explosive devices as the type of weapon that al Qaeda will most likely use for a maritime attack, and cites maritime facilities, infrastructure, merchant vessels, and warships as the most likely maritime targets. According to the assessment, the second most likely weapon is a bomb used against a cruise ship or ferry. [REDACTED]

The NTA uses a three-tiered classification to rank the threat posed to the United States by known terrorist groups. This classification system allows FBI and other government officials to allocate resources to different groups based on the threat level. [REDACTED]

However, the NTA does not use a similar system to rank tactics or targets. Instead, the FBI uses phrases such as "most favored" and "remains committed to" to describe the likelihood of terrorist use of various tactics. For example, it says that al Qaeda remains committed to using commercial aircraft in future attacks. Unlike the ranking of terrorist groups, FBI managers cannot use the narrative descriptions to compare the relative risk of attack using various tactics. In addition, the narrative descriptions do not discuss all potential terrorist tactics. Because the narrative descriptions of tactics and targets do not allow for a relative comparison, they may not provide a sufficient basis to allow the FBI to allocate resources according to the various terrorist tactics and methods.

### *Disseminated Intelligence Products*

The FBI has three primary intelligence products: intelligence assessments, Intelligence Information Reports (IIR), and intelligence bulletins. Intelligence assessments may be either strategic or tactical. Strategic assessments support FBI-wide programs, plans and strategies or provide information to policy makers. Tactical assessments support FBI cases or operations, or cover specific threats. IIRs contain single-source intelligence that the FBI has not deeply evaluated. Intelligence bulletins are unclassified descriptions of significant developments or trends.

Between FYs 2002-2005, the FBI disseminated a total of 38 intelligence products which, to varying degrees, discussed maritime-related terrorism.<sup>15</sup> For example, one intelligence bulletin discussed how terrorist groups could use combat divers to attack the United States, while another intelligence bulletin issued by a field office discussed terrorist issues in that field office's territory and included only data on the number of maritime suspicious incidents it had received in the last month.

---

<sup>15</sup> The FBI provided us with 41 disseminated intelligence products that it said were maritime-related. However, 38 were applicable to our audit. The remaining three dealt with other issues such as the country's water supply. In addition, during the course of our audit, the FBI provided us with two additional assessments that discussed maritime terrorism but the FBI did not include these products in its list of maritime-related disseminated intelligence products.

**Disseminated FBI Intelligence Products that Addressed Maritime Terrorism, FYs 2002-2005**

	2002	2003	2004	2005
Intelligence Assessment	0	2	4	0
Intelligence Information Report	0	7	6	3
Intelligence Bulletin	0	3	4	9
<b>Total</b>	<b>0</b>	<b>12</b>	<b>14</b>	<b>12</b>

Source: OIG analysis of FBI data

The Newark and Chicago field offices issued 9 of the 16 intelligence bulletins the FBI provided. While the intelligence bulletins issued by the CTD focused on seaport security and maritime issues, the intelligence bulletins issued by the two field offices were summaries of all terrorism activity that contained limited maritime information, usually the number of maritime-related threats received by the office in the last month. Although the amount of maritime information in these intelligence bulletins was limited, we believe the concept of providing trend data to local law enforcement and intelligence partners is worthwhile because it provides information about the current threat environment. However, we have three concerns about such bulletins.

- There is no FBI policy requiring field offices to issue regular intelligence summaries to federal, state, and local partners in their territory. The FBI provided intelligence bulletins from only 2 of its 56 field offices and, combined, these intelligence bulletins covered only 5 months. The Newark intelligence bulletins began in April 2005 and appeared to be ongoing at the time of our audit. The Chicago intelligence bulletins appear to have been limited to 2 months in 2004.
- The frequency and content of the intelligence bulletins varied, and the suspicious incident categories used by each field office also varied. While we recognize that individual field offices may have the need to highlight areas that other field offices do not, we believe that standardized categories would be helpful in allowing FBI managers to compare the activity of

different offices. The table below summarizes the differences in frequency and content between the intelligence bulletins produced by the Chicago and Newark field offices.

**Frequency and Content of Chicago and Newark Intelligence Bulletins**

	<b>Chicago</b>	<b>Newark</b>
Frequency	Monthly	Weekly
Data sources	Guardian database	FBI intelligence assessments and IIRs; Department of Defense reporting Terrorism Situation Reports, DHS intelligence bulletins and intelligence assessments; Guardian database; and a list of upcoming significant dates
Suspicious incident categories	8 to 9 types	21 types and 22 geographic areas
Suspicious incident categories in common	Airports/aircraft Chicago Transit Authority Rail Federal facilities Maritime	Aviation Rail Government building Maritime
Detailed description of suspicious activities, including status	Yes	No

Source: OIG analysis of FBI data

- It was not clear that the field office intelligence bulletins had been disseminated to the FBI's maritime partners. For example, the Newark intelligence bulletins included a distribution list, and neither the Coast Guard nor the Area Maritime Security Committee was included on the list.<sup>16</sup> The FBI must ensure that its intelligence products reach all

<sup>16</sup> These Coast Guard-sponsored committees were mandated by the Maritime Transportation Security Act of 2002. See Finding 1 for a detailed discussion.

REDACTED AND UNCLASSIFIED

relevant federal, state, and local law enforcement and intelligence entities.

In our judgment, summary field office intelligence bulletins are a significant opportunity for the FBI's field offices to share with their partners a snapshot of the local threat environment. We believe each field office should publish summary intelligence bulletins using a standard format that specifies the content, frequency, and distribution of the intelligence bulletins.

Of the 38 maritime-related intelligence products the FBI provided us, 29 (76 percent) dealt solely with maritime terrorism. Of those 29, 55 percent were IIRs. As shown in the following table, IIRs were most likely to cover threats about WMD or terrorist attacks against specific targets or cities. While the intelligence assessments and intelligence bulletins varied in scope, they normally focused on the maritime tactics terrorists may employ. Specifically, 85 percent of these products focused on diving, infiltration, small boat attacks, and mines (including improvised explosive devices). One target, passenger ferries, received substantial attention. Over 80 percent of the intelligence assessments focused on the maritime capabilities of a specific terrorist group. Over one-third of the finished intelligence products focused on just two potential tactics: attacks by scuba divers or combat swimmers and infiltrating the United States by various methods. For example, although terrorists have indicated a strong desire to use a weapon of mass destruction (WMD) and vessels can be used to transport a WMD for detonation in a port or elsewhere, none of the FBI's finished maritime-related intelligence products assessed the potential use of smuggling a WMD aboard a ship.<sup>17</sup>

---

<sup>17</sup> Finished intelligence products, such as intelligence assessments and intelligence bulletins, are developed from multiple sources and fully addresses an issue or threat. In contrast, raw intelligence, the type of information in most IIRs, is unevaluated information, generally from a single source.

**Characteristics of FBI Maritime Intelligence Products, FYs 2002-2005<sup>a</sup>**

<b>Topic</b>	<b>Intelligence Assessments</b>	<b>IIRs</b>	<b>Intelligence Bulletins</b>	<b>Total</b>
Divers	2	2	3	7
Infiltration	2	3	1	6
Improvised explosive devices/mines	2	1	1	4
Small boat attacks	1	1	2	4
Ferries	1	2	1	4
Group-specific	5	1	0	6
WMD	0	6	0	6
Target or target-city specific	3	5	0	8
Data on trend analysis	2	0	0	2
Indicators	2	0	4	6
Requirements	2	0	0	2
Other	0	2	0	2

Source: OIG analysis

Note: (a) The table includes the 29 disseminated FBI intelligence products (6 intelligence assessments, 16 IIRs, and 7 intelligence bulletins) that deal solely with maritime terrorism. Several of these intelligence products had more than one of the characteristics listed in this table, so the sum of the numbers in the columns does not equal the number of intelligence products.

[REDACTED]

[REDACTED]

[REDACTED]

However, the intelligence bulletins should also provide readers with instructions or points of contact if they observe someone engaging in a suspicious activity.

[REDACTED]

**Intelligence Requirements**

[REDACTED]

19

[REDACTED]



[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

We reviewed the FBI's intelligence collection set for international terrorism to determine the scope of the FBI's requirements for maritime terrorism.

[REDACTED]

*Internal Controls for Standing Intelligence Requirements*

Currently, the FBI's Directorate of Intelligence cannot ensure that the FBI's operational divisions and field offices are addressing the intelligence requirements in the collection sets, so the Directorate of Intelligence cannot determine what progress the FBI has made toward satisfying its maritime-related and other intelligence requirements. Also, the Directorate of Intelligence cannot identify what FBI products meet a certain requirement, so it cannot identify those intelligence products that discuss maritime terrorism. For the FBI's intelligence analysts to be able to fully analyze the threat of maritime terrorism, they must be able to identify all the relevant information the FBI has gathered on the threat.

The Directorate of Intelligence is aware of this shortcoming and has identified three methods that can ultimately be used to ensure that the FBI's operational divisions and field offices address the intelligence requirements in the FBI's collection sets. First, the Directorate of Intelligence is requiring each operational division to present a "battle plan" that shows how it will address the intelligence requirements relevant to its work. Second, the Directorate of Intelligence has begun providing training and guidance on the importance of citing the requirements with which each intelligence product responds. For example, the Field Intelligence Operations Handbook discusses the need for each product to cite an intelligence requirement. Third, the inspections done by the FBI's Inspection Division will, in the future, assess an office's contribution to the FBI's intelligence requirements.

However, according to the section chief of the Directorate of Intelligence's Intelligence Management Section (IMS), his section has made little progress in implementing these methods or otherwise monitoring what intelligence requirements are being addressed. The Directorate of Intelligence recognizes that the FBI also needs to improve integration of its intelligence requirements, collections, and production. An FBI official said that generally, FBI personnel need to understand what the intelligence requirements are, collect information to meet them, and then ensure that information the FBI collects against its intelligence requirements is reported to the widest audience possible.

