United States Government Accountability Office

GAO

Report to Congressional Requesters

November 2011

COAST GUARD

Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations

November 2011

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-14, a report to congressional requesters

COAST GUARD

Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations

Why GAO Did This Study

Since the terrorist attacks of September 11, 2001, the nation's ports and waterways have been viewed as potential targets of attack. The Department of Homeland Security (DHS) has called for using risk-informed approaches to prioritize its investments, and for developing plans and allocating resources that balance security and the flow of commerce. The U.S. Coast Guard—a DHS component and the lead federal agency responsible for maritime security—has used its Maritime Security Risk Analysis Model (MSRAM) as its primary approach for assessing and managing security risks. GAO was asked to examine (1) the extent to which the Coast Guard's risk assessment approach aligns with DHS risk assessment criteria, (2) the extent to which the Coast Guard has used MSRAM to inform maritime security risk decisions, and (3) how the Coast Guard has measured the impact of its maritime security programs on risk in U.S. ports and waterways. GAO analyzed MSRAM's risk assessment methodology and interviewed Coast Guard officials about risk assessment and MSRAM's use across the agency.

What GAO Recommends

GAO recommends that the Coast Guard provide more thorough documentation on MSRAM's assumptions and other sources of uncertainty, make MSRAM available for peer review, implement additional MSRAM training, and report the results of its risk reduction performance measure in a manner consistent with risk analysis criteria. The Coast Guard agreed with these recommendations.

View GAO-12-14. For more information, contact Stephen L. Caldwell at (202) 512-9610 or caldwells@gao.gov.

What GAO Found

MSRAM generally aligns with DHS risk assessment criteria, but additional documentation on key aspects of the model could benefit users of the results. MSRAM generally meets DHS criteria for being complete, reproducible, documented, and defensible. Further, the Coast Guard has taken actions to improve the quality of MSRAM data and to make them more complete and reproducible, including providing training and tools for staff entering data into the model. However, the Coast Guard has not documented and communicated the implications that MSRAM's key assumptions and other sources of uncertainty have on MSRAM's risk results. For example, to assess risk in MSRAM, Coast Guard analysts make judgments regarding such factors as the probability of an attack and the economic and environmental consequences of an attack. These multiple judgments are inherently subjective and constitute sources of uncertainty that have implications that should be documented and communicated to decision makers. Without this documentation, decision makers and external MSRAM reviewers may not have a complete understanding of the uses and limitations of MSRAM data. In addition, greater transparency and documentation of uncertainty and assumptions in MSRAM's risk estimates could also facilitate periodic peer reviews of the model—a best practice in risk management.

MSRAM is the Coast Guard's primary tool for managing maritime security risk, but resource and training challenges hinder use of the tool by Coast Guard field operational units, known as sectors. At the national level, MSRAM supports Coast Guard strategic planning efforts, which is consistent with the agency's intent for MSRAM. At the sector level, MSRAM has informed a variety of decisions, but its use has been limited by lack of staff time, the tool's complexity, and competing mission demands, among other things. The Coast Guard has taken actions to address these challenges, but providing additional training on how MSRAM can be used at all levels of sector decision making could further the Coast Guard's risk management efforts. MSRAM is capable of informing operational, tactical, and resource allocation decisions, but the Coast Guard has generally provided MSRAM training only to a small number of sector staff who may not have insight into all levels of sector decision making.

The Coast Guard developed an outcome measure to report its performance in reducing maritime risk, but has faced challenges using this measure to inform decisions. Outcome measures describe the intended result of carrying out a program or activity. The measure is partly based on Coast Guard subject matter experts' estimates of the percentage reduction of maritime security risk subject to Coast Guard influence resulting from Coast Guard actions. The Coast Guard has improved the measure to make it more valid and reliable and believes it is a useful proxy measure of performance, noting that developing outcome measures is challenging because of limited historical data on maritime terrorist attacks. However, given the uncertainties in estimating risk reduction, it is unclear if the measure would provide meaningful performance information with which to track progress over time. In addition, the Coast Guard reports the risk reduction measure as a specific estimate rather than as a range of plausible estimates, which is inconsistent with risk analysis criteria. Reporting and using outcome measures that more accurately reflect mission effectiveness can give Coast Guard leaders and Congress a better sense of progress toward goals.

Contents

Abbreviations

CREATE	National Center for Risk and Economic Analysis of Terrorism Events
DHS	Department of Homeland Security
EGIS	Enterprise Geographic Information System
ICC	Intelligence Coordination Center
IMPLAN	Impact Analysis for Planning
IV&V	independent verification and validation
MCIKR	maritime critical infrastructure and key resources
MSRAM	Maritime Security Risk Analysis Model
MSRO	Maritime Security and Response Operations
MTSA	Maritime Transportation Security Act of 2002
NIPP	*National Infrastructure Protection Plan*
OMB	Office of Management and Budget
PSRAT	Port Security Risk Assessment Tool
PWCS	Ports, Waterways, and Coastal Security
VV&A	verification, validation, and accreditation

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

November 17, 2011

The Honorable John D. Rockefeller, IV
Chairman
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Candice S. Miller
Chairwoman
Subcommittee on Border and Maritime Security
Committee on Homeland Security
House of Representatives

Since the terrorist attacks of September 11, 2001, the nation's ports have been viewed as potential targets of attack for many reasons. Ports, waterways, and vessels are part of an economic engine handling more than $700 billion in merchandise annually, according to the Department of Homeland Security (DHS), and an attack on this system could have a widespread impact on global shipping, international trade, and the U.S. economy. The U.S. Coast Guard—a component of DHS—is the lead federal agency for maritime security, which includes the protection of U.S. ports, coasts, and inland waterways as part of its Ports, Waterways, and Coastal Security (PWCS) mission. This mission involves protecting the maritime domain and marine transportation system, including preventing terrorist attacks, and responding to and recovering from attacks that do

occur. In addition to its PWCS mission, the Coast Guard has 10 other statutory missions.[1]

Since it is not practical or economically feasible to protect all assets against every possible terrorist risk, DHS has called for using risk-informed approaches to prioritize its investments and for developing plans and allocating resources that balance security and the flow of commerce. Risk management is a tool for informing policymakers' decisions about assessing risks, allocating resources, and taking actions under conditions of uncertainty. 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. DHS detailed this approach in its *National Infrastructure Protection Plan* (NIPP), which it issued in June 2006 and updated in 2009.[2] The 2009

[1]The Coast Guard's 11 statutory missions are (1) PWCS, (2) migrant interdiction, (3) defense readiness, (4) drug interdiction, (5) other law enforcement, (6) search and rescue, (7) living marine resources, (8) Aids to Navigation, (9) ice operations, (10) marine environmental protection, and (11) marine safety. 6 U.S.C. § 468. Organizationally, the Coast Guard is divided into headquarters and several field commands including; the Atlantic and Pacific Areas; 9 districts; and 35 sectors, which are operational units that carry out the full range of Coast Guard missions. There are 35 geographically-based Coast Guard sectors in the continental United States, Alaska, Hawaii, Puerto Rico, and Guam.

[2]DHS, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009). The NIPP is the document that articulates the risk management framework for DHS. The NIPP defines risk as a function of threat, vulnerability, and consequence. Threat is an indication of the likelihood that a specific type of attack will be initiated against a target. Vulnerability is the probability that a particular attempted attack will succeed against a particular target. Consequence is the effect of a successful attack. For more information on the NIPP, see GAO, *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*, GAO-10-296 (Washington, D.C.: Mar. 5, 2010).

update of the NIPP increased the plan's emphasis on risk management, including providing the core criteria of a risk assessment approach.[3]

The Coast Guard's primary approach to assessing and managing security risks has been embodied in its Maritime Security Risk Analysis Model (MSRAM). Since its development and implementation in 2005, MSRAM has provided the Coast Guard with a standardized way of assessing risk to maritime infrastructure, referred to in MSRAM as targets, which can include chemical facilities, oil refineries, hazardous cargo vessels, passenger ferries, and cruise ship terminals, to name a few. MSRAM is designed to allow comparison between different targets at the local, regional, and national levels with the goal of reducing risk by prioritizing security activities and resources. MSRAM calculates the risk of terrorist attack based on scenarios—a combination of target and attack mode—in terms of threats, vulnerabilities, and consequences to more than 28,000 maritime targets. For example, a MSRAM scenario related to cruise ships could include a boat bomb or an attack by a hijacked vessel.

Since 2004, we have examined Coast Guard efforts to implement a risk management framework, noting how the Coast Guard's risk management and risk assessment efforts have developed and evolved, as well as how the Coast Guard has made progress in assessing maritime security risks using MSRAM. For example, in 2005, we reported that by developing MSRAM, the Coast Guard had begun to address the limitations of its previous port security risk model.[4] In 2010, we reported that the Coast Guard has strengthened risk management through the development and use of MSRAM to help prioritize limited port security resources, identify capabilities needed to combat future threats, and identify the highest-risk

[3]According to the NIPP, risk assessments should be complete, reproducible, documented, and defensible. To be complete, the methodology should assess *consequence, vulnerability*, and *threat* for every defined risk scenario. To be reproducible, the methodology must produce comparable, repeatable results, and must minimize the number of subjective judgments. To be documented, the methodology and the assessment must clearly document what information is used and how it is synthesized to generate a risk estimate. To be defensible, the methodology must logically integrate its components and be free from significant errors or omissions. These core criteria are described in detail later in this report.

[4]GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91 (Washington, D.C.: Dec. 15, 2005).

scenarios and targets in the maritime domain.[5] We also reported in 2010 that the Coast Guard was assessing risk to cruise ships and facilities in accordance with DHS risk assessment guidance and that the Coast Guard was using MSRAM to help concentrate maritime security activities where relative risk is believed to be greatest.[6] In light of the tight fiscal environment combined with the Coast Guard's multiple missions, it is critically important for the Coast Guard to make the most effective use of its limited resources and to ensure that all levels of the Coast Guard are equipped to make risk-informed decisions regarding maritime security.

You asked us to examine the Coast Guard's progress in using MSRAM to assess and manage maritime security risk and to assess its progress implementing DHS's risk management framework—specifically, how the Coast Guard is establishing security priorities based on risk, implementing protective programs and strategies, and measuring the effectiveness of its actions. This report addresses the following questions:

- To what extent does the Coast Guard's risk assessment approach align with DHS risk assessment criteria, and what challenges, if any, exist in this effort?
- To what extent has the Coast Guard used MSRAM to inform maritime security risk decisions, and what challenges, if any, exist in this effort?
- How has the Coast Guard measured the impact of its maritime security programs on risk in U.S. ports and waterways, and what challenges, if any, exist in this effort?

To address our first objective, we focused on MSRAM, which is the Coast Guard's primary model for assessing maritime security risk. We compared MSRAM's risk assessment methodology and processes to relevant criteria, including the risk assessment component of the 2009 NIPP and our related reports on risk management, such as our 2005 report examining Coast Guard risk management efforts.[7] We interviewed

[5]GAO, *Maritime Security: DHS Progress and Challenges in Key Areas of Port Security*, GAO-10-940T (Washington, D.C.: July 21, 2010).

[6]GAO, *Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain*, GAO-10-400 (Washington, D.C.: Apr. 9, 2010).

[7]GAO-06-91.

Coast Guard headquarters officials to discuss their national-level perspectives on the overall management and implementation of the MSRAM risk model and we interviewed officials from the Coast Guard's Intelligence Coordination Center to discuss how intelligence information is incorporated into MSRAM.[8] In addition, we interviewed officials from all 35 Coast Guard sectors to obtain their views on MSRAM. We asked these officials to provide information on the MSRAM risk assessment process, MSRAM training, and processes and procedures for ensuring MSRAM data integrity. The interview was a mix of specific questions using a rating scale and questions asking for open-ended or narrative responses. During these interviews, we interviewed staff responsible for collecting and updating MSRAM data, as well as management-level officials in the sectors' response, prevention, planning, and command units. To minimize any inconsistencies or errors in the information we collected, our subject matter experts developed the interview questions in collaboration with a social science survey specialist and we pretested the interview with officials from two Coast Guard sectors. We provided an advance copy of the interview questions to each of the sectors to allow time to prepare responses, conduct preliminary research, and identify appropriate points of contact. We also validated selected interview response information by corroborating it with other sources, such as MSRAM documentation provided by the Coast Guard. We conducted these interviews from May 2011 through August 2011. We also conducted interviews with officials from three of the nine Coast Guard districts to obtain their perspectives on MSRAM. These districts encompass 15 sectors over the West Coast, East Coast, Gulf Coast, and Mississippi River area. Since we selected a nonprobability sample of districts, the information obtained from these interviews cannot be generalized to all districts but provides us with information on how officials from these selected districts view MSRAM. In addition, we reviewed external studies on MSRAM, including a MSRAM verification and validation report[9] and a report by the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) at the University of

[8]We did not review or validate the intelligence information incorporated in MSRAM.

[9]Dr. Ted Lewis and Dr. Thomas J. Mackin, Naval Postgraduate School, *Maritime Security Risk Analysis Model (MSRAM) Independent Verification and Validation (IV&V) Report*, prepared for the Coast Guard Research and Development Center, March 2010.

Southern California,[10] and we met with the author of the MSRAM verification and validation report to discuss the report's findings and recommendations. We also reviewed the National Research Council of the National Academies study on DHS risk models and spoke with individuals involved in conducting that study.[11] Although this study did not specifically review MSRAM, it provided broad information on risk analysis and modeling applicable to MSRAM. We reviewed the methodologies of these studies and found them sufficiently reliable for the purposes of our report. In addition, we met with risk management experts from DHS's Office of Risk Management and Analysis to obtain their views on risk analysis. We also met with an external risk management expert familiar with MSRAM and Coast Guard risk management efforts to gain additional perspective on MSRAM. While our review focused on MSRAM, we also obtained information regarding other Coast Guard risk management models that are under development to see how these models are expected to align with MSRAM.

To address our second objective, we also focused on MSRAM because it is the Coast Guard's primary maritime security risk management tool. We reviewed Coast Guard documents describing MSRAM's current and intended uses at headquarters and in the field. We also relied on the interviews with officials from the 35 Coast Guard sectors and the 3 Coast Guard districts as previously described. During these interviews, we obtained information on how sectors and districts use MSRAM at the local level to guide tactical, operational, and strategic security efforts and strengths and limitations of MSRAM for these purposes. Based on the information provided by these interviews, we compared sectors' reported uses of MSRAM for informing risk-based decision making with Coast Guard documentation on the intended uses of MSRAM, including Commandant Instructions and internal Coast Guard risk management guidance documents. We verified the intended uses of MSRAM with

[10]A. Barret et al., *Evaluation of U.S. Coast Guard Terrorism Risk and Decision Analysis Models and Processes for Port, Waterways and Coastal Security* (Los Angeles: National Center for Risk and Economic Analysis of Terrorism Events, University of Southern California, 2009). Established in 2004, CREATE is an interdisciplinary national research center based at the University of Southern California and funded by the U.S. Department of Homeland Security. CREATE is focused on risk and economic analysis of the United States and comprises a team of experts from across the country, including partnerships with numerous universities and research institutions.

[11]National Research Council of the National Academies, *Review of the Department of Homeland Security's Approach to Risk Analysis* (Washington, D.C.: 2010).

officials from Coast Guard headquarters. At Coast Guard headquarters, we interviewed personnel from Coast Guard offices that use MSRAM information to support decision making, as well as officials responsible for developing risk assessment training standards within the Coast Guard.

To address our third objective, we focused on the Coast Guard's risk reduction performance measure and its supporting model. This measure is the Coast Guard's primary method for measuring and reporting its overall performance in reducing risk in the maritime domain. We reviewed Coast Guard documentation on the risk reduction measure and supporting model, as well as relevant criteria, including our criteria for performance measurement,[12] the NIPP framework, and the Office of Management and Budget (OMB) *Updated Principles for Risk Analysis*.[13] Additionally, we interviewed Coast Guard officials to discuss how the risk reduction measure and supporting model are used as well as recent and planned improvements. We also discussed the Coast Guard's risk reduction measure with a senior DHS official responsible for reviewing department and component-level performance measures.

We conducted this performance audit from October 2010 through November 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[12]See, for example, GAO, *Managing for Results: Enhancing Agency Use of Performance Information for Management Decision Making*, GAO-05-927 (Washington, D.C.: Sept. 9, 2005); *Managing for Results: Challenges Agencies Face in Producing Credible Performance Information*, GAO/GGD-00-52 (Washington, D.C.: Feb. 4, 2000); and *The Results Act: An Evaluator's Guide to Assessing Agency Annual Performance Plans,* GAO/GGD-10.1.20 (Washington, D.C.: April 1998).

[13]OMB, *Updated Principles for Risk Analysis*, Memorandum M-07-Z4 (Washington, D.C.: Sept. 19, 2007).

Background

Risk Management

In recent years, we, Congress, the 9/11 Commission, and others have recommended that federal agencies with homeland security responsibilities utilize a risk management approach to help ensure that finite resources are dedicated to assets or activities considered to have the highest security priority. The purpose of risk management is not to eliminate all risks, as that is an impossible task. Rather, given limited resources, risk management is a structured means of making informed trade-offs and choices about how to use available resources effectively and monitoring the effect of those choices. Thus, risk management is a continuous process that includes the assessment of threats, vulnerabilities, and consequences to determine what actions should be taken to reduce or eliminate one or more of these elements of risk.

To provide guidance to agency decision makers, we developed a risk management framework, which is intended to be a starting point for applying risk-informed principles. Our risk management framework 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. Additional information on risk management, including our risk management framework, can be found in appendix I.

DHS is required by statute to utilize risk management principles with respect to various DHS functions.[14] With regard to the Coast Guard, federal statutes call for the Coast Guard to use risk management in specific aspects of its homeland security efforts. The Maritime Transportation Security Act of 2002 (MTSA), for example, calls for the Coast Guard and other port security stakeholders, through implementing regulations, to carry out certain risk-based tasks, including assessing risks and developing security plans for ports, facilities, and vessels.[15] In

[14]For example, the Homeland Security Act of 2002 (Pub. L. No. 107-296, §201, 116 Stat. 2135, 2146 (2002)) requires DHS to perform risk assessments of key resources and critical infrastructure, and the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. No. 108-458, §4001, 118 Stat. 3638, 3710 (2004)) requires that DHS's National Strategy for Transportation Security include the development of risk-based priorities across all transportation modes.

[15]Pub. L. No. 107-295, 116 Stat. 2064, 2068-72 (2002).

addition, the Coast Guard Authorization Act of 2010 requires, for example, the Coast Guard to (1) develop and utilize a national standard and formula for prioritizing and addressing assessed security risks at U.S. ports and facilities, such as MSRAM; (2) require Area Maritime Security Committees[16] to use this standard to regularly evaluate each port's assessed risk and prioritize how to mitigate the most significant risks; and (3) make MSRAM available, in an unclassified version, on a limited basis to regulated vessels and facilities to conduct risk assessments of their own facilities and vessels.[17]

Coast Guard Security Risk Models

From 2001 to 2006, the Coast Guard assessed maritime security risk using the Port Security Risk Assessment Tool (PSRAT), which was quickly developed and fielded after the terrorist attacks of September 11, 2001. PSRAT served as a rudimentary risk calculator that ranked maritime critical infrastructure and key resources (MCIKR) with respect to the consequences of a terrorist attack and evaluated vessels and facilities that posed a high risk of a transportation security incident. While PSRAT provided a relative risk of targets within a port region, it could not compare and prioritize relative risks of various infrastructures across ports, among other limitations.

Recognizing the shortcomings of PSRAT that had been identified by the Coast Guard and us, in 2005 the Coast Guard developed and implemented MSRAM to provide a more robust and defensible terrorism risk analysis process. MSRAM is a risk-based decision support tool designed to help the Coast Guard assess and manage maritime security risks throughout the Coast Guard's area of responsibility. Coast Guard units throughout the country use this tool to assess security risks to over 28,000 key maritime infrastructure assets—also known as targets—such

[16]Area Maritime Security Committees—with representatives from the federal, state, local, and private sectors—offer a venue to identify and deal with vulnerabilities in and around ports, as well as a forum for sharing information on issues related to port security.