REDACTED AND UNCLASSIFIED

The IMS section chief also said his section is responsible for monitoring the FBI's progress in addressing its intelligence requirements. However, he said that IMS's capability is limited by three factors: (1) all field office personnel need training on the importance of intelligence requirements and the integrity of the intelligence cycle, (2) information that satisfies intelligence requirements needs to be culled from FD-302 interview records and recordings made under the Foreign Intelligence Surveillance Act of 1978, and (3) reported information (generally IIRs) needs to cite the intelligence requirement.<sup>20</sup>

Two other issues, staffing and information technology, affect the IMS's ability to address these three factors. Many units in the IMS have 40-to-50-percent vacancy rates, so the personnel necessary to systematically evaluate intelligence collection against intelligence requirements is not available. In addition, the FBI does not have an information technology tool that allows the IMS to search data collected by the FBI to identify information that meets a given intelligence requirement. Currently, the FBI's nascent capability to search its data to determine if the information meets a specific intelligence requirement consists of searching: (1) the Automated Case Support (ACS) system for documents or data that might meet a given intelligence requirement, and (2) a stand-alone database of the CTD's IIRs, by topic, customer, and subject line.

While the international terrorism intelligence collection set included 25 observable events related to the maritime domain, none of the maritime-related intelligence products the FBI disseminated cited the intelligence requirement or indicator. To determine what information the FBI has collected about indicators of maritime terrorism or intelligence requirements with a maritime component, the FBI would have to perform a tedious and time-consuming search of the cumbersome ACS or the CTD's standalone IIR database.

---

<sup>20</sup> When a witness is interviewed as part of a criminal investigation, FBI agents use an FD-302 to document what was said during the interview. The Foreign Intelligence Surveillance Act of 1978 allows for court-approved electronic surveillance of people suspected of being engaged in espionage or terrorism for a foreign power against the United States.

*Ad Hoc Intelligence Requirements*

In addition to the standing intelligence requirements, the FBI may receive or initiate ad hoc intelligence requirements. Ad hoc requirements address more immediate needs created by an agency's tactical operations. For example, after the London subway bombings in July 2005, the FBI received ad hoc intelligence requirements related to those bombings. Regarding maritime terrorism, the FBI has received intelligence requirements from the Office of Naval Intelligence, which asked the FBI to collect intelligence on whether terrorist groups are using maritime methods to transport operatives or contraband. Ad hoc intelligence requirements are communicated to the relevant units and offices within the FBI via EC and the "setting of leads."<sup>21</sup> The IMS is the focal point for ad hoc requirements and is responsible for setting leads for FBI offices to collect information against the requirements. The results of the FBI's collection efforts in response to ad hoc requirements are reported in IIRs. If a recipient (consumer) of an IIR has questions about its content or has additional ad hoc intelligence requirements, the consumer will contact the author of the IIR directly and address those questions or requirements. The Directorate of Intelligence did not initiate any ad hoc maritime-related intelligence requirements during FY 2005.

To improve the FBI's intelligence base and ultimately help it identify terrorists within the United States, the FBI's NJTTF created Operation Tripwire in July 2003. Through Operation Tripwire, the CTD sends local JTTFs tasks or requirements to collect information related to certain entities. The collection requirements are specific to a threat and provide information about who or what can provide the information. For example, one maritime-related Tripwire EC we reviewed directed a field office to contact the executive in charge of a certain line of business at a particular company. According to the NJTTF, the ultimate goal of these tasks is to develop a useful set of indicators for terrorist sleeper cells. The CTD intended for the requirements to have a secondary purpose in assisting field office managers by providing guidance on how to enhance their intelligence base and more accurately define their technical requirements.

---

<sup>21</sup> When an FBI office needs assistance or information from another FBI office, it "sets a lead" specifying the assistance it needs.

*Information Management Systems for Intelligence Products*

The FBI does not have an information management system to store and manage the all of the FBI's intelligence products, but the Directorate of Intelligence is developing a searchable database for all the FBI's intelligence products. Currently, all IIRs are stored in the FBI Intelligence Information Reports Dissemination System. However, this system does not have any management capability to allow Directorate of Intelligence managers to search for an IIR by intelligence requirement. A new version of this information system, due in FY 2006, is expected to provide such a search capability.

While there is no information management system that stores and manages the FBI's finished intelligence products (intelligence assessments and intelligence bulletins), the Directorate of Intelligence maintains an Access database of the terms of reference of all these products. When analysts start a new intelligence assessment or intelligence bulletin, they must input the terms of reference — a description of the approach, purpose and scope of a proposed intelligence product — into the database. The terms of reference are then reviewed by the FBI's Intelligence Production Board at its monthly meeting. The board evaluates the terms of reference against the relevant collection set and other ongoing intelligence assessments and determines whether the proposed intelligence assessment addresses a known collection requirement or whether it duplicates work already being done. The IMS's Strategic Analysis Unit prescreens the terms of reference of each proposed intelligence product before it is passed to the board. Also, intelligence assessments and intelligence bulletins should be uploaded into the ACS, but the IMS section chief said that often this is not done.

**Data on the Number of Maritime Threats**

FBI headquarters and its field offices receive warnings daily about terrorist threats and suspicious activities. These warnings come from a variety of sources, including other intelligence agencies, law enforcement agencies, and concerned citizens. The FBI Director has made it clear to all employees that the FBI's highest priority is the resolution of all terrorist threats. While the FBI has created the Guardian Threat Tracking System (Guardian) to manage the resolution of threats and suspicious incidents, this system is neither easily searchable nor a useful tool for identifying trends in types of incidents.

As a result, during our audit the FBI could not identify the number of maritime-related threats from 2002 to the present. Instead, in response to our request for a list of maritime-related threats to which the FBI had responded, the FBI manually reviewed reports of monthly compilations of significant incidents, called threat information reports, and identified 68 maritime-related incidents that it tracked from September 2004 to September 2005. Two of the FBI's six maritime-related intelligence assessments also included data about the scope of the maritime threat.

*Intelligence Assessments with Data on Maritime Incidents*

A May 2004 intelligence assessment by an FBI field office highlights the difficulty the FBI has in determining the scope of the threat of maritime terrorism and offers potential methods for resolving those difficulties. Two intelligence analysts, one FBI and one Coast Guard, reviewed 157 suspicious incidents reported to law enforcement involving a ferry system.<sup>22</sup> They also assessed the likelihood of whether the incidents were indicative of pre-operational planning for a terrorist attack.

Our review of the intelligence assessment noted the following difficulties encountered by the analysts. First, the FBI had to ensure it had data on all of the incidents reported to local, state and federal agencies. To accomplish this, Seattle's Field Intelligence Group attempted to collect from its law enforcement partners all suspicious activity reports related to the ferries. Second, the FBI and its partners did not have a standardized reporting format for suspicious incidents. As a result, the partners submitted their reports in various formats which the FBI had to manually summarize. Third, multiple agencies often reported on the same incident. Inconsistencies between various reports — such as date and number of suspects — made it difficult for the analysts to identify the number of incidents. Fourth, the incident reports did not provide enough detail about the suspects or their vehicles. Fifth, the reports did not indicate whether the event had been thoroughly investigated when feasible. Finally, the FBI had no standardized guidance for assessing the likelihood that a given suspicious activity was indicative of pre-operational planning.

\_\_\_\_\_

[REDACTED]

REDACTED AND UNCLASSIFIED

Despite concerns about the quality of its data, the Seattle FBI office developed a weighted ranking system to assess the likelihood that a given incident was indicative of pre-operational planning. The ranking system included the following six categories: "not applicable," "extremely high," "high," "medium," "low," and "not weighted." Each category had a set of criteria against which all the incidents were assessed. For example, incidents classified as "extremely high" met the following criteria:

[REDACTED]

[REDACTED]

[REDACTED]

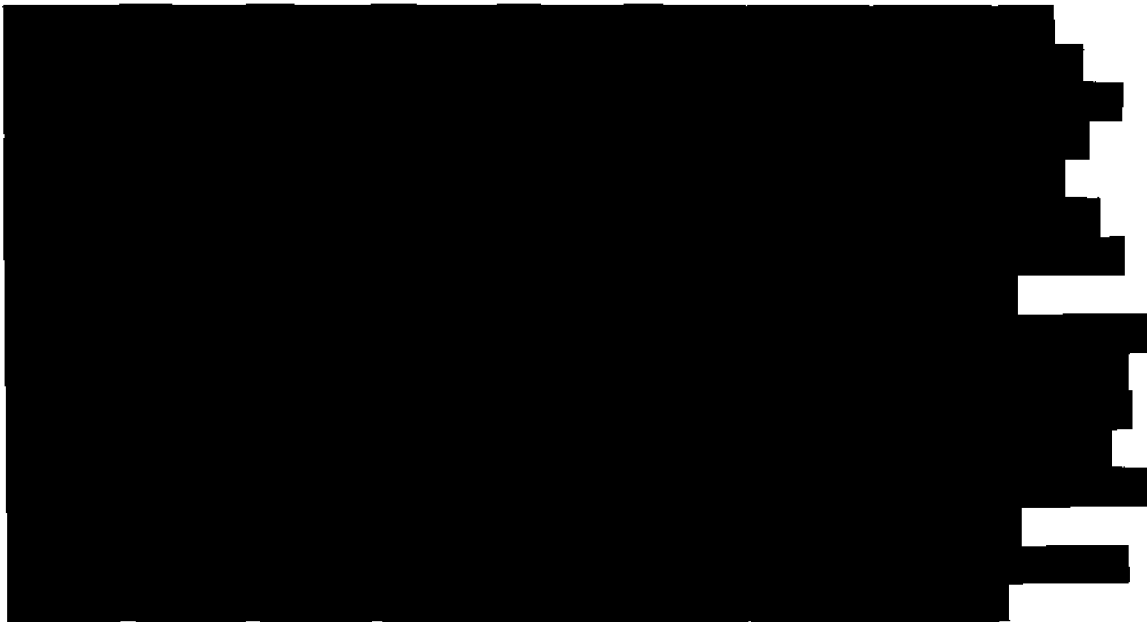
[REDACTED]

The Seattle intelligence assessment also included two checklists intended to improve the quality of information collected about suspicious incidents. The first checklist was for law enforcement personnel responding to suspicious incidents, reminding them to:

- photograph or videotape the incident;
- record information about the subject's vehicle, its occupants, and location; and
- record descriptive information about the suspect and the suspect's actions.