[17]Pub. L. No. 111-281, 124 Stat. 2905, 3004-05 (2010). In response to this statutory requirement, the Coast Guard developed the Industry Risk Analysis Model (IRAM). IRAM is a risk analysis tool that allows owners/operators of port facilities or vessels to perform a terrorism-focused, security risk analysis of their property. The intended uses of IRAM results are to characterize the terrorism risk for a specific asset as evaluated by the owner/operator, provide a risk-based planning capability for updating facility or vessel operations plans, and provide a means to communicate risk between owners/operators and first responders. The Coast Guard expects to release IRAM in fall 2011.

as chemical facilities, passenger terminals, and bridges, as well as vessels such as cruise ships, ferries, and vessels carrying hazardous cargoes, among other things.[18] Unlike PSRAT, MSRAM is designed to capture the security risks facing different types of targets, allowing comparison between different targets and geographic areas at the local, regional, and national levels. MSRAM's risk assessment methodology assesses the risk of a terrorist attack based on different scenarios; that is, it combines potential targets with different attack modes for each target/attack mode combination (see table 1). MSRAM automatically determines which attack modes are required to be assessed for each target type, though local MSRAM analysts have the ability to evaluate additional optional attack modes against any target.[19] For each target/attack mode combination, MSRAM can provide different risk results, such as the inherent risk of a target and the amount of risk mitigated by Coast Guard security efforts.

[18]The Coast Guard requires that at a minimum, MSRAM's list of targets should include all MTSA-regulated facilities, vessels, and barges. Department of Defense vessels and facilities, such as submarines, aircraft carriers, or naval bases, are optional in MSRAM. Smaller targets such as recreational boats, small commercial vessels, small waterside retail stores, and other targets with limited consequence potential should not be listed.

[19]MSRAM does not address the use of the maritime transportation system as a means of transferring weapons or terrorists into the country.

Table 1: Target Types and Attack Modes in MSRAM

Examples of target types	Examples of attack modes
• MTSA-regulated facilities and offshore platforms • Domestic/foreign barges carrying certain dangerous cargoes • Certain vessels • Key infrastructure (e.g., pipelines, bridges, and tunnels) • Key assets (e.g., nuclear power plants and dams) • Non-regulated high consequence targets that are critical to port operations (e.g., non-maritime bridges feeding the port area) • Non-regulated high consequence targets that are plausibly attackable from boat bombs, such as high-rise buildings located directly on water • Special events and waterside attractions • Targets involved in military outloads	• Boat bomb • Truck bomb • Small suicide aircraft • Swimmer/diver/underwater delivery systems • Passenger/passerby explosives/improvised explosive device • Mines (aquatic) • Attack by hijacked vessel • Attack by hijacked large aircraft • Attack by terrorist assault team • Sabotage • Boat bomb (while vessel is present) • Multiple boat attack

Source: U.S. Coast Guard.

MSRAM calculates risk using the following risk equation: Risk = Threat x Vulnerability x Consequence. Numerical values representing Coast Guard's assessment of threat (or relative likelihood of attack), vulnerability should an attack occur, and consequences of a successful attack are combined to yield a risk score for each maritime target. The model calculates risk using threat judgments provided by the Coast Guard Intelligence Coordination Center (ICC), and vulnerability and consequence judgments provided by MSRAM users at the sector level—typically Coast Guard port security specialists—which are reviewed at the district, area, and headquarters levels. The risk equation variables are as follows:

Threat

Threat represents the relative likelihood of an attempted attack on a target. The ICC provides threat probabilities to MSRAM, based upon judgments regarding specific intent, capability, and geographic preference of terrorist organizations to deliver an attack on a specific type of maritime target class—for example, a boat bomb attack on a ferry terminal. To make these judgments, ICC officials use intelligence reports generated throughout the broader intelligence community to make qualitative determinations about certain terrorist organizations and the threat they

pose to the maritime domain. At the sector level, Coast Guard MSRAM users do not input threat probabilities and are required to use the threat probabilities provided by the ICC. This approach is intended to ensure that threat information is consistently applied across ports.

Vulnerability

Vulnerability represents the probability of a successful attack given an attempt. MSRAM users at the sector level assess the vulnerability of targets within their respective areas of responsibility. Table 2 shows the factors included in the MSRAM vulnerability assessment.

Table 2: Description of Vulnerability Factors in MSRAM

Vulnerability factors	Definitions
Achievability	A measure of the ability to successfully attack the target in the absence of security measures. This factor is designed to capture the innate degree of difficulty of the attack on a target. For example, weather or climate requirements for the scenario (wind, temperature, etc.) may alter the potential likelihood of the attack.
System security	A measure of the probability that the security strategy in place, made up of the owner/operator, law enforcement agencies, or the Coast Guard, will successfully interdict a terrorist attack before it occurs.
Target hardness	A measure of the target's ability to physically withstand the specific attack type.

Source: U.S. Coast Guard.

Consequence

Consequence represents the projected overall impact of a successful attack on a given target or asset.[20] Similar to vulnerability assessments, MSRAM users at the sector level assess the consequences of a successful attack on targets within their respective area of responsibility. Table 3 shows the factors included in the MSRAM consequence assessment.

[20]MSRAM's risk assessment process asks users to evaluate each scenario considering the target's reasonable worst-case consequences. The Coast Guard defines this as the "maximum level of consequence for which there is at least a moderate likelihood of the attack mode being able to cause that damage level."

Table 3: Description of Consequence Factors in MSRAM

Consequence factors	Definitions
Death/injury	Represents the expected number of deaths/injuries from a successful attack. This includes both deaths at the time of attack, and deaths that occur later but are still clearly a direct result of the attack (e.g., burn victims, or victims who become sick and die from exposure to chemical or biological agents).
Economic - primary	Represents the expected property damage and immediate business interruption from a successful attack. This includes the actual costs of replacing or repairing maritime infrastructure, as well as business losses resulting from the attack.
Environmental	Represents the expected environmental impacts of a successful attack. This impact predominately captures impacts from oil and oil-like substances.
National security	Represents the expected impact of a successful attack on a target involved in providing national security.
Symbolic	Represents the symbolic impact of a successful attack based on the iconic value of the target in terms of its local, regional, national, and international importance.
Economic - secondary	Represents the expected follow-on economic effects of a successful attack. For example, an attack on a fuel refinery could interrupt energy production and distribution, which is considered a secondary economic effect. This assessment should take into account redundancy and recoverability of the target.

Source: U.S. Coast Guard.

In addition to the consequence factors listed in table 3, sector MSRAM users also assess the response capabilities of the Coast Guard, port stakeholders, and other governmental agencies and their ability to mitigate death/injury, primary economic, and environmental consequences of a successful attack. Because there is a broad array of target types operating in the maritime domain that can result in different types of impacts if successfully attacked, MSRAM uses an approach for drawing equivalencies between the different types of impacts. This approach was based on establishing a common unit of measure, called a

consequence point. One consequence point represents $1 million of equivalent loss to the American public.[21]

To support MSRAM development and risk analysis at the headquarters level, the Coast Guard has provided MSRAM-dedicated staff and resources. According to the Coast Guard, resources for MSRAM or port security risk analysis are not from a specific budget line item. From fiscal year 2006 to fiscal year 2011, the Coast Guard reported assigning from two to five staff (full-time equivalents) and from $0.6 million to $1.0 million annually to support MSRAM at headquarters. There are no MSRAM-dedicated staff at the area, district, and sector levels; rather, MSRAM assessment and analysis is generally conducted by port security specialists, who have other responsibilities. The port security specialist typically has responsibility for numerous activities, including the Port Security Grant Program, Area Maritime Security Committees, and Area Maritime Security Training Exercise Program, among others.

DHS Risk Management Criteria

The NIPP is DHS's primary guidance document for conducting risk assessments and includes core criteria that identify the characteristics and information needed to produce quality risk assessment results. The NIPP's basic analytical principles state that risk assessments should be complete, reproducible, documented, and defensible, as defined in table 4.

[21]For impacts that are quantifiable in nature, such as numbers of fatalities, environmental spill sizes, and economic losses, the Coast Guard leveraged results from research for the monetization of impacts. For example, to monetize the death and injury determination, MSRAM uses $6.3 million per value of a statistical life, which is based on peer-reviewed research.

Table 4: National Infrastructure Protection Plan Core Criteria for Risk Assessments

Criterion	Description
Complete	The methodology should assess *consequence, vulnerability*, and *threat* for every defined risk scenario and follow the more specific guidance given in NIPP, such as documenting the scenarios assessed, estimating the number of fatalities, describing all protective measures in place, and identifying attack methods that may be employed.
Reproducible	The methodology must produce comparable, repeatable results, even though assessments of different critical infrastructure and key resources may be performed by different analysts or teams of analysts. It must minimize the number and impact of subjective judgments, leaving policy and value judgments to be applied by decision makers.
Documented	The methodology and the assessment must clearly document what information is used and how it is synthesized to generate a risk estimate. Any assumptions, weighting factors, and subjective judgments need to be transparent to the user of the methodology, its audience, and others who are expected to use the results. The types of decisions that the risk assessment is designed to support and the timeframe of the assessment (e.g., current conditions versus future operations) should be given.
Defensible	The risk methodology must logically integrate its components, making appropriate use of the professional disciplines relevant to the analysis, and be free from significant errors or omissions. Uncertainty associated with consequence estimates and confidence in the vulnerability and threat estimates should be communicated.

Source: NIPP.

MSRAM Risk Assessments Generally Align with DHS Criteria, but Challenges Remain

MSRAM generally aligns with DHS's criteria for a complete and reproducible risk assessment, but some challenges remain, such as the limited time for Coast Guard personnel to complete assessments. MSRAM also generally aligns with the NIPP criteria for a documented and defensible risk assessment, but the Coast Guard could improve its documentation of the model's assumptions and other sources of uncertainty, such as the subjective judgments made by Coast Guard analysts about vulnerabilities and consequences, and how these assumptions and other sources of uncertainty affect MSRAM's results. In addition to providing decision makers with an understanding of how to interpret any uncertainty in MSRAM's risk estimates, greater transparency and documentation could facilitate periodic peer reviews of the model—a best practice in risk management.

MSRAM Generally Aligns with NIPP Criteria for a Complete and Reproducible Risk Assessment

MSRAM generally aligns with NIPP criteria for a complete risk assessment. In accordance with NIPP criteria for a complete risk assessment, MSRAM assesses risk using three main variables—consequence, vulnerability, and threat. MSRAM's risk assessment methodology also follows the NIPP criteria for factors that should be assessed in each of the three risk variables. Specifically, for threat, MSRAM generally follows the NIPP criteria by identifying attack methods that may be employed and by considering the adversary's intent and capability to attack a target. MSRAM generally follows the vulnerability assessment criteria by estimating the likelihood of an adversary's success for each attack scenario and describing the protective measures in place, and MSRAM generally follows the consequence assessment criteria by estimating economic loss in dollars, estimating fatalities, and describing psychological impacts, among other things.

MSRAM's risk assessment methodology also generally aligns with the NIPP criteria for a reproducible risk assessment. To be reproducible, the methodology must produce comparable, repeatable results and minimize the number and impact of subjective judgments, among other things. Although Coast Guard officials acknowledge that MSRAM risk data are inherently subjective, the MSRAM model and data collection processes include features designed to produce comparable, repeatable results across sectors. For instance, the Coast Guard prepopulates threat data into MSRAM from the Coast Guard's ICC. This allows for nationally vetted threat scores that do not rely on multiple subjective local judgments. DHS, in its 2010 Transportation Systems Sector-Specific Plan, stated that MSRAM produces comparable, repeatable results.[22]

Coast Guard Efforts That Contribute to MSRAM Being Complete and Reproducible

The Coast Guard has taken numerous actions that contribute to MSRAM being a complete and reproducible risk assessment model. To improve the quality and accuracy of MSRAM data and reduce the amount of subjectivity in the MSRAM process, the Coast Guard conducts an annual review and validation of MSRAM data produced at each sector; provides MSRAM

[22]DHS, *Transportation Systems Sector-Specific Plan, an Annex to the National Infrastructure Protection Plan* (Washington, D.C.: 2010). This is the strategic plan for the sector implementing the requirements of Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, and the requirements of the Intelligence Reform and Terrorism Prevention Act of 2004 (as amended) for the National Strategy for Transportation Security. The plan describes collaboratively developed strategies to reduce risks to critical transportation infrastructure from the broad range of known terrorism threats.

users with tools, calculators, and benchmarks to assist in calculating consequence and vulnerability; and provides training to sectors on how to enter data into MSRAM. Specific actions are detailed below.

Annual validation and review. The Coast Guard uses a multilevel annual validation and review process, which helps to ensure that MSRAM risk data are comparable and repeatable across sectors. According to a 2010 review of MSRAM, conducting a thorough review process across sectors is especially important if the data are to be used for national-level decision making.[23] This process includes sector, district, area, and headquarters officials and aims to normalize MSRAM data by establishing national averages of risk scores for attack modes and targets and by identifying outliers.[24] The annual MSRAM validation and review process begins with sectors completing vulnerability and consequence assessments for targets within their areas of responsibility.[25] Once the sector Captain of the Port validates the assessments, the risk assessment data are sent to district and area officials for review.[26] Following these reviews, Coast Guard headquarters officials combine each sector's data into a national classified dataset and perform a statistical analysis of the data. The statistical analysis involves calculating national averages for vulnerability, consequence, and response capabilities risk scores.[27] When determining whether a sector's risk score for a specific target is questionable or is an outlier, reviewers consider the

[23]Lewis and Mackin, *Maritime Security Risk Analysis Model (MSRAM) Independent Verification and Validation (IV&V) Report*.

[24]The Coast Guard defines an outlier as a score greater than two standard deviations from the national average for a given target class and scenario.

[25]According to the Coast Guard, assessment and validation should not be limited to an annual cycle but should occur throughout the year as risk information changes. Sectors are expected to validate or update risk data annually. This can involve updating existing assessments if new information on a target is available or validating assessments if risk information is unchanged.

[26]The Captain of the Port is the Coast Guard officer designated by the Commandant to enforce, within his or her respective area, port safety, security, and maritime environmental protection regulations, including, without limitation, regulations for the protection and security of vessels, harbors, and waterfront facilities.

[27]Response capabilities are defined as the ability of the Coast Guard, port stakeholders and other governmental agencies to mitigate death/injury, primary economic, and environmental consequences of a successful attack.

results of the statistical analysis as well as supporting comments or rationale provided by sector officials.

According to the Coast Guard, for each outlier identified during the national review process, sector officials reconsider the data point in question and either change the inputs to reflect national averages or provide additional justification for why the risk score for the target in question should be outside of the national average. Headquarters officials explained that they generally accept justification for data outliers and that a goal of the review process is to spur discussions related to maritime risk rather than forcing compliance with national data averages. For example, officials from one sector told us that a small port in their sector is critical for their state's energy imports, and accordingly, the port infrastructure is high risk on a national scale. The officials said that Coast Guard headquarters officials have questioned the relatively high risk rankings of the port's infrastructure because they are statistical outliers, but have deferred to the expertise of the sector regarding the risk scores.

Tools and calculators. Recognizing that sector port security specialists who assess risk using MSRAM generally do not have expertise in all aspects of assessing vulnerability and consequence, the Coast Guard has regularly added new tools and calculators to MSRAM to improve the quality, accuracy, and consistency of vulnerability and consequence assessments. For example, MSRAM now includes a blast calculator that allows users to more easily determine the death and injury consequences of an explosion close to population centers. Coast Guard officials from 29 sectors (82 percent of sectors) cited a variety of challenges with assessing vulnerability and consequence values in MSRAM, but officials from 10 sectors said that it was becoming easier to do over time and officials from 14 sectors said that the tools and calculators in MSRAM have helped.

Benchmarks and recommended ranges. To limit inconsistencies caused by different judgments by individual MSRAM users and to minimize user subjectivity, the Coast Guard built into MSRAM a suggested range of scores for each risk factor—including vulnerability, consequence, and response capabilities—as well as averages, or benchmarks, of scores for each factor. The benchmarks are based on Coast Guard and expert evaluation of target classes and attack modes. The benchmarks and recommended ranges are reviewed and updated each year following the annual data revalidation cycle.

Training. The Coast Guard has also provided annual training for MSRAM users, including beginning, intermediate, and advanced courses intended to standardize the data entry process across the Coast Guard. Officials from 34 sectors (97 percent) reported finding the training moderately to very useful in terms of enhancing their ability to assess, understand, and communicate the risks facing their sectors. In 2011, Coast Guard headquarters also started providing live web-based training sessions on various MSRAM issues, such as resolving national review comments, to help sector staff gain familiarity with MSRAM's features on an as-needed basis. In addition to MSRAM training provided by headquarters, one Coast Guard district official we spoke with had developed and provided localized training to the sector-level port security specialists on assessing the vulnerability of chemical facilities. The district official told us that Coast Guard headquarters was interested in this local model for delivering training and was planning to pilot a similar training program in a different district.

Remaining Challenges and Limitations to Making MSRAM Complete and Reproducible

MSRAM generally aligns with DHS's criteria for a complete and reproducible risk assessment, but challenges remain with the MSRAM methodology and risk assessment process. The Coast Guard has acknowledged these challenges and limitations and has actions underway to address them and make MSRAM more complete and reproducible. Coast Guard officials noted that some of these challenges are not unique to MSRAM and are faced by others in the homeland security risk assessment community. Specific challenges are detailed below.

Data subjectivity. While the Coast Guard has taken actions to minimize the subjectivity of MSRAM data, officials acknowledged that assessing threat, vulnerability, and consequence is inherently subjective. To assess threat, the Coast Guard's ICC quantifies judgments related to the intent and capability of terrorist organizations to attack domestic maritime infrastructure. However, there are limited national historic data for domestic maritime attacks and thus intelligence officials must make a number of subjective judgments and draw inferences from international maritime attacks. Further, GAO has previously reported on the inherently difficult nature of assessing the capability and intent of terrorist groups.[28] Vulnerability and consequence assessments in MSRAM are also inherently subjective. For example, officials from 20 sectors we

[28]GAO-06-91.

interviewed said that even with training, tools, and calculators, assessing consequences can be challenging and that it often involved subjectivity and uncertainty. Officials noted that assessing economic impacts—both primary and secondary—was particularly challenging because it required some level of expertise in economics—such as supply chains and industry recoverability—which port security specialists said is often beyond their skills and training.[29] The input for secondary economic impacts can have a substantial effect on how MSRAM's output ranks a target relative to other potential targets. Undervaluing secondary economic impacts could result in a lower relative risk ranking that underestimates the security risk to a target, or inversely, overvaluing secondary economic impacts could result in overestimating the security risk to a target. Recognizing the challenges with assessing secondary economic impacts, Coast Guard officials said they are working with the DHS Office of Risk Management and Analysis to study ways to more accurately assess secondary economic impacts. Additionally, during the course of our review the Coast Guard implemented a tool called IMPLAN that has the potential to inform judgments of secondary economic impacts by showing what the impact could be for different terrorist scenarios.[30]

Limited time to complete assessments. Officials from 19 sectors (54 percent) told us that the lack of time to complete their annually required vulnerability and consequence assessments is a key challenge and many expressed that they believed their sector's data suffered in quality as a result. Each year, sectors are required to update and validate their risk assessments for targets in their areas of responsibility, which can involve site visits to port facilities and discussions with facility security officers to obtain information on vulnerability and consequences. Officials from a Gulf Coast sector noted that obtaining this information from facilities can be challenging because of the number of facilities in the sector and the time involved in meeting with each facility. Officials from an inland river sector also noted that gathering data from certain facilities—such as information on a chemical plant's security enhancements or the expected loss of life from a terrorist attack—is challenging because facilities may not want to share proprietary information that could be damaging in the

[29]According to the Coast Guard, secondary economic impacts represent the expected follow-on economic effects of a successful attack.

[30]IMPLAN stands for Impact Analysis for Planning. It is a tool that assesses economic relationships between primary and secondary economic impacts.

hands of a competitor. As a result, it often takes additional visits, phone calls, e-mails, and time to obtain this information. Officials from a northeastern sector said that having the people and time to update MSRAM data is their key challenge and completing the update is a heavy lift because the update is required at the same time as several other requirements, such as reviewing investment justifications for the Port Security Grant Program. Coast Guard sector officials and one district official we spoke with reported raising concerns to headquarters about the time it takes to complete MSRAM assessments. Headquarters staff also said they were looking into additional ways to make the assessment process easier for sectors, such as providing job aids and examining the possibility of completing the data update at different times in the year.

Limitations in modeling methodology—adaptive terrorist behavior. There are inherent limitations in the overall methodology the Coast Guard uses to model risk. For instance, MSRAM threat information does not account for adaptive terrorist behavior, which is defined by the National Research Council as an adversary adapting to the perceived defenses around targets and redirecting attacks to achieve its goals.[31] Accounting for adaptive terrorist behavior could be modeled by making threat a function of vulnerability and consequence rather than the MSRAM formula which treats threat, vulnerability, and consequence as independent variables.[32] Not accounting for adaptive terrorist behavior is a critique of MSRAM raised by terrorism risk assessment experts. For example, officials from the DHS Office of Risk Management and Analysis have stressed the need to account for adaptive terrorist behavior in risk models. In addition, DHS's 2011 *Risk Management Fundamentals* guidance states that analysts should be careful when calculating risk by multiplying threats, vulnerabilities, and consequences (as MSRAM does),

[31]National Research Council, *Department of Homeland Security Bioterrorism Risk Assessment: A Call for Change, Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis* (Washington D.C.: 2008).