The second checklist provided questions that FBI or JTTF personnel should ask law enforcement when they report a suspicious incident to the FBI.

[REDACTED]



*Guardian Threat Tracking System*

In September 2004, to facilitate the accurate, complete, and timely reporting on the existence and status of terrorist threats, the FBI launched a database called Guardian.<sup>23</sup> Guardian is available on the FBI Intranet, and all field offices and legal attaches are required to enter into Guardian new terrorism threats and suspicious incidents originating in their territory and use it to track resolution. As of September 2005, the FBI had entered information into Guardian on 51,000 threats. However, because of Guardian's limited search capabilities, the system cannot readily be used to identify maritime or other sector-specific threats or to produce data for trend analyses.

At our request, the FBI's Threat Monitoring Unit (TMU) queried Guardian in an attempt to identify the number of maritime-related incidents within the database, but the system was unable to conduct such a search. Instead, Guardian could be queried on the number of times certain words occurred in the system. Even this search was not simple because maritime-related terms, such as "port," are a subset of other words that occur frequently in Guardian. For example, "report" and "airport" both include "port," so the search for port had to be

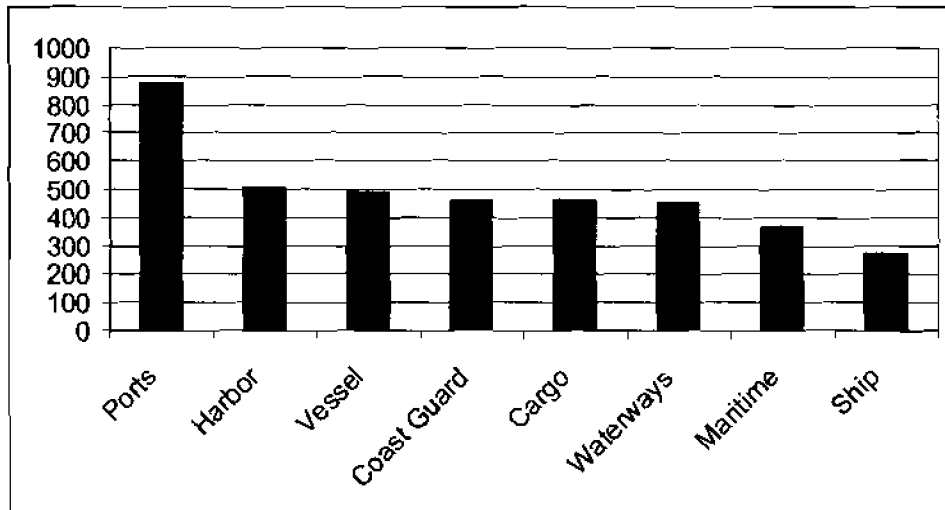
---

<sup>23</sup> The scope of our work on Guardian was limited to those aspects affecting the FBI's maritime role such as data on the number of maritime incidents. We did not examine information technology management practices used to develop or implement Guardian.



modified to exclude these other words. The chart below shows the results of the FBI's efforts to identify the number of times a certain word occurred in Guardian.

**Number of Maritime-Related Hits in the Guardian Threat Tracking System September 2004–September 2005**



Source: The FBI

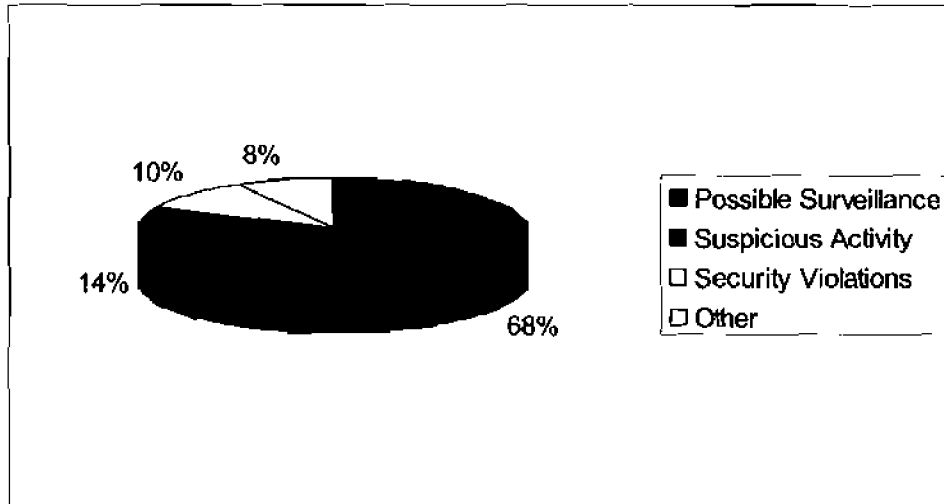
Since the FBI was unable to use Guardian to identify the number of maritime-related incidents, the Threat Monitoring Unit manually reviewed threat information reports from September 2004 to September 2005 to identify the most significant maritime-related incidents in Guardian.<sup>24</sup> Based on this review, the FBI identified 68 maritime-related incidents, with the greatest concentration found in the Seattle area. In addition, there were a substantial number of threats along the Gulf Coast, which most likely involved suspected surveillance of energy facilities and oil tankers.

The FBI categorized 68 percent of the 68 incidents as possible surveillance. As shown below, the remaining 32 percent of the

<sup>24</sup> Threat information reports originated in 2004 in response to a need for an up-to-date summary of threat information from the '04 Task Force. The '04 Task Force was formed to prepare for several special events in 2004 including the presidential elections, the Olympics, and the Democratic and Republican National Conventions. These reports provide monthly summaries of significant threat reporting by region, type, and target.

incidents were classified as suspicious activity, security violations, or other.

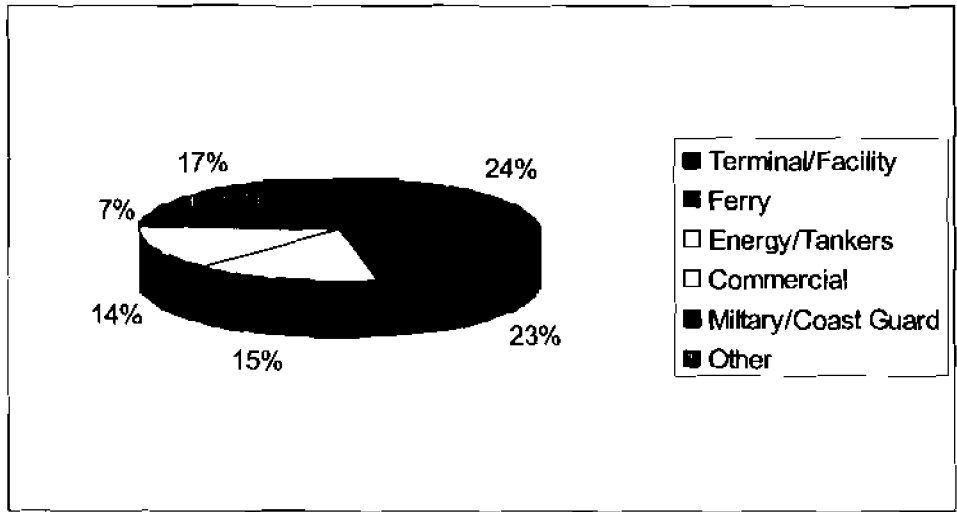
### Threat Information Report Threat Categories



Source: The FBI

The FBI identified 6 categories of maritime targets, each of which accounted for at least 7 percent of the 68 incidents. The most commonly targeted maritime infrastructures were terminals and ferries, both of which were frequently filmed or photographed in the Seattle area by people acting suspiciously. Together these targets accounted for 47 percent of the incidents. Assuming the data from these 68 incidents is indicative of pre-operational activity, the FBI believes that ferries in the Seattle area and fuel tankers in the Gulf Coast region appear to be the most likely targets of maritime terrorism. The chart below shows the distribution of targets for the 68 incidents.

**Threat Information Report Maritime Incidents by Target**



Source: The FBI

TMU officials expressed concern that the entries in Guardian, and the threat information reports, are not representative of all the maritime suspicious incidents. Guardian generally includes only the threats the FBI has received or investigated. The FBI database does not include Coast Guard reporting on suspicious incidents, nor does it include data from the FBI's state and local law enforcement partners such as port authority police departments. The Seattle intelligence assessment on ferries also recognized this weakness and compensated for it by canvassing other law enforcement agencies for suspicious activity reports.

The FBI plans to correct several of the weaknesses in its ability to collect and analyze suspicious activities and other security incidents by upgrading Guardian and establishing an Internet-accessible version of the database, called E-Guardian. The upgraded version, Guardian 2.0, is scheduled to be deployed in March 2006. Guardian 2.0 is expected to have improved search capabilities. In addition to improved search capabilities, Guardian 2.0 will allow users to bookmark items of interest, hyperlink items, and save the results of searches.

The FBI plans to deploy E-Guardian in April 2006. E-Guardian will allow law enforcement and intelligence personnel to enter information into Guardian through an Internet-based system

REDACTED AND UNCLASSIFIED

accessible only to authorized users. While E-Guardian users will be able to add or update entries at any time, the data in the E-Guardian website will be updated every 6 or 8 hours. A TMU official said the exact update interval had not yet been determined. Further, E-Guardian will not include classified information. We believe E-Guardian will be a significant improvement because it will help standardize suspicious incident reporting and collect information from other law enforcement agencies.