[32]For more information on adaptive terrorist behavior, see A. Cox, "Some Limitations of "Risk = Threat x Vulnerability x Consequence" for Risk Analysis of Terrorist Attacks," *Risk Analysis*, vol. 28, no. 6 (2008): 1749-1761. This article identifies potential limitations in the Risk = Threat x Vulnerability x Consequence formula for modeling risk that can undermine the ability of the model to guide resource allocations or optimize risk reductions. According to Cox, trying to directly assess probabilities for the actions of intelligent adversaries—instead of modeling how they adaptively pursue their goals—can produce ambiguous or mistaken risk estimates.

especially for terrorism, because of interdependencies between the three variables.[33] Coast Guard officials agreed with the importance of accounting for adaptive terrorist behavior and with the risks of treating threat, vulnerability, and consequence as independent variables. The officials explained that although they did not design MSRAM to account for adaptive terrorist behavior, they are working to develop the Dynamic Risk Management Model, which will potentially address this issue.[34]

Limitations in modeling methodology—network effects. Understanding the intent and capabilities of an intelligent adversary is also critical for understanding network effects. Network effects involve the ripple effect of an incident or simultaneous incidents on key sectors of the economy. Assessing network effects could involve determining whether a terrorist attack on a few key assets would have a disproportionate effect on the performance of the network. A starting point for understanding network effects involves gaining a greater understanding of how a network is vulnerable to a diverse range of threats. Examining how such vulnerabilities create strategic opportunities for intelligent adversaries with malevolent intent is central to this understanding.[35] MSRAM does not assess network effects because, according to Coast Guard officials, these types of assessments are beyond the intended use of MSRAM. The 2009 NIPP, the 2010 DHS Quadrennial Review,[36] and the National Academies[37] have determined that gaining a better understanding of network effects would help to understand multiplying consequences of a terrorist attack or simultaneous attacks on key facilities. Although MSRAM does not assess network effects, officials from four sectors said they had undertaken local

[33]DHS, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine* (Washington, D.C.: April 2011).

[34]According to the Coast Guard, the Dynamic Risk Management Model is intended to enable decision makers to identify plausible future situations and identify robust risk management options with an adaptive adversary component. The Coast Guard is developing the prototype and expects to review and test the model over the next year.

[35]For more information on network effects, see Gerald G. Brown, W. Matthew Carlyle, Javier Salmerón, and Kevin Wood, Operations Research Department, Naval Postgraduate School, *Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses* (Monterey, Calif.: 2005).

[36]DHS, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (Washington, D.C.: February 2010).

[37]National Research Council of the National Academies, *Review of the Department of Homeland Security's Approach to Risk Analysis.*

initiatives to identify and document networked systems of targets that if successfully attacked would have large ripple effects throughout the port or local economy. Coast Guard officials agreed that assessing network effects is a challenge and they are examining ways to meet this challenge.[38] However, the Coast Guard's work in this area is still in its infancy and there is uncertainty regarding the way in which the agency will move forward in measuring network effects.

Additional Documentation Could Align MSRAM with NIPP Criteria for Documented and Defensible Risk Assessments

MSRAM is generally documented and defensible, but the Coast Guard could improve its documentation of the model's assumptions and other sources of uncertainty, such as subjective judgments made by Coast Guard analysts about threats, vulnerabilities, and consequences, and how these assumptions and other sources of uncertainty affect MSRAM's results. The NIPP states that for a risk assessment methodology to be documented, any assumptions and subjective judgments need to be transparent to the individuals who are expected to use the results. For a risk assessment methodology to be defensible, uncertainty associated with consequence estimates and the level of confidence in the vulnerability and threat estimates should also be communicated to users of the results.

There are multiple assumptions and other sources of uncertainty in MSRAM. For example, assumptions used in MSRAM include the particular dollar value for a statistical life or the assumed dollar amount of environmental damage resulting from oil or hazardous material spilled as the result of a terrorist attack. MSRAM also relies on multiple subjective judgments made by Coast Guard analysts, which mean a range of possible values for risk calculated from the model. For example, to assess risk in MSRAM, Coast Guard analysts make judgments regarding such factors as the likelihood of success in interdicting an attack and the number of casualties expected to result from an attack. These subjective judgments are sources of uncertainty with implications that, according to

[38]The MSRAM analysis processes focuses on evaluating terrorist attacks to individual targets, not systemwide attacks or simultaneous attacks on multiple maritime targets, which could lead to higher consequences.

the NIPP and risk management best practices, should be documented and communicated to decision makers.[39]

MSRAM's primary sources of documentation provide information on how data are used to generate a risk estimate and information on some assumptions, and the Coast Guard has made efforts to document and reduce the number of assumptions made by the field-level user in order to increase the consistency of MSRAM's data. For example, the MSRAM training and software manual states that MSRAM users are expected to specify the assumptions they make in evaluating various attack modes and provides assumptions for users to consider when scoring attack scenarios, such as specifying the type and amount of biological agent used in a biological attack scenario and assuming that attackers are armed and suicidal in a boat bomb attack scenario.

While these documentation efforts are positive steps to reduce MSRAM data subjectivity and increase data consistency, we found that the Coast Guard has not documented all the sources of uncertainty associated with threat, vulnerability, and consequence assessments and what implications this uncertainty has for interpreting the results, such as an identification of the highest-risk targets in a port. As a result, decision makers do not know how robust the risk rankings of targets are and the degree to which a list of high-risk targets could change given the uncertainty in the risk model's inputs and parameters. Moreover, overlapping ranges of possible risk values caused by uncertainty could have implications for strategic decisions or resource allocation, such as allocating grant funding or targeting patrols. Overlapping ranges of risk values due to uncertainty also underscores the importance of professional judgment in decision making because risk models do not produce precise outcomes that should be followed without a degree of judgment and expertise.

[39]The National Research Council of the National Academies states that because of the uncertainties inherent in terrorism risk analysis, it is crucial that DHS provide decision makers with complete information about how these uncertainties could affect decision making. See National Research Council of the National Academies*, Review of the Department of Homeland Security's Approach to Risk Analysis*. Also, DHS's *Risk Management Fundamentals* notes the importance of being transparent about methodology, limitations, and uncertainty so that decision makers have the most accurate, defensible, and practical information on which to base risk management decisions.

According to the NIPP, the best way to communicate uncertainty will depend on the factors that make the outcome uncertain, as well as the amount and type of information that is available. The NIPP states that in any given terrorist attack scenario there is often a range of outcomes that could occur, such as a range of dollar amounts for environmental damage or a range of values for a statistical life. For some incidents, the range of outcomes is small and a single estimate may provide sufficient data to inform decisions. However, if the range of outcomes is large, the scenario may require additional specificity about conditions to obtain appropriate estimates of the outcomes. Often, this means providing a range of possible outcomes rather than a single point estimate. Coast Guard officials agreed with the importance of documenting and communicating the sources and implications of uncertainty for MSRAM's risk estimates, and noted that they planned to develop this documentation as part of an internal MSRAM verification, validation, and accreditation (VV&A) process that they expect to complete in the fall of 2011.[40] According to the Coast Guard, accreditation is an official determination that a model or simulation is acceptable to use for a specific purpose. While this accreditation process is expected to document the scope and limitations of MSRAM's capabilities and determine whether these capabilities are appropriate for MSRAM's current use, the Coast Guard's draft accreditation plan does not discuss how the Coast Guard plans to assess and document uncertainty in its model or communicate those results to decision makers.

In addition to providing decision makers with an understanding of how to interpret uncertainty in MSRAM's risk estimates, greater transparency and documentation of uncertainty and assumptions could also facilitate periodic peer reviews of the model—a best practice in risk management. According to the National Research Council of the National Academies, periodic reviews and evaluations of risk model outputs are important for transparency with respect to decision makers.[41] Further, these reviews should involve specialists in modeling and in the problems that are being

[40]The Coast Guard conducted its verification and validation of MSRAM in 2009. The accreditation process began in February 2011. According to Coast Guard policy, MSRAM should have been internally accredited prior to implementation in 2005; however, officials explained that they did not conduct the accreditation of MSRAM prior to its initial deployment because of ongoing changes to the model. The officials added that MSRAM is now at an appropriate place in its development and evolution to be formally accredited.

[41]National Research Council of the National Academies, *Review of the Department of Homeland Security's Approach to Risk Analysis*.

addressed and should address the structure of the model, the types and certainty of the data, and how the model is intended to be used. Peer reviews can also identify areas for improvement and can facilitate sharing best practices. As we have previously reported, external peer reviews cannot ensure the success of a model, but they can increase the probability of success by improving the technical quality of projects and the credibility of the decision-making process.[42] MSRAM has been reviewed twice—in 2010 by risk experts affiliated with the Naval Postgraduate School and, to a lesser extent, in 2009 by CREATE at the University of Southern California. The authors of the Naval Postgraduate School report stated that their review was intended to validate and verify the equations used in MSRAM, evaluate MSRAM's quality control procedures, and review the use of MSRAM outputs to manage risk.[43] The authors of the CREATE report stated that their review focused on suggestions for improvement rather than a comprehensive evaluation, and they suggested that the Coast Guard continue to seek feedback and reviews from the risk and decision analysis community, as well as from practitioners of other disciplines.[44] Coast Guard officials told us that they have generally benefited from reviews of MSRAM and have worked to implement many of the resulting recommendations. Officials noted they intend to pursue external reviews of MSRAM as part of the ongoing VV&A process, but they have not identified who would be conducting the reviews, or when the reviews would occur. As the Coast Guard's risk assessment model continues to evolve, the Coast Guard could benefit from periodic external peer review to ensure that the structure and outputs of the model are appropriate for its given uses and to identify possible areas for improvement.

[42]GAO, *Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection*, GAO-04-557T (Washington D.C., Mar. 31, 2004).

[43]Lewis and Mackin, *Maritime Security Risk Analysis Model (MSRAM) Independent Verification and Validation (IV&V) Report*.

[44]Barret et al., *Evaluation of U.S. Coast Guard Terrorism Risk and Decision Analysis Models and Processes for Port, Waterways and Coastal Security*.

Coast Guard Has Used a Risk-Informed Approach to Manage Maritime Security Risk, but Challenges Hinder Sector Efforts

MSRAM Informs Several National-Level Risk Management Efforts

MSRAM is a security risk analysis and risk management tool and the Coast Guard intends for it to be used to inform risk management decisions at all levels of command.[45] As such, in a May 2011 guidance document, the Coast Guard set expectations for how MSRAM should be used at the national and sector levels. At the national level, the Coast Guard expects its offices to use MSRAM to support strategic plans, policy, and guidance; to integrate MSRAM into maritime security programs; and to ensure that sectors have adequate personnel ready to perform MSRAM duties, among other goals.

At the national level, MSRAM assists in the development and implementation of several operational and strategic planning efforts, which align with the Coast Guard's expectations for how risk information should be used.[46] One key use of MSRAM data at the national level has been to refine the national MCIKR list, which the Coast Guard reports has allowed it to focus resources on the highest-risk maritime targets. Coast Guard headquarters requires sectors to meet certain operational activity standards, such as MCIKR visits, patrol frequencies, and vessel escort requirements set under the Maritime Security and Response Operations

[45]According to the Coast Guard, MSRAM information is not used exclusively in most cases, but is used in conjunction with other pertinent facts and factors to inform decision making. For example, MSRAM information, when combined with resource costs, national and Coast Guard strategic priorities, and Coast Guard legal mandates, is intended to be used to support risk-informed resource allocation decisions at the sector, district, area, and headquarters levels and risk-informed policy formulation at the national and area levels.

[46]Operational activities include conducting boat escorts, implementing positive control measures—that is, stationing armed Coast Guard personnel in key locations aboard a vessel to ensure that the operator maintains control—and providing a security presence through various actions.

(MSRO) program.[47] By identifying the nation's highest-risk maritime targets, MSRAM helps establish the national MCIKR list, which sectors use to complete their annually required number of MCIKR visits. According to Coast Guard officials, MSRAM has aided in reducing the MCIKR list from 740 assets to 324 assets and allowed the Coast Guard to further prioritize within that more focused list of 324, since MSRAM analysis demonstrated that a small number of assets make up the majority of the nation's risk.[48]

MSRAM has also been used as a tool to inform resource allocation and performance measurement, which is consistent with the Coast Guard's goals for MSRAM.[49] For instance, risk-informed methods and processes or models, such as MSRAM, are used in the Coast Guard's annual Standard Operational Planning Process, which establishes a standardized process to apportion major assets, such as boats, aircraft, and deployable specialized forces. Coast Guard officials said that MSRAM data supports the PWCS mission in this process by demonstrating how risk is distributed geographically. In addition, Coast Guard used MSRAM to support a funding request for boats, personnel, and associated support costs to assist with Coast Guard efforts to reduce the risk of certain dangerous cargoes by escorting ships passing through coastal ports carrying cargoes such as liquefied natural gas. MSRAM also supports resource allocation through the Port Security Grant Program by informing the risk formula used by DHS to allocate grant funding.[50] MSRAM data are also used in the

[47]MSRO, formerly referred to as Operation Neptune Shield, are those operations conducted by the Coast Guard and its maritime partners to deny the use and exploitation of the maritime domain to criminal or hostile actors. Activities include vessel escorts, support to military outloads, periodic visits to maritime critical infrastructure and key resources, and security boardings, among other things. The required frequencies are considered classified.

[48]The most recent MCIKR update occurred in spring 2011 and was informed by the past several years of MSRAM data, according to Coast Guard officials.

[49]The Coast Guard's overarching goals for MSRAM include informing risk management decisions to preserve the marine transportation system; informing national, regional, and local security policy; and institutionalizing MSRAM throughout the Coast Guard as the security risk assessment and analysis program to support senior leadership decision-making, budget formulation, resource allocation, and performance measurement; among other goals.

[50]For more information on the Port Security Grant Program, see GAO, *Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened*, GAO-12-47 (Washington, D.C.: Nov. 17, 2011).

Coast Guard's model for measuring its performance in the PWCS mission, which is discussed in depth later in this report.

MSRAM has also supported strategic documents and efforts throughout DHS. Specifically, the Coast Guard reported that MSRAM data are an essential building block for a number of key strategic documents, such as the National Maritime Strategic Risk Assessment, the National Maritime Terrorism Threat Assessment, and the Combating Marine Terrorism Strategic and Performance Plan, among others.[51] In addition, the Coast Guard uses MSRAM, among other inputs, to provide DHS with maritime risk information for the Transportation Sector Security Risk Assessment tool.[52] DHS also reported that the Coast Guard has shared MSRAM-based identification of critical assets beyond the transportation system with 13 of the 18 DHS critical infrastructure and key resource sectors.[53]

[51]The National Maritime Strategic Risk Assessment generates a 5-year strategic maritime risk profile to serve as the basis for informing (1) the Coast Guard's budget and planning process, (2) the enterprise strategic planning direction, and (3) DHS's integrated planning process. The most recent plan came out in 2006. The National Maritime Terrorism Threat Assessment is prepared in coordination with the DHS Homeland Infrastructure Threat and Risk Analysis Center and addresses terrorist threats to the U.S. maritime domain and serves as a comprehensive analysis of maritime terrorist threats for Coast Guard to pass along critical information to local security partners. The most recent assessment was conducted in July 2010. According to Coast Guard officials, a new National Maritime Terrorism Threat Assessment is anticipated to be released in the fall of 2011. The Combating Marine Terrorism Strategic and Performance Plan, released in July 2008, is the second iteration of the Coast Guard's strategy for the PWCS mission. It identifies essential roles and responsibilities for Coast Guard mission managers and senior operational commanders and informs DHS and partner agencies on how the Coast Guard will be addressing the security issues for which it is responsible. The next plan will be issued in 2015.

[52]According to the 2010 DHS Transportation Systems Sector-Specific Plan, the Transportation Sector Security Risk Assessment tool is used to conduct modal security risk assessments for each of the primary transportation modes, as well as sub-modal groups, such as the school bus transportation system.

[53]There are 18 critical infrastructure and key resource sectors addressed by the NIPP. They are (1) agriculture and food; (2) banking and finance; (3) chemical; (4) commercial facilities; (5) communications; (6) critical manufacturing; (7) dams; (8) defense industrial base; (9) emergency services; (10) energy; (11) government facilities; (12) healthcare and public health; (13) information technology; (14) national monuments and icons; (15) nuclear reactors, materials, and waste; (16) postal and shipping; (17) transportation systems; and (18) water. Each of these sectors has data in MSRAM except banking and finance, public health, emergency services, information technology, and postal and shipping.

For example, MSRAM has been used to assess the risk of some chemical facilities and power plants.

MSRAM Has Informed Some Local-Level Risk Management Efforts, but Its Use Has Been Limited by Several Factors

MSRAM has been used to inform a variety of efforts at the sector level, such as strategic planning, communication with port stakeholders, and operational and tactical decision making, but its use for operational and tactical risk management efforts has been limited by a lack of staff time, the complexity of the MSRAM tool, and competing mission demands, among other factors. The Coast Guard expects its 35 sectors, with support from its nine districts, to integrate MSRAM data into strategic, operational, and tactical plans, operations, and programs as necessary and required, among other actions.[54]

Based on results from our interviews with officials from all 35 Coast Guard sectors, officials from 26 sectors (74 percent) reported finding MSRAM moderately to very useful for informing strategic planning, which includes developing portions of local Area Maritime Security Plans and planning security exercises.[55] For example, officials from a Gulf Coast sector reported using MSRAM to find the highest-risk areas in which to conduct exercises. Further, lessons learned from the exercises are incorporated into strategic plans, which officials said leads to planning process improvements and overall better plans. However, officials from a southeastern sector pointed out that MSRAM is a snapshot view of port risk and therefore long-term strategic plans require additional information from many sources.

For communicating risk information to port security stakeholders, such as local law enforcement or facility owners, officials from 26 sectors (74

[54]In a May 2011 guidance document, the Coast Guard states that sector commanders should integrate MSRAM analysis into their operations to support risk communication, special security events, determining a daily security risk profile for a given area, port security exercises, risk management planning, Area Maritime Security Plans, and the Port Security Grant Program field review process, among other areas.

[55]Area Maritime Security Plans have been established pursuant to the Maritime Transportation Security Act of 2002. Content requirements for the plans were established by 33 C.F.R. § 103.505 and expanded by the Security and Accountability For Every Port (SAFE Port) Act of 2006 to include a Salvage Response Plan. The plans are intended to sponsor and support engagement with port community stakeholders to develop, test, and when necessary, implement joint efforts for responding to and mitigating the effects of a maritime transportation security incident.

percent) said that MSRAM was moderately to very useful. For instance, officials from a southeastern sector said that MSRAM is used to communicate and justify additional security procedures. Further, during annual compliance inspections, MSRAM data are discussed with facility security officers and compared to security data that the facility security officers have calculated. In addition, officials from a Gulf Coast sector reported that MSRAM provides a convenient, objective way to communicate risk to port security stakeholders, and stakeholders appreciate that risk information from MSRAM is computer driven and based on a rigorous process.

For informing sector operational and tactical decision making, such as planning MSRO activities, developing local critical infrastructure lists, and planning for special events, officials from 18 sectors (51 percent) reported that MSRAM moderately or greatly provided them with the information needed to make risk-informed decisions regarding port security. Regarding planning MSRO activities, one eastern sector reported that MSRAM was very helpful for identifying priority targets for MSRO patrols and escorts. Regarding developing local critical infrastructure lists, officials from an eastern sector said that since the sector has no assets on the national MCIKR list, they were able to use MSRAM to generate a local list to help determine patrols and other security efforts. Regarding special event planning, officials from 16 sectors (45 percent) told us they used MSRAM to determine where to allocate resources for special events, such as the Fourth of July, dignitary visits, or political conventions. For example, officials from an inland river sector said that they used MSRAM to identify possible attack scenarios and to help identify what security resources they should request to provide security for a special event. See figure 1 for photographs of various Coast Guard security-related activities that can be informed by MSRAM. In addition to using MSRAM to inform maritime security decisions, officials from almost every sector noted that they also assess and manage risk using other tools or methods, such as the High Interest Vessel matrix, outreach to

port partners, working relationships with Area Maritime Security Committees, or professional judgment.[56]

[56]The High Interest Vessel matrix is a risk-based tool used by Coast Guard sectors to evaluate the security risk of a vessel entering into port. According to DHS, sector staff use multiple databases and intelligence data to complete the matrix, focusing on security factors such as the vessel's size, cargo, operations, and security performance. Each of these security factors constitutes a component of the vessel's High Interest Vessel matrix score. When a vessel's score meets or exceeds a specific number, the Sector Commander designates the vessel as a high interest vessel and takes action to mitigate the risk it poses.