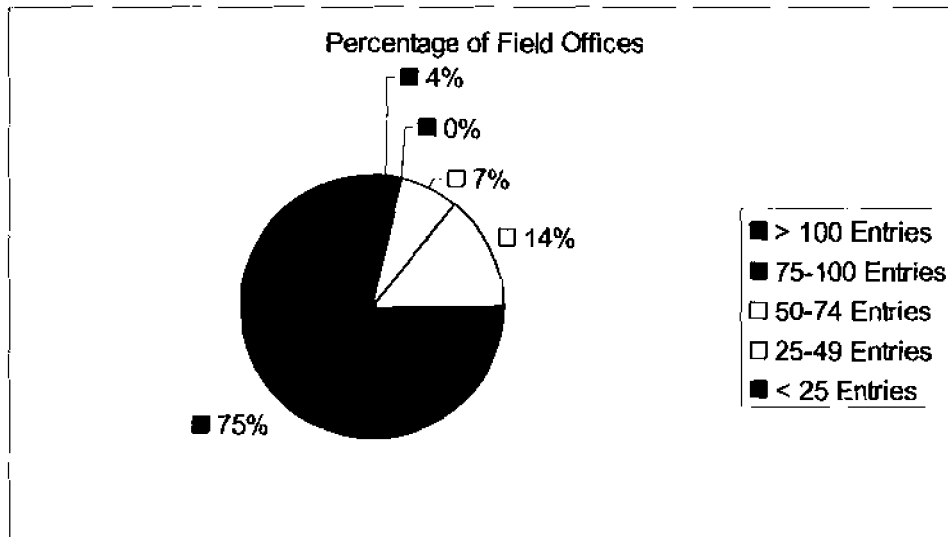
In the EC announcing Guardian, the FBI Deputy Assistant Director for Operational Support noted, "Given the current world situation, it is imperative that all threats and suspicious activity be closely monitored and fully exploited." However, the FBI has not established controls to ensure that field offices enter all terrorism threats, suspicious activity, and events into either version of Guardian. Without these controls, the FBI cannot be assured that Guardian contains all threat information gathered by the FBI or that this information is entered and resolved according to the established guidelines.

Since January 2005, the CTD has sent eight ECs to its field offices and legal attaches reminding them of the requirement to enter all terrorism information into Guardian and to resolve the entries. In March 2005, the TMU reviewed entries into Guardian over the previous 30 days and sent an EC to FBI field offices and legal attaches reporting "some trends showing that several offices are not fully utilizing the Guardian System and taking advantage of its capabilities." During that 30-day period, only two field offices — New York and Baltimore — recorded more than 100 entries, accounting for 21 percent of the 1,211 entries made by field offices. As shown in the following table, 75 percent of the FBI's 56 field offices recorded less than 25 entries. Major FBI field offices, including Boston and Dallas, recorded five or fewer entries.<sup>25</sup>

---

<sup>25</sup> See Appendix II for the number of Guardian entries for each field office.

**Field Office Guardian Usage,  
30-Day Period Ending March 28, 2005**



Source: OIG Analysis of FBI data

We are concerned that not all field offices are fully utilizing Guardian. In our judgment, the underutilization of Guardian prevents the TMU from developing a complete understanding of threat trends, including threats associated with the maritime domain.

Ensuring that each Guardian entry is investigated to its logical end and documenting the investigation are two other challenges the TMU faces and has been actively managing. TMU has sent field offices two ECs concerning unresolved Guardian entries that needed further investigation or management review. The first EC, sent in January 2005, reported that 30 percent of all Guardian entries were unresolved. When the second EC was sent in August 2005, unresolved entries accounted for 13 percent of all entries. As shown in the following table, in August 2005 the majority of the 6,028 unresolved entries were entered by field offices. Forty-eight percent of the unresolved entries were more than 90 days overdue.

**Unresolved Guardian Entries,  
August 2005<sup>a</sup>**

	Total Unresolved Entries	Unresolved for 30 Days or Less	Unresolved for 31 to 90 Days	Unresolved for More Than 90 Days
Field Offices	5,082 (84%)	1,796	901	2,385
Legal Attaches	625 (10%)	202	106	317
Headquarters	321 (5%)	90	62	169
Total	6,028	2,088 (35%)	1,069 (18%)	2,871 (48%)

Source: The FBI

Note: (a) Percentages do not total to 100 percent due to rounding.

**Conclusion**

The FBI has not conducted or reviewed a threat assessment that ranks the different tactics or targets that terrorists may employ. It therefore does not have any assurance that the amount of resources allocated to the various initiatives aimed at preventing terrorism in segments of the economy — such as seaports, aviation, mass transit, energy, agriculture, and other critical infrastructures — are proportional to the threat. Moreover, the FBI’s Directorate of Intelligence did not monitor the FBI’s intelligence products to ensure they met its intelligence requirements. The FBI’s threat-monitoring database, Guardian, is promising, but a number of limitations must be resolved before it can produce a complete and accurate picture of maritime threats and suspicious incidents. We identified two intelligence initiatives at FBI field offices — intelligence bulletins with a field office’s recent Guardian data, and an intelligence assessment that included non-FBI suspicious incident reporting — that the FBI may want to consider implementing more broadly.

**Recommendations**

We recommend that the FBI:

13. Assess the threat and risk of maritime terrorism compared to other terrorist threats and ensure the National Threat Assessment ranks the various modes of attack and targets.

REDACTED AND UNCLASSIFIED

14. Ensure the amount of FBI resources dedicated to maritime terrorism is based on the extent of the maritime threat in relation to other threats.
15. Monitor the progress of operating divisions and field offices in answering intelligence collection requirements pertaining to seaports and maritime terrorism.
16. Focus intelligence reporting to more comprehensively address potential maritime-related terrorist targets and methods.
17. Name a unit within the Counterterrorism Division to monitor the volume and substance of all FBI maritime-related intelligence.
18. Consider establishing a requirement for regular field office intelligence bulletins to summarize the field office's suspicious incident reporting and, if such a requirement is adopted, establish standardized frequency, content, and distribution requirements.

## **STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS**

We have audited the FBI's efforts to prevent and respond to a maritime terrorism attack. The audit was conducted in accordance with the *Government Auditing Standards*. As required by the standards, we reviewed management processes and records to obtain reasonable assurance that the FBI's compliance with laws and regulations that could have a material effect on FBI operations. Compliance with laws and regulations applicable to the FBI's terrorism efforts in the maritime domain is the responsibility of the FBI's management.

Our audit included examining, on a test basis, evidence about laws and regulations. The specific laws and regulations against which we conducted our tests are contained in:

- 28 U.S.C. § 533;
- Presidential Decision Directive 39;
- Presidential Decision Directive 62; and
- National Security Presidential Directive 41/Homeland Security Presidential Directive 13.

Our audit identified no areas where the FBI was not in compliance with the laws and regulations referred to above. With respect to those transactions not tested, nothing came to our attention that caused us to believe that FBI management was not in compliance with the laws and regulations cited above.



## **STATEMENT ON INTERNAL CONTROLS**

In planning and performing our audit, we considered the FBI's internal controls for the purpose of determining audit procedures. This evaluation was not made for the purpose of providing assurance on the internal control structure as a whole. However, we noted certain matters that we consider to be reportable conditions under the *Government Auditing Standards*.

Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of the internal control structure that, in our judgment, could adversely affect the FBI's ability to manage its maritime terrorism efforts. As discussed in the Findings and Recommendations sections of this report, we found that:

- The FBI does not allocate the amount of its resources dedicated to maritime terrorism based on the maritime threat;
- The FBI does not ensure that every intelligence product cites an intelligence requirement;
- The FBI does not ensure that all indicators with a nexus to terrorism in the human smuggling collection set includes a reporting requirement to the relevant officials in the CTD;
- The FBI does not have a threat-based or risk-based method of allocating MLAs to its different divisions and field offices;
- The FBI cannot measure the amount of resources devoted to maritime efforts;
- The Manual of Investigative Operations and Guidelines does not clearly state which types of exercises, special events, and FBI responses require an after-action report; and
- The FBI does not ensure that its field offices submit annual critical incident reports to the Critical Incident Response Group.

REDACTED AND UNCLASSIFIED

Because we are not expressing an opinion on the FBI's internal control structure as a whole, this statement is intended solely for the information and use of the FBI in managing its maritime terrorism efforts. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

## OBJECTIVES, SCOPE, AND METHODOLOGY

### Objectives

The primary objectives of the audit were to determine: (1) the FBI's roles, responsibilities, and capabilities for preventing and responding to terrorist attacks in the maritime domain, including U.S. seaports; and (2) the extent and effectiveness of FBI interagency coordination, planning, assistance, and investigation to help ensure maritime domain security.

### Scope and Methodology

The audit was performed in accordance with the *Government Auditing Standards*, and included tests and procedures necessary to accomplish the audit objectives. We conducted field work at the FBI's headquarters in Washington, D.C., facility in Quantico, Virginia, and Baltimore, Maryland, field office. In addition, we also conducted work at the Washington, D.C., headquarters of the DOJ and Coast Guard.

We interviewed officials from the FBI, DOJ, Coast Guard, and CBP. We also interviewed officials from state and county law enforcement in Maryland. The FBI officials we interviewed were from the CTD, the CIRG, Directorate of Intelligence, and the Baltimore field office. We also reviewed documents related to the FBI's Maritime Liaison Agent program initiative, Maritime Security Program, intelligence requirements and collection sets, intelligence products, response capability, and organizational structures. In addition, we reviewed relevant laws, directives, national plans, congressional testimony, and prior OIG and GAO reports.

To determine the FBI's roles, responsibilities, and capabilities for preventing and responding to terrorist attacks in the maritime domain, we reviewed federal statutes, national directives, and memoranda of understanding pertaining to terrorism and to maritime authority. We examined the FBI's maritime-related counterterrorism efforts by reviewing existing FBI maritime program and capability documents and interviewing FBI officials. We also reviewed the FBI's threat data and intelligence products concerning maritime terrorism. In addition, we visited the Baltimore field office to observe maritime training and

REDACTED AND UNCLASSIFIED

interview officials regarding the FBI's interagency cooperation and maritime response capabilities. While at the Baltimore field office, we observed FBI maritime training involving the Baltimore SWAT team and the Hostage Rescue Team.