Figure 1: MSRAM Can Be Used to Inform a Variety of Coast Guard Activities and Operations, Including Escorting Ferries, Naval Vessels, or Cruise Ships and Performing Waterborne or Aerial Patrols of Critical Infrastructure or National Symbols

Source: U.S. Coast Guard.

Although officials from most sectors found that MSRAM provided useful risk information for sector-level decision making, officials from 32 sectors (91 percent) reported that their overall use of MSRAM data in managing risk was hindered by a lack of staff time for data analysis, the complexity of the MSRAM tool, or competing mission demands, among other things. These challenges are discussed below.

Limited staff time for analyzing and using MSRAM. Officials from 21 sectors (60 percent) told us that limited staff time posed a challenge to incorporating MSRAM into strategic, operational, and tactical planning efforts. For example, officials from a northeastern sector said that a lack of available staff time was one of the most significant limitations to utilizing MSRAM. These officials stated that they would like to have dedicated MSRAM personnel to develop the tool and make it useful on a daily basis. They added that even though MSRAM had many capabilities, they were unable to use it to its full capability because their port security specialist—the primary user of MSRAM—was busy with other programs, such as the Port Security Grant Program. Each of the port security specialists from the three districts we interviewed—which encompass 15 sectors over the West Coast, East Coast, Gulf Coast, and Mississippi River area—echoed the challenges with the level of sector resources for MSRAM.[57] For example, one district official stated that although Coast Guard headquarters has dedicated MSRAM staff, there are no full-time MSRAM analysts at the sector level. He added that each sector would need a dedicated person for MSRAM and risk analysis to bring MSRAM analysis into operational and tactical decision making.

Complexity of the MSRAM tool. Officials from 14 sectors (40 percent) reported that MSRAM use has been limited because data outputs require a substantial degree of analysis to use in decision making, or because the MSRAM tool itself is not easy to use. Some of the challenges raised by sectors that contribute to the complexity of the tool and interpreting its outputs included keeping abreast of yearly changes to the MSRAM tool and bridging knowledge gaps that occur when staff familiar with MSRAM rotate or leave the sector. In its MSRAM core document, the Coast Guard recognized that the frequent rotation of active duty personnel presents a

[57]The Coast Guard expects personnel in each of its nine districts to maintain competency in MSRAM to assist sector personnel, and to support sectors in validating MSRAM data, among other things.

risk to both the consistency of the MSRAM risk scoring efforts and the application of risk results.

Competing mission demands and resource constraints. Officials from 14 sectors (40 percent) reported that competing mission demands or resource constraints limited the use of MSRAM. Specifically, officials from 11 sectors reported that MSRAM's usefulness was limited by the fact that it only considers risk in the PWCS mission, which is 1 of the Coast Guard's 11 statutorily required missions. For example, a Great Lakes sector told us that while MSRAM identifies the risks in the sector, the sector is limited in its ability to move assets to address those security risks because the assets are also fulfilling other Coast Guard mission requirements, such as search and rescue. Additionally, officials from 6 sectors said that limited resources, such as boats or personnel, constrained their sectors' ability to address the risks identified by MSRAM. For example, officials from 2 inland river sectors said that MSRAM identifies their security risks and demonstrates where they should patrol and plan for special events, but that they do not have the resources to carry out the plans. Further, officials from 1 of the inland river sectors added that their response boats are often busy escorting the Army Corps of Engineers or engaged in flood relief efforts. This leaves the work of security patrols to the local harbor patrol, which the officials said does not have the same capabilities, in terms of boats and weapons, as the Coast Guard.

Other challenges. Sector officials also identified other challenges with using MSRAM for informing decision making. Specifically, officials from 16 sectors (45 percent) said that MSRAM would be more useful if it was linked to other Coast Guard data systems, such as the Coast Guard's inspections database, or if MSRAM was integrated into the sector command center. For example, officials from an east coast sector told us that they would like to see MSRAM linked to other databases in the sector command center, such as the Coast Guard's vessel tracking system. Similarly, officials from a west coast sector said that integrating MSRAM into the Coast Guard's inspections database would keep MSRAM continually updated and reflective of inspection results. Further, the command center has to consider other mission response needs, such as for pollution incidents or search and rescue, among others, and if MSRAM was integrated into the sector command center it could be used more in day-to-day operations. In addition, officials from 5 sectors noted

that MSRAM does not capture dynamic risk, which limits its ability to inform daily decisions at the sector level.[58] For instance, officials from a Gulf Coast sector said that they did not use MSRAM on a daily basis to allocate resources because daily fluctuations in vessel and barge risk are their greatest concern and this risk is not currently captured in MSRAM. The sectors that raised these issues believed that linking MSRAM into other data systems, integrating MSRAM into the command center, and having MSRAM account for dynamic risks could contribute to making its data more accurate, robust, and useful for decision making.

Coast Guard Has Taken Steps to Address Challenges, but Could Increase MSRAM's Use by Expanding Training Opportunities

Coast Guard headquarters officials told us that they were aware of the challenges field-level MSRAM users were facing and have taken some steps to address them, but providing additional training could help integrate MSRAM throughout sector decision making. The Coast Guard's current actions to address MSRAM user challenges include assessing the feasibility of adding additional risk analyst staff, increasing the data's usability, developing decision-supporting modules, and providing training. These actions are described below.

Examining the feasibility of dedicated risk analysts. Presently, there is no dedicated risk analyst or MSRAM analyst position at the sector level, but headquarters officials told us in June 2011 that they are examining the feasibility of assigning additional port security specialists to the field and submitted a resource proposal for the additional staff. According to a senior Coast Guard budget official, given competing priorities and a constrained resource environment, it is unclear when or if this resource proposal will be funded.

Deploying MSRAM to sector command centers. To help make MSRAM more dynamic and increase its usability, the Coast Guard is piloting an Enterprise Geographic Information System (EGIS) display for sector command centers, which layers facility and vessel locations onto a satellite-based map and visually displays changing risk as vessels move into and out of ports. Officials from 7 sectors that participated in or were familiar with the initial EGIS test group reported that the functionality was

[58]Coast Guard officials told us that MSRAM provides a static picture of risk at a given point in time, but maritime risk can be dynamic. For example, as a barge carrying dangerous cargo moves through a port area, the risk to assets in that port area changes based on the location of the barge.

very useful and had the potential to substantially increase MSRAM's use for sector risk management efforts. In addition, headquarters officials told us in June 2011 that efforts were under way to integrate MSRAM into the Coast Guard's inspections database, which would allow MSRAM to be continually updated and reflective of year-round facility and vessel inspection results.

Developing risk management modules. To assist with incorporating risk assessment information into decision making, in the fall of 2008, the Coast Guard began developing risk management modules within MSRAM that are able to provide specific types of analyses, such as comparing alternative security strategies. We asked officials from all 35 sectors their views on four modules—the Alternatives Evaluation Module, the Simplified Reporting Interface, the Daily Risk Profile, and the Risk Management Module.[59] Sectors had mixed views on the utility of these modules. Specifically, officials from 14 sectors (40 percent) found the Alternatives Evaluation module very useful and cited such uses as evaluating Port Security Grant Program proposals and planning security for special events,[60] and officials from 15 sectors (42 percent) found the Simplified Reporting Interface very useful for communicating risk information to port partners.[61] However, with respect to the other two modules—the Daily Risk Profile and Risk Management Module—officials from 2 sectors (5 percent) found the Daily Risk Module very useful and officials from 3 sectors (8 percent) found the Risk Management Module very useful. For both modules, officials from 18 sectors (51 percent) reported that either they had not seen them or they were aware of the

[59]According to the Coast Guard, the Alternatives Evaluation Module enables users to characterize the differences in their risk profile for a number of alternative environments, such as seasonal changes, technology changes, or changes in threat, consequence, or vulnerability. The Simplified Reporting Interface is designed to provide a simple interface for generating risk information tailored to support decision-making processes inside and outside the Coast Guard, and was designed to be used by sector staff who may only have a basic understanding of MSRAM's capabilities. The Daily Risk Profile allows users to identify which targets in their dataset are within their area of responsibility each day. The Risk Management Module provides the capability to develop and communicate risk mitigation strategies that the Coast Guard and its partners provide for every maritime scenario within the user's area of responsibility.

[60]Officials from 11 sectors did not know or could not provide an answer on the usefulness of the Alternatives Evaluation Module.

[61]Officials from 5 sectors did not know or could not provide an answer on the usefulness of the Simplified Reporting Interface.

modules but did not have the time or training, among other reasons, to use them. Many of the modules are new and headquarters and some sector officials reported that they expected the modules would be more useful in the future as sectors gained familiarity with them through additional exposure and the annual MSRAM training.

Providing training. While the Coast Guard offers annual MSRAM training, officials from 25 sectors (71 percent) identified areas of the training for improvement, which the Coast Guard could do more to address.[62] Specifically, officials from these sectors said that increasing the number of people who take MSRAM training, providing MSRAM training to command-level staff or senior management, and offering training on how to conduct risk analysis to inform decision making, among other things, would help integrate MSRAM throughout sector decision-making processes. Since MSRAM is a collateral duty, MSRAM training is not part of any Coast Guard personnel's required training curriculum.[63] However, Coast Guard guidance from May 2011 states that area, district, and sector commanders are responsible for ensuring that adequate numbers of appropriate personnel are trained in MSRAM. Only one sector did not, at the time of our interview, have at least one staff person trained in MSRAM.[64] Officials from a Gulf Coast sector said that the training provided on the MSRAM tool itself is good, but the training does not teach the skills needed to make decisions in the field. Officials from a Great Lakes sector suggested that the Coast Guard develop an advanced course on how to use MSRAM to inform operational decisions. Officials from a southeastern sector added that the Coast Guard provides guidance on how to assess risks using MSRAM, but needs to provide more training on how to communicate MSRAM results and how those

[62]The training focuses on understanding the basics of MSRAM, establishing or improving risk analysis and risk management skills, establishing or improving risk communication skills, and promoting risk management best practices, among other goals.

[63]Additionally, efforts are under way to formalize MSRAM training, which begins with a training needs analysis. Officials added that the analysis will focus on how best to support MSRAM users in the field and will identify what a MSRAM user has to know or be able to do to use MSRAM. The analysis will also identify job skills needed for MSRAM users and will identify forms of support, such as job aids and training.

[64]In the case of the 1 sector without a MSRAM specialist, their port security specialist had unexpectedly left the sector and the district-level port security specialist was managing the sector's MSRAM duties until a port security specialist could be hired. The sector officials reported that they expected to hire and train a new port security specialist before the end of calendar year 2011.

results can be used. In addition, a sector commanding officer who participated in one of our interviews told us that he was provided minimal training on MSRAM and wanted to understand more about how it can be used to support command-level decisions.