To determine the extent and effectiveness of FBI interagency coordination, planning, assistance, and investigation to help ensure maritime domain security, we interviewed FBI, Coast Guard, and CBP officials. We interviewed FBI officials to learn about its maritime initiatives, efforts at interagency cooperation, and information sharing with maritime partners. We reviewed FBI participation in maritime terrorism-related exercises.

In addition, we interviewed Coast Guard headquarters officials, Coast Guard Investigative Service officials assigned to the National Joint Terrorism Task Force and the Baltimore Joint Terrorism Task Force, and Maryland state and county law enforcement officials to assess their working relationships with the FBI, including information sharing and interagency cooperation.

**APPENDIX II**

**FIELD OFFICE GUARDIAN ENTRIES, 30-DAY PERIOD ENDING MARCH 28, 2005**

<b>Field Office</b>	<b>Guardian Entries</b>
New York City	159
Baltimore	101
Los Angeles	74
Houston	62
Seattle	62
Atlanta	61
Chicago	41
Philadelphia	41
Washington	37
Buffalo	33
New Orleans	33
Cincinnati	30
Phoenix	26
Tampa	25
Detroit	24
Newark	24
Springfield	24
Pittsburgh	22
San Francisco	21
Denver	19
New Haven	19
Kansas City	18
Oklahoma City	18
Minneapolis	17
San Diego	17
Charlotte	16
Anchorage	15
Columbia	14
Louisville	14
Portland	13
St. Louis	13
Miami	11
Norfolk	11
Richmond	10
Cleveland	8

REDACTED AND UNCLASSIFIED

<b>Field Office</b>	<b>Guardian Entries</b>
Sacramento	8
Honolulu	7
Memphis	6
San Antonio	6
Dallas	5
Indianapolis	5
Milwaukee	5
Boston	4
Knoxville	4
Las Vegas	4
Little Rock	4
Omaha	4
Birmingham	3
El Paso	3
Albany	2
Jackson	2
Jacksonville	2
Salt Lake City	2
Albuquerque	1
Mobile	1
San Juan	0
<b>TOTAL ENTRIES</b>	<b>1,211</b>

**APPENDIX III**

**MARITIME ACTIVITY AND RISK OF MARITIME TERRORISM  
CONCENTRATED IN THE TERRITORY OF 24 FBI FIELD OFFICES**

	<b>Field Office</b>	<b>Ports In Territory</b>
1	Anchorage, AK	Anchorage, AK (E), Valdez, AK (E)
2	Atlanta, GA	Savannah, GA (V,T,E)
3	Baltimore, MD	Baltimore, MD (V,T,E), Wilmington, DE (E)
4	Boston, MA	Boston, MA (E), Portland, ME (E), Portsmouth, NH (E), Providence, RI (E)
5	Columbia, SC	Charleston, SC (V,E)
6	Houston, TX	Houston, TX (V,T,E); Port Arthur, TX (T,E), Beaumont, TX (V,T,E), Corpus Christi, TX (V,T,E), Freeport, TX (T,E), Texas City, TX (T,E), Victoria, TX (E)
7	Jackson, MS	Vicksburg, MS (E), Greenville, MS (E), Pascagoula, MS (T,E)
8	Jacksonville, FL	Jacksonville, FL (V,E), Pensacola, FL (E)
9	Los Angeles, CA	Los Angeles, CA (V,T,E), Long Beach, CA (V,T,E), Port Hueneme, CA (E)
10	Memphis, TN	Memphis, TN (E), Nashville, TN (E)
11	Miami, FL	Miami, FL (V,E)
12	Minneapolis, MN	Minneapolis, MN (E), St. Paul, MN (E)
13	Mobile, AL	Mobile, AL (T,E)
14	New Haven, CT	New Haven, CT (E), Bridgeport, CT (E)
15	New Orleans, LA	New Orleans, LA (V,T,E), Plaquemines, LA (T,E), Port of South Louisiana (La Place), LA (T,E), Baton Rouge, LA (T,E), Morgan City, LA, Lake Charles, LA (T,E)
16	New York City, NY	New York, NY (V,T,E)
17	Newark, NJ	Newark, NJ (E)
18	Norfolk, VA	Norfolk, VA (V,T,E), Newport News, VA (E)
19	Philadelphia, PA	Philadelphia, PA (V,T,E), Camden, NJ (E)
20	Pittsburgh, PA	Pittsburgh, PA (E), Huntington, WV (E)
21	Portland, OR	Portland, OR (V,E)
22	San Francisco, CA	San Francisco, CA (E), Oakland, CA (V,E), Richmond, CA (E)
23	Seattle, WA	Seattle, WA (E), Tacoma, WA (V,E), Vancouver, WA (E)
24	Tampa, FL	Tampa, FL (E), Port Canaveral, FL (E), Port Everglades, FL (V,E)

<p><b>Legend</b>  V: Top 20 Port by Value  T: Top 20 Port by Tonnage  E: Port eligible for FY 2005 Port Security Grant</p>
--

**ACRONYMS**

ACS	Automated Case Support
AMSC	Area Maritime Security Committee
CBP	Customs and Border Protection
CFR	Code of Federal Regulations
CIRG	Critical Incident Response Group
CTD	Counterterrorism Division
DHS	Department of Homeland Security
EC	Electronic Communication
FBI	Federal Bureau of Investigation
FY	Fiscal Year
GAO	Government Accountability Office
IIR	Intelligence Information Report
HDRU	Hazardous Devices Response Unit
HRT	Hostage Rescue Team
JTTF	Joint Terrorism Task Force
IMS	Intelligence Management Section
MIOG	Manual of Investigative Operations and Guidelines
MLA	Maritime Liaison Agent
MOTR	Maritime Operational Threat Response
MOU	Memorandum of Understanding
MSST	Maritime Safety and Security Team
MTSA	Maritime Transportation Security Act of 2002
NJTTF	National Joint Terrorism Task Force
NTA	National Threat Assessment
OIG	Office of the Inspector General
PDD	Presidential Decision Directive
SWAT	Special Weapons and Tactics
TMU	Threat Monitoring Unit
TSC	Terrorist Screening Center
USC	United States Code
WMD	Weapon of Mass Destruction



**FEDERAL BUREAU OF INVESTIGATION'S RESPONSE  
TO THE DRAFT REPORT**



U.S. Department of Justice

Federal Bureau of Investigation

---

Washington, D. C. 20535-0001

March 17, 2006

The Honorable Glenn A. Fine  
Inspector General  
Office of the Inspector General  
United States Department of Justice  
Room 4322  
950 Pennsylvania Avenue, Northwest  
Washington, D.C. 20530

Dear Mr. Fine:

I would like to thank you for providing the Federal Bureau of Investigation (FBI) the opportunity to respond to your report entitled, "The FBI's Efforts to Prevent and Respond to Maritime Terrorism."

I recognize the substantial challenge the Office of the Inspector General (OIG) has in producing timely reports on complex issues such as this. This challenge is even more difficult when assessing FBI operations because of the rapid changes it continues to undergo to optimally position itself to address the evolving threats to our Nation.

In large part, the FBI agrees with the findings and recommendations of this report. Accordingly, Executive Management from the Counterterrorism Division (CTD) of the FBI and personnel from the appropriate programs within the FBI have reviewed OIG's draft report concerning the FBI's efforts to prevent and respond to maritime terrorism. Ideally, we would like for the report to be updated to provide a current status of maritime security efforts in the FBI, and to that end have set forth several points of information for you to consider.

- The FBI initiated the Maritime Security Program (MSP) in July 2005. This proactive measure was taken by CTD Executive Management in recognition of the potential threat of maritime terrorism. It is worth noting that this program was established without additional funding by reallocating resources within CTD.
- Availability of resources has also influenced the FBI's participation in various exercises. Although the FBI would like to participate in additional exercises, the

## REDACTED AND UNCLASSIFIED

Mr. Glenn A. Fine

FBI is currently able to support the joint exercises that are coordinated through the National Exercise Program.

- The FBI is actively working with the United States Coast Guard (USCG) and other agencies to resolve potential coordination issues in advance of actual threats and incidents in the maritime domain.

Additionally, the following comments are to correct or clarify statements made in the text of the audit report:

1. Page "v", first paragraph and page 25, first paragraph: The MSP prepared an Electronic Communication (EC) to the field to request that an FBI Special Agent (SA), as opposed to a Task Force Officer (TFO) be designated as the primary Maritime Liaison Agent (MLA). Although this EC was drafted, it was not approved by CTD management. As a result, in many Field Offices a TFO serves as the primary or only MLA.
2. Page "vi", first bullet: This point may need to be modified to include the capabilities of the Laboratory Division's Hazardous Materials Response Unit (HMRU) in dealing with a weapon of mass destruction (WMD) incident. HMRU provides technical and scientific operational response to WMD incidents, including, but not limited to, crime scene management, evidence recovery, emergency decontamination and scientific assessments. The responsibilities of the Hazardous Devices Response Unit (HDRU) includes the response to threats and actual devices before they are detonated or used in an "attack." HDRU does not respond to post-detonation attacks; that is the responsibility of HMRU and/or the Laboratory Division's Explosive Unit.
3. Page "viii", last paragraph: The statement, "The FBI has not collected complete data on the number of suspicious activities or terrorist threats involving seaports," is correct. However, the MSP has begun to collect this information from all available sources. The MSP has created a data base to capture this information which will be used to identify and track possible trends in suspicious activity at ports and port facilities. The MSP is also in the process of creating a standardized reporting mechanism for use by the MLAs when responding to incidents. These reports will be maintained in the MSP case file and the information will also be entered into the data base. Finally, the MSP maintains liaison with other agencies

REDACTED AND UNCLASSIFIED

Mr. Glenn A. Fine

and the private sector, such as the USCG, Office of Naval Intelligence (ONI) and the International Council of Cruise Lines (ICCL), for the sharing of pertinent threat information.

4. Page 20, bottom of the page: It should be noted that the MSP will present the 2006 Maritime Liaison Agent Training Conference in Long Beach, California from 04/03-07/2006. The Port of Long Beach is one of the busiest ports in the United States with a variety of inter-modal transportation systems. This site was specifically chosen because it offers hands on/familiarization training using various port facilities and vessels. The curriculum for this conference is expected to include presentations on the impact of maritime directives under the National Strategy for Maritime Security (NSMS); informant and liaison development; legal issues; enhancing maritime domain awareness; the FBI's capabilities and resources to respond to a maritime incident; and guidance to the field on best practices.
5. Page 24, first full paragraph: The report indicates that as a result of placing responsibility for managing the MLA Program under the MSP, all of the FBI's transportation related counterterrorism programs are located within the same organizational unit. This is not the case as the National Joint Terrorism Task Force (NJTTF) initiated the Rail Liaison Agent (RLA) Program via EC dated 10/24/2005. The NJTTF requested each Field Office to designate an FBI SA or TFO as a primary and secondary RLA. A separate initiative is currently underway to evaluate the feasibility of creating a program or unit focused on all aspects of the transportation sector. It is important to note this initiative is unfunded and would be created by reallocating existing resources.
6. Page 24, last paragraph: The report mentions that one of the objectives of the MSP was to create a website on the FBI's Intranet to facilitate the dissemination of information pertaining to directives, training, intelligence and other matters. This objective has been accomplished. The MSP website address is <http://ctd.fbinet.fbi/semu/maritime/>. This website contains information on maritime directives including National Security Presidential Directive (NSPD)-41/Homeland Security Presidential Directive (HSPD)-13, the NSMS and key supporting plans; maritime related statutes; intelligence reports; points of

## REDACTED AND UNCLASSIFIED

Mr. Glenn A. Fine

contact; and links to related programs including the Directorate of Intelligence (DI), and the Office of the General Counsel (OGC). Information is continually updated or added to the website. The MLAs are notified of information posted to the website via e-mail. The website has generated positive feedback from the MLAs and is a readily available source of standardized information for the field.

7. Page 24, last paragraph: The report also mentions that another objective of the MSP was to review maritime related suspicious activity reports to identify any trends that may be indicative of pre-operational planning. As noted above, the MSP has already started this process, which is ongoing. This effort is complicated by the lack of standardized reporting and difficulty in retrieving this information, as stated elsewhere in the findings.
8. Page 25, middle of the page: The report states that the MSP has not reviewed the eight supporting plans under the NSMS to identify the FBI's responsibilities nor identified all of the FBI's representatives assigned to the corresponding working groups. That information was supplied to OIG at the inception of the MSP. Since then, the MSP has thoroughly reviewed NSPD-41/HSPD-13, the NSMS and all eight of the supporting plans. The FBI's responsibilities under these directives have been identified and are being addressed. NSPD-41/HSPD-13, the NSMS and key supporting plans are posted to the MSP website. Due to limited resources, the MSP must prioritize which of the working groups to attend in support of these efforts. In that regard, representatives from the MSP have regularly attended and participated in the Maritime Security Policy Coordinating Committee (in support of Executive Management); the Maritime Security Working Group; the Maritime Operational Threat Response (MOTR) Implementation Team; and the Maritime Domain Awareness Implementation Team. In addition, an interagency MOTR Joint Working Group (JWG) has recently been established to address the planning, standardization and exercise requirements that will be deleted from the final version of the MOTR Plan as the Homeland Security Council has indicated. The MSP participates in this JWG as well as the Border and Transportation Security Policy Coordinating Committee.
9. Page 25, fourth paragraph: The report states neither the MSP's FY 2006 goals and objectives nor the critical

REDACTED AND UNCLASSIFIED

Mr. Glenn A. Fine

duties of an MLA include the need for the FBI to develop relationships with people who can inform the FBI about maritime operations. It should be noted that at the time the MSP's goals and objectives were established (via EC dated 08/19/2005), the MSP did not have responsibility for managing the MLA Program. In fact, the first objective identified in that EC was to coordinate with the NJTTF to assume responsibility for the MLA Program. That objective was accomplished on 10/04/2005, when the MSP assumed responsibility for managing the MLA Program.

Furthermore, within the goals and objectives (via EC dated 08/19/2005), the MSP established various objectives for the field. One of these objectives was to "ensure effective liaison between the MLA and various law enforcement agencies, port and shipping officials in respect to counterterrorism preparedness." In the goals and objectives EC, the MSP identified five core competencies which included the establishment of a human intelligence base. Finally, in an EC to all Field Offices dated 07/12/2004, the NJTTF stated, "The goal of the MLA Program is to enhance the maritime environment through increased interaction between MLA members, private industry, state and local port authorities, to include law enforcement and other federal agencies with maritime responsibilities. These enhancements will result from the establishment of close working relationships between the MLAs and concerned entities within the maritime field." The EC goes on to provide additional guidance and an extensive list of recommended liaison contacts, including participation in the local Area Maritime Security Committee (AMSC). In addition to these specific recommendations, every FBI SA, including those designated as MLAs, are evaluated on specific critical elements. One of the core critical elements for all FBI SAs is the development of an intelligence base, which includes source development. This process encompasses identifying, initiating and developing relationships with individuals or organizations that may provide information or assistance in investigations and assignments. Therefore, CTD believes the need for the FBI to develop relationships with people who can inform the FBI about maritime operations has been thoroughly addressed.

As you requested, the MSP has provided responses to pertinent recommendations. Additionally, recommendations not

## REDACTED AND UNCLASSIFIED

Mr. Glenn A. Fine

under MSP's purview were provided to the appropriate offices, (i.e., the DI, the Critical Incident Response Group (CIRG), and CTD's Counterterrorism Analysis Section.) Responses to the recommendations are set forth below.

### **Recommendation #1**

**OIG Recommendation:** Ensure that MLA guidance is consistent with the actual role of MLAs.

**FBI Response:** FBI agrees with this recommendation. The MSP has already made significant progress in this regard.

Through the creation of the MSP website, which contains information on maritime directives, including NSPD-41/HSPD-13, the NSMS and key supporting plans; maritime related statutes; intelligence reports; points of contact; and links to related programs including the DI and the OGC. Information is continually updated or added to the website. The MLAs are notified of information posted to the website via e-mail. The website has generated positive feedback from the MLAs and is a readily available source of standardized information for the field.

The MSP is in the process of planning the 2006 Maritime Liaison Agent Training Conference in Long Beach, California from 04/03-07/2006. This site was specifically chosen because the Port of Long Beach is one of the busiest ports in the United States with a variety of inter-modal transportation systems. The conference will include hands on/familiarization training using various port facilities and vessels. The curriculum for this conference is expected to include presentations on the impact of maritime directives under the NSMS; informant and liaison development; legal issues; enhancing maritime domain awareness; the FBI's capabilities and resources to respond to a maritime incident; and guidance to the field on best practices.

Finally, now that the MSP has responsibility for management of the MLA Program, the MSP will establish specific, quantifiably measurable and attainable goals and objectives that are consistent with the responsibilities assigned to the MLAs, to include recommendations for participation in various local working groups and liaison contacts.

### **Recommendation #2**

**OIG Recommendation:** Assign MLAs based on an assessment of the threat and risk of a terrorist attack to critical seaports.

## REDACTED AND UNCLASSIFIED

Mr. Glenn A. Fine

**FBI Response:** FBI agrees with this recommendation. FBI will ensure that resources are assigned or available necessary to address the risk or threat based on the assessment.

### **Recommendation #3**

**OIG Recommendation:** Measure the amount of resources devoted to maritime efforts by establishing a maritime case classification under the general Counterterrorism Preparedness classification.

**FBI Response:** FBI agrees with this recommendation. The MSP has already taken certain steps which would enhance the FBI's ability to measure the amount of resources devoted to maritime efforts.

FBI is in the process of establishing a classification for maritime matters.

In August 2005, the MSP provided recommendations to the Counterintelligence Division for changes to the Investigative Accomplishment Report (FD-542) to capture activity conducted in support of the MLA Program. Finalization of the modifications to this report are pending.

### **Recommendation #4**

**OIG Recommendation:** Require field offices to name at least one MLA to each AMSC.

**FBI Response:** FBI agrees with this recommendation. FBI will ensure that adequate resources are dedicated to each Area Maritime Security Committee to address priority matters.

### **Recommendation #5**

**OIG Recommendation:** Require field offices to immediately notify the Maritime Security Program of any MLA appointments or reassignments.

**FBI Response:** FBI agrees with this recommendation. The MSP updates the MLA list on a regular basis. The MLA list is maintained by the MSP and is available on the MSP web site. The list identifies, by Field Office, all of the MLAs as well as the JTTF Supervisors who have oversight of the MLA Program. The list provides contact information, identifies if the MLAs are assigned to a Resident Agency (RA) and which ports they cover. The MSP has advised field offices to immediately notify the MSP of any personnel changes affecting the MSP, and this guidance will be

## REDACTED AND UNCLASSIFIED

Mr. Glenn A. Fine

reiterated through training such as the 2006 Maritime Liaison Agent Training Conference.

### **Recommendation #6**

**OIG Recommendation:** Ensure that the Maritime Security Program has measurable objectives.

**FBI Response:** FBI agrees with this recommendation and recognizes that significant changes and progress in the MSP require the establishment of more specific, quantifiably measurable and attainable goals and objectives.

While FBI recognizes that the goals and objectives established for the MSP (via EC dated 08/19/2005) did not include quantifiable measures, it should be noted that the MSP was a new program and no previous goals and objectives had been established. Furthermore, the MSP did not have responsibility for managing the MLA Program at the time the initial objectives were established. The first objective of the MSP was to coordinate with the NJTTF to assume responsibility for the MLA Program.

It is also worth noting that the NSMS and all of the supporting plans were released in the final quarter of 2005, after the date on which these objectives were established. Final directives under the NSMS have not been established, even as of the date of this response. Under these circumstances, it is difficult to quantify the amount of training and/or reference materials required to train MLAs in the field.