MSRAM has the capability of informing operational, tactical, and resource allocation decisions at all levels of a sector, but the Coast Guard has generally provided MSRAM training to a limited number of sector staff with specific MSRAM risk assessment responsibilities, such as port security specialists, rather than sector staff who may have command or management responsibilities where MSRAM may apply. Coast Guard headquarters officials said that this was because of limited resources to provide training for numerous sector personnel and variations in how MSRAM responsibilities are managed at different sectors. *Standards for Internal Control in the Federal Government* states that effective management of an organization's workforce is essential to achieving results. Further, only when the right personnel for the job are on board and are provided the right training and tools, among other things, is operational success possible. To this end, management should ensure that training is aimed at developing and retaining employee skill levels to meet changing organizational needs.[65] Coast Guard headquarters officials agree that providing MSRAM training to additional sector staff, particularly those with command and management responsibilities, would be valuable. Such training on how MSRAM can be used at all levels of command for risk-informed decision making—including how MSRAM can assist with the selection of different types of security measures to address areas of risk and the evaluation of their impacts—could further the Coast Guard's efforts to implement its risk management framework and meet its goal to institutionalize MSRAM as the risk management tool for maritime security.

[65]GAO, *Standards for Internal Control in the Federal Government,* GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

Coast Guard Measures Risk Reduction but Has Faced Challenges Using This Measure to Inform Decisions

Coast Guard Developed a Measure to Report Performance in Reducing Risk

The Coast Guard developed a performance measure and supporting model to measure and report its overall performance in reducing maritime security risk. This measure identifies the percentage reduction of maritime security risk, subject to Coast Guard influence, resulting from various Coast Guard actions.[66] The Coast Guard considers this performance measure its key outcome measure for its PWCS mission.[67] According to DHS's *Risk Management Fundamentals* and the NIPP, it is crucial that a process of performance measurement be established to evaluate whether actions taken ultimately achieve the intended performance objective, such as reducing risk. This is important not only in evaluating program performance but also in holding the organization accountable for progress. We have also previously reported on the importance of developing outcome-based performance goals and measures as part of results management efforts.[68] From fiscal years 2006 to 2010, the Coast Guard annually reported reducing from 15 to 31 percent of the maritime

[66]The Coast Guard does not include risk reduction efforts taken by private industry in the percentage of risk Coast Guard reduces. The portion of maritime risk subject to Coast Guard influence was estimated by Coast Guard officials in 2005.

[67]Outcome measures describe the intended result of carrying out a program or activity. The Coast Guard has three additional risk reduction performance measures for its PWCS mission, which are considered subsets of the overall risk reduction measure: percentage reduction of maritime security risk resulting from Coast Guard consequence management, percentage reduction of maritime security risk resulting from Coast Guard efforts to prevent a terrorist entering the United States via maritime means, and the percentage reduction of maritime security risk resulting from Coast Guard efforts to prevent a weapon of mass destruction from entering the United States via maritime means. In addition, the Coast Guard has additional output and activity metrics to support performance evaluation in this mission area.

[68]GAO, *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*, GAO-07-454 (Washington, D.C.: Aug. 17, 2007).

risk it is responsible for, in each year either meeting or exceeding its target. For fiscal years 2011 and 2012, the Coast Guard's planned performance targets are to reduce more than 44 percent of the maritime security risk for which it is responsible.[69]

To measure how its actions have reduced risk, the Coast Guard developed a model that uses a two-step approach. The first step is to estimate the total amount of terrorism risk that exists in the maritime domain, in the absence of any Coast Guard activities. This is referred to as raw risk, and this information comes primarily from MSRAM.[70] The second step relies on an elicitation process whereby Coast Guard subject matter experts estimate how various security activities and operations, maritime domain awareness programs, and regulatory structures—referred to by the Coast Guard as regimes—that the Coast Guard has implemented have reduced risk to U.S. ports and waterways. This step involves Coast Guard subject matter experts assessing the probability of these Coast Guard efforts failing to prevent a successful terrorist attack for 16 potential maritime terrorist attack scenarios.[71]

Eliciting the opinions of subject matter experts is a method that can be used to estimate terrorism risk, particularly when the historical record is either nonexistent or is not appropriate for collecting data on a specific scenario, according to DHS's *Risk Management Fundamentals*.[72] The Coast Guard relies on subject matter experts to estimate performance in mitigating risk because, unlike risk analyses for other Coast Guard

[69]Targets for fiscal years 2011 and 2012 have increased because of a revised methodology for estimating risk reduction that will take effect in fiscal year 2011. This revised methodology is discussed later in this section.

[70]Information also comes from DHS's Risk Analysis Process for Informed Decision Making (RAPID) project, which is designed to provide strategic planning guidance and support resource allocation decisions at the DHS level.

[71]According to Coast Guard officials, the subject matter experts are drawn from the three pillars of the PWCS mission: maritime domain awareness, regime, and MSRO. Although a reviewer of the model recommended using outside independent experts to help estimate risk reduction, Coast Guard uses only internal subject matter experts. Coast Guard officials explained that using external experts would be challenging because of the time needed to inform them about Coast Guard operations and activities.

[72]According to DHS's Risk *Management Fundamentals*, elicitations involve using structured questions to gather information from individuals with in-depth knowledge of specific areas or fields.

missions, such as search and rescue, there is not a rich historical data set of maritime terrorism incidents that the Coast Guard can use to measure its actual performance. In other words, in the absence of an actual domestic maritime terrorism event, the Coast Guard uses internal subject matter experts to estimate risk reduction as a proxy measure of performance—an attempt to measure performance against a terrorism incident that did not occur.[73]

Coast Guard Faces Challenges Using the Risk Reduction Performance Measure to Inform Decision Making

The Coast Guard's efforts to develop an outcome measure to quantify the impact its actions have had on risk is a positive step. However, the use of the measure has been limited, and even with recent improvements, the Coast Guard faces challenges using this measure to inform decision making. Performance goals and measures are intended to provide Congress and agency management with information to systematically assess a program's strengths, weaknesses, and performance. Thus, measures should provide information for management decision making. Coast Guard officials explained that the primary purpose of the risk reduction measure has been for external performance reporting, and to a more limited extent for informing strategic decision making and for conducting internal analysis of performance to identify areas for improvement. Specifically, officials said the measure has been used to compare risk across maritime terrorism scenarios and compare those results to other studies and analysis on maritime terrorism scenarios, which provided information on whether PWCS activities were appropriately balanced to address those risks. However, Coast Guard officials stated that over time, internal and external reviews identified

[73]The risk reduction model makes use of estimates of how often terrorists would be expected to attack maritime targets together with information from MSRAM on threats, vulnerabilities, and consequences. In addition, the Coast Guard has many activities that can reduce risk that are not focused on individual targets and are therefore not estimated in MSRAM, such as maritime regulations enforcement and vessel security boardings. These activities are factored into the risk reduction measure. The risk reduction measure also includes two attack scenarios—weapons of mass destruction and terrorist transfer scenarios—that are not included in MSRAM.

limitations in the risk reduction measure, such as not allowing for comparisons of performance across sectors.[74]

Recognizing these limitations, in 2010, the Coast Guard made improvements to the risk reduction model intended to enhance its utility for management decision making and to provide a more accurate measure of risk reduction. For example, the updated model includes information on the locations of Coast Guard assets and potential targets, which can be used to calculate the probability that Coast Guard assets will be able to intercept attacks. The Coast Guard also improved the elicitation techniques by which subject matter experts provided their estimates of Coast Guard risk reduction performance, and expanded the size and diversity of the subject matter experts involved in the elicitation process.[75] According to Coast Guard officials, these improvements have made the measure and supporting model more useful for informing strategic decisions by allowing, for example, the ability to calculate risk reduction at the sector, district, area, and national levels and the risk reduction value of each element of the Coast Guard's strategy. In other words, the updated model is able to show the risk reduction value of Coast Guard operational assets, such as small boats or helicopters, compared with regime activities, such as regulation enforcement. This information can help inform resource allocation decisions because it could identify which actions provide the greatest risk-reduction, according to these officials. The Coast Guard plans to use the updated model to measure its performance in reducing risk for the 2011 fiscal year.

Since the Coast Guard has not yet used the new measure or supporting model for management analysis and decision making, it is too soon to determine how useful the information will ultimately be for Coast Guard decision makers or external stakeholders; nevertheless, the Coast Guard may continue to face challenges using this measure to inform decision

[74]For example, see Barret et al., *Evaluation of U.S. Coast Guard Terrorism Risk and Decision Analysis Models and Processes for Port, Waterways and Coastal Security*. In addition, see M.E. Cutts, *Improving the Coast Guard Ports, Waterways, and Coastal Security Outcome Measure* (Monterey, Calif.: Naval Postgraduate School, June 2009). These reviews recommended a number of improvements, many of which the Coast Guard incorporated into the model.

[75]According to the Coast Guard, in 2009 a total of 26 subject matter experts were used, mostly from headquarters. In 2010, a total of 46 subject matter experts were used coming from headquarters, areas, districts, sectors, and operational units.

making. For example, given the inherent uncertainties in estimating risk reduction, it is unclear if a measure of risk reduction would provide meaningful performance information for tracking progress against goals and performance over time. According to our performance measurement criteria, to be able to assess progress toward the achievement of performance goals, the measures used must be reliable and valid.[76] Reliability refers to the precision with which performance is measured, while validity is the extent to which the measure adequately represents actual performance. Therefore, the usefulness of agency performance information depends to a large degree on the reliability of performance data. We have also reported that decision makers must have assurance that the program data being used to measure performance are sufficiently reliable and valid if the data are to inform decision making.[77] Although the Coast Guard has taken steps to improve the quality of the supporting model to provide a more accurate measure, estimating risk reduction is inherently uncertain and this measure is based on largely subjective judgments of Coast Guard personnel, and therefore the risk reduction results reported by the Coast Guard are not based on measurable or observable activities.[78] As a result, it is difficult to independently verify or assess the validity or appropriateness of the judgments or to determine if this is an accurate measure of Coast Guard performance in the PWCS mission. However, Coast Guard officials told us that they believe these reported results provide a useful proxy measure of Coast Guard performance, and noted that this is one of several metrics the Coast Guard uses to assess performance in the PWCS mission.

According to DHS's *Risk Management Fundamentals*, it is also important to be transparent about assumptions