Despite the lack of specific, quantifiably measurable objectives at the inception of the program, the MSP accomplished several of the stated objectives, including the following:

- The MSP assumed responsibility for managing the MLA Program on 10/04/2005;
- Training and reference materials to assist the MLAs have been distributed via e-mail, posted to the FBI's Intranet, and will be presented at the 2006 Maritime Liaison Agent Training Conference scheduled to take place 04/03-07/2006;
- The MSP established a web site on the FBI's Intranet where current information including, but not limited to, maritime directives, statutes and intelligence is maintained;



## REDACTED AND UNCLASSIFIED

Mr. Glenn A. Fine

- The MSP continually identifies, analyzes and disseminates information pertaining to maritime threats, vulnerabilities and safety/security issues;
- The MSP continually coordinates with other programs within the FBI to enhance situational awareness for the MSP, other programs, FBIHQ and the field;
- The MSP has already begun to review and track suspicious activity reports to determine if there are any trends which could indicate terrorist activity and has disseminated information to the field in this regard; and
- The MSP is actively engaged in liaison with other government agencies as well as the private sector. This effort and the fact that the MSP serves as a primary point of contact and a coordination center within the FBI for maritime issues has enhanced the FBI's liaison with these groups.

### **Recommendation #7**

**OIG Recommendation:** Ensure that the Maritime Security Program's objectives include developing human intelligence.

**FBI Response:** FBI agrees with this recommendation and asserts that the MSP and the NJTTF have already provided such guidance to the MLAs.

As stated above, at the time the MSP's goals and objectives were established, the MSP did not have responsibility for managing the MLA Program. Even so, the MSP established various objectives for the field. One of these objectives was to "ensure effective liaison between the MLA and various law enforcement agencies, port and shipping officials in respect to counterterrorism preparedness." In the goals and objectives EC, the MSP identified five core competencies which included the establishment of a human intelligence base.

Prior to the existence of the MSP, in an EC to all Field Offices dated 07/12/2004, the NJTTF stated, "The goal of the MLA Program is to enhance the maritime environment through increased interaction between MLA members, private industry, state and local port authorities, to include law enforcement and other federal agencies with maritime responsibilities. These enhancements will result from the establishment of close working relationships between the MLAs and concerned entities within the maritime field..." The EC goes on to provide additional guidance and an extensive list of recommended liaison contacts, including participation in the local AMSC.

REDACTED AND UNCLASSIFIED

Mr. Glenn A. Fine

In addition to these specific recommendations, every FBI SA, including those designated as MLAs, are evaluated on specific critical elements. One of the core critical elements for all FBI SAs is the development of an intelligence base, which includes source development. This process encompasses identifying, initiating and developing relationships with individuals or organizations that may provide information or assistance in investigations and assignments. Therefore, FBI believes the need for the FBI to develop relationships with people who can inform the FBI about maritime operations has been thoroughly addressed.

The MSP also plans to address liaison and the development of a human intelligence base during the 2006 Maritime Liaison Agent Training Conference which is scheduled for 04/03-07/2006. In addition, the MSP will include specific recommendations to the MLAs in the objectives which will be established for FY 2007.

**Recommendation #8**

**OIG Recommendation:** Ensure that the FBI's MOTR operations plan examines high risk scenarios, determines the required response time, and evaluates how FBI resources would address the scenarios.

**FBI Response:** The FBI's maritime operational response plan takes into account various high-risk scenarios to include the criminal/terrorist use of biological, chemical or radiological WMD, as well as Improvised Explosive Devices (IEDs) and Improvised Nuclear Devices (INDs). Other high-risk scenarios include a large number of hostages on a maritime platform and/or the involvement of sophisticated criminal/terrorist adversaries. The TSB's tactical response to maritime threats mirrors the response to any other tactical response. That is, the FBI tactical response is a tiered approach which recognizes that local field offices will respond as necessary (Tier 1), with regional response (Tier 2) added as the evaluation of the situation may dictate. National response, as required (Tier 3), will involve the deployment of the Hostage Rescue Team (HRT), as well as other FBI SWAT teams and possibly the HDRU and the Laboratory's HMRU, as the scenarios would necessitate. Response times vary as a consequence of venue.



**Recommendation #9**

**OIG Recommendation:** Establish a requirement for joint FBI/Coast Guard exercises in field offices assessed as having high-risk seaports.

## REDACTED AND UNCLASSIFIED

Mr. Glenn A. Fine

**FBI Response:** CIRG will require the fourteen (14) field offices that have been given enhanced tactical maritime training to make overtures to the USCG to conduct joint exercises on an annual basis. It should be noted that the FBI is not in a position to require USCG participation, however, the FBI will extend the invitation to the USCG as well as to other appropriate entities.

### **Recommendation #10**

**OIG Recommendation:** Resolve potential role and incident command conflicts in the event of a maritime terrorist incident through joint exercises and, if necessary, a revised and broadened MOU with the Coast Guard.

**FBI Response:** FBI concurs in stating that this is currently being addressed through the revision of the final interagency MOTR Plan. It may be premature to determine if a revised memorandum of understanding (MOU) with the USCG will be necessary until the final MOTR Plan has been approved and vetted through exercises and/or operations. Again, the FBI is not in a position to require the USCG to enter into a renewed MOU.

### **Recommendation #11**

**OIG Recommendation:** Prepare after-action reports after all maritime-related exercises and use the reports to identify and disseminate lessons learned and best practices.

**FBI Response:** This is being addressed in a separate joint initiative within the FBI. It is anticipated an After Action Report (AAR) template will be developed that applies to all critical incidents, special events and exercises. CIRG's Crisis Management Unit (CMU) is responsible for program oversight for the production of AARs per the Manual of Investigative and Operational Guidelines (MIOG), Part 2, section 30-1.8 (1) (a), (b) and (c) which specifically sets out the requirements for AARs.

### **Recommendation #12**

**OIG Recommendation:** Ensure that all field offices submit critical incident reports to the CIRG by January 15 each year; require the FBI's Maritime Security Program, in consultation with the CIRG, to use the reports to conduct maritime-specific reviews of the FBI's crisis management policies and practices - including any requirements for field office crisis management plans - and to disseminate maritime-related lessons learned and best practices.

REDACTED AND UNCLASSIFIED

Mr. Glenn A. Fine

**FBI Response:** CIRG's CMU ensures adherence to the MIOG's Part 2, section 30-1.8 which requires that field offices submit critical incident reports to CIRG by January 15th of each year. CTD's MSP will provide information concerning maritime related lessons learned and best practices.

**Recommendation #13**

**OIG Recommendation:** Assess the threat and risk of maritime terrorism compared to other terrorist threats and ensure the National Threat Assessment ranks the various modes of attack and targets.

**FBI Response:** FBI will ensure that intelligence gaps are identified and action is initiated to resolve any deficiencies.

**Recommendation #14**

**OIG Recommendation:** Ensure the amount of FBI resources dedicated to maritime terrorism is based on the extent of the maritime threat in relation to other threats.

**FBI Response:** FBI agrees with this recommendation. FBI will ensure that adequate resources are allocated to address priority threats.

**Recommendation #15**

**OIG Recommendation:** Monitor the progress of operating divisions and field offices in answering intelligence collection requirements pertaining to seaports and maritime terrorism.

**FBI Response:** The Directorate of Intelligence will provide a response to this recommendation.

**Recommendation #16**

**OIG Recommendation:** Focus intelligence reporting to more comprehensively address potential maritime-related terrorist targets and methods.

**FBI Response:** The Directorate of Intelligence will provide a response to this recommendation.

**Recommendation #17**

**OIG Recommendation:** Name a unit within the Counterterrorism Division to monitor the volume and substance of all FBI maritime-related intelligence.

REDACTED AND UNCLASSIFIED

Mr. Glenn A. Fine

**FBI Response:** FBI Counterterrorism Division will ensure that Maritime related intelligence as well as investigations are monitored and properly managed.

**Recommendation #18**

**OIG Recommendation:** Consider establishing a requirement for regular field office intelligence bulletins to summarize the field office's suspicious incident reporting and, if such a requirement is adopted, establish standardized frequency, content, and distribution requirements.

**FBI Response:** The Directorate of Intelligence will provide a response to this recommendation.

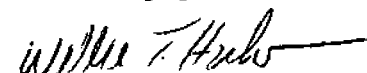
The FBI has prepared the appropriate responses to the recommendations found in your report. The responses have undergone a classification review (Enclosure 1) and Sensitivity Review (Enclosure 2).

The responses were coordinated through the FBI's Inspection Division. Please contact Shirlene Savoy of the Inspection Division should you have any questions. Ms. Savoy can be reached at (202) 324-1833.

I want to thank you again for your efforts in producing this report, and I welcome the opportunity to discuss in detail the progress the FBI continues to make in this area.

Please contact me should you have any questions regarding this matter.

Sincerely yours,



Willie T. Hulon  
Assistant Director  
Counterterrorism Division

REDACTED AND UNCLASSIFIED



U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to  
File No.

March 23, 2006

The Honorable Glenn A. Fine  
Inspector General  
Office of the Inspector General  
United States Department of Justice  
Room 4322  
950 Pennsylvania Avenue, Northwest  
Washington, D.C. 20530

Dear Mr. Fine:

I would like to thank you for providing the Federal Bureau of Investigation (FBI) the opportunity to respond to your report entitled, "The FBI's Efforts to Prevent and Respond to Maritime Terrorism."

I have reviewed the recommendations made in the report which pertain to intelligence collection and production issues. Our responses are set forth below.

**15. Monitor the progress of operating divisions and field offices in answering intelligence collection requirements pertaining to seaports and maritime terrorism.**

The FBI agrees with this recommendation, and notes that such monitoring is part of the normal business process of our Intelligence Program. It is a shared responsibility of both our Headquarters and Field Office executive management.

The Directorate of Intelligence (DI) has partnered with the Information Technology Operations Division to enhance the FBI's Intelligence Information Report Dissemination System (FIDS) during Fiscal Year (FY) 2006 and FY 2007 to incorporate a capability to produce management reports to evaluate the quality of FBI raw intelligence reporting. Inherent in these expected enhancements is the ability to identify reporting that is responsive to specific intelligence requirements.

We recently worked with the Inspection Division to revise all appropriate inspection review documents, which we believe will strengthen the inspection review of critical intelligence processes, including the collection and production of intelligence against published requirements.

- 96 -

REDACTED AND UNCLASSIFIED

## REDACTED AND UNCLASSIFIED

**16. Focus intelligence reporting to more comprehensively address potential maritime-related terrorist targets and methods.**

The FBI agrees with this recommendation, and notes that actions related to it were initiated prior to the OIG inquiry.

The FBI has established maritime and seaport intelligence requirements within its International Terrorism Standing Intelligence Requirements Set and other related requirements sets. The FBI has integrated related requirements received from the Office of Naval Intelligence and the U.S. Northern Command and will continue to incorporate maritime and seaport requirements issued by the intelligence and homeland security communities that are within the FBI's capability and authority to collect.

We note, however, the intelligence reporting is tied to the collection of intelligence that merits reporting when viewed against requirements. The FBI, like other members of the U.S. Intelligence Community, takes its principal guidance from the priority intelligence requirements set forth by the Director of National Intelligence in the National Intelligence Priorities Framework. While this recommendation focuses on reporting, it is important to understand that collection capabilities against requirements form the basis for reporting.

We were informed that this recommendation was also intended to address the production of analytic reports which adequately considered maritime-related terrorist methods of attack, e.g. weapons of mass destruction, when that reporting was found in Intelligence Information Reports. This issue will be addressed in the weekly Intelligence Production Board discussions between senior intelligence managers.

**18. Consider establishing a requirement for regular field office intelligence bulletins to summarize the field office's suspicious incident reporting and, if such a requirement is adopted, establish standardized frequency, content, and distribution requirements.**

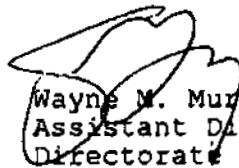
The FBI agrees to consider this recommendation, and notes that in September 2005, the FBI issued policy and procedural guidance to its Field Offices with respect to the production of Intelligence Bulletins. This guidance addressed content, frequency of production, and customer distribution.

REDACTED AND UNCLASSIFIED

The CTD Threat Monitoring Unit currently produces quarterly summaries of suspicious incident reports originating from all 56 field office territories using the GUARDIAN system. This unit plans to start producing monthly reports, by regions of the country, which provide material that can logically be incorporated into periodic Intelligence Bulletins disseminated by Field Offices.

My staff is available for any additional follow-up to the recommendations and issues discussed herein.

Sincerely,



Wayne M. Murphy  
Assistant Director  
Directorate of Intelligence



## APPENDIX VI

**OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE REPORT**

The OIG provided a draft of this audit report to the FBI on March 6, 2006, for its review and comment. The FBI provided written responses to the draft report, which are included as Appendix 5 of this final report. The response from the Counterterrorism Division, dated March 17, 2006, addresses 15 of the report's recommendations. The response from the Directorate of Intelligence, dated March 23, 2006, addresses the remaining 3 recommendations. The FBI agreed with the 18 recommendations in the audit report and provided both general comments and technical comments. We incorporated the technical comments into the report as appropriate.

**FBI's General Comments**

In its response, the FBI noted that it had created its Maritime Security Program without additional funding, that resource availability influences its participation in maritime exercises, and that it is working with the Coast Guard to resolve potential coordination issues in advance of any terrorist threat or incident in the maritime domain. In addition, the FBI provided updates on the activities of the Maritime Security Program in the areas of suspicious incident and threat reporting, training, information sharing, and implementation of the National Strategy for Maritime Security.

**Status of Recommendations**

1. **Resolved.** The FBI agreed with the recommendation and described three initiatives intended to ensure that the guidance provided to Maritime Liaison Agents is consistent with the actual role of MLAs. This recommendation can be closed when we receive documentation that shows the guidance provided to MLAs is consistent with their actual role.
2. **Resolved.** The FBI agreed with the recommendation and reported that it will ensure that resources are assigned, or made available, to address the assessed threat and risk of a terrorist attack. This recommendation can be closed when we receive documentation

REDACTED AND UNCLASSIFIED

that shows the FBI has assigned its MLAs based on an assessment of the threat and risk of a terrorist attack to critical seaports.

3. **Resolved.** The FBI agreed with the recommendation and described two steps the Maritime Security Program has taken to address the recommendation. This recommendation can be closed when we receive documentation that shows the FBI has established a maritime case classification under the general Counterterrorism Preparedness classification.
4. **Resolved.** The FBI agreed with the recommendation and stated that the FBI would ensure that it devotes adequate resources to Area Maritime Security Committees. This recommendation can be closed when we receive documentation that shows the FBI has named at least one MLA to each AMSC.
5. **Resolved.** The FBI agreed with the recommendation and stated that the MSP updates the MLA list regularly. This recommendation can be closed when we receive documentation that shows the FBI has required its field offices to immediately notify the MSP of any MLA appointments or reassignments.
6. **Resolved.** The FBI agreed with the recommendation and stated that it recognized that significant changes to the MSP require the program to have more specific and quantifiable goals and objectives. This recommendation can be closed when we receive documentation that shows the FBI has established measurable objectives for the MSP.
7. **Resolved.** The FBI agreed with the recommendation and stated that it believed that the MSP and the National Joint Terrorism Task Force had provided guidance to MLAs on developing human intelligence. We agree that the electronic communication outlining the MSP's goals and objectives identifies five core competencies of the FBI, including the ability to establish a human intelligence base, and states that the MSP will be built upon those competencies. However, the MSP's goals and objectives do not make it clear how this competency will be used. The intent of our recommendation is to ensure that that MSP build a base of informants with knowledge about port operations that cannot be obtained through increased interaction with law enforcement, other federal agencies, port authorities, and the private sector.

## REDACTED AND UNCLASSIFIED

This recommendation can be closed when we receive documentation showing that the MSP's objectives include developing human intelligence.

8. **Resolved.** This recommendation is resolved based on the FBI reporting that its maritime operational response plan examines various high-risk scenarios and evaluates how FBI resources would address the scenarios. This recommendation can be closed when we receive documentation that shows that the FBI's Maritime Operational Threat Response plan examines high-risk scenarios, determines the required response times, and evaluates how FBI resources would address the scenarios.
9. **Resolved.** This recommendation is resolved based on the FBI reporting that the Critical Incident Response Group will require the 14 field offices with enhanced maritime SWAT teams to annually invite the Coast Guard to participate in joint exercises. This recommendation can be closed when we receive documentation that shows that the FBI has established a requirement for joint FBI-Coast Guard exercises in field offices assess as having high-risk seaports.
10. **Resolved.** This recommendation is resolved based on the FBI reporting that is actively attempting to resolve potential role and incident command issues that may occur with the Coast Guard in the event of a maritime terrorist incident. This recommendation can be closed when we receive documentation that shows that the FBI has resolved potential role and incident command conflicts in the event of a maritime terrorist incident through joint exercises and, if necessary, a revised and broadened memorandum of understanding with the Coast Guard.
11. **Resolved.** This recommendation is resolved based on the FBI reporting that a current initiative will develop a template for after-action reports that will apply to all critical incidents, special events and exercises. This recommendation can be closed when we receive documentation that shows that the FBI prepares after-action reports after all maritime-related exercises and uses the reports to identify and disseminate lessons learned and best practices.

REDACTED AND UNCLASSIFIED

12. **Resolved.** This recommendation is resolved based on the FBI stating that the Crisis Management Unit will ensure that all field offices comply with annual critical incident reporting requirements and that the MSP will provide the CMU with maritime-related lessons learned and best practices. This recommendation can be closed when we receive documentation that shows that the FBI: (1) has ensured that all field offices submit critical incident reports to the Critical Incident Response Group by January 15 each year, and (2) requires its MSP, in consultation with CIRG, to use the reports to conduct maritime-specific reviews of the FBI's crisis management policies and practices and to disseminate maritime-related lessons learned and best practices.
13. **Resolved.** This recommendation is resolved based on the FBI reporting that it will ensure that intelligence gaps are identified and action is taken to resolve any deficiencies. This recommendation can be closed when we receive documentation that shows that the FBI has assessed the threat and risk of maritime terrorism compared to other terrorist threats and ensures the National Threat Assessment ranks the various modes of attack and targets.
14. **Resolved.** The FBI agreed with the recommendation and stated that it would ensure that adequate resources are allocated to address priority threats. This recommendation can be closed when we receive documentation that shows the FBI has ensured the amount of resources dedicated to maritime terrorism is based on the extent of the maritime threat in relation to other threats.
15. **Resolved.** The FBI agreed with the recommendation and described two initiatives intended to ensure that its intelligence reporting is responsive to its intelligence requirements. This recommendation can be closed when we receive documentation that shows the FBI monitors the progress of operating divisions and field offices in answering intelligence collection requirements pertaining to seaports and maritime terrorism.
16. **Resolved.** The FBI agreed with the recommendation and reported that its Intelligence Production Board, made up of senior intelligence managers, would ensure that the FBI's analytic products adequately address maritime-related terrorist methods. The Directorate of Intelligence noted that the ability to collect

REDACTED AND UNCLASSIFIED

intelligence against a specific requirement is based on the availability and capability of sources and terrorist activities. This recommendation can be closed when we receive documentation that shows the FBI is focusing its intelligence reporting to more comprehensively address potential maritime-related terrorist targets and methods.

17. **Resolved.** This recommendation is resolved based on the FBI's reporting that the Counterterrorism Division will ensure that maritime-related intelligence is monitored and properly managed. This recommendation can be closed when receive documentation showing the FBI has named a unit within the Counterterrorism Division to monitor the volume and substance of all FBI maritime-related intelligence.
18. **Resolved.** The FBI agreed to consider the recommendation and noted that in September 2005 it had issued guidance to its field offices on the content, frequency, and dissemination of intelligence bulletins. This recommendation can be closed when we receive documentation indicating that the FBI considered establishing a requirement for regular field office intelligence bulletins to summarize the field office's suspicious incident reporting. If such a requirement is adopted, closure of the recommendation will require documentation showing that the FBI established standardized frequency, content, and distribution requirements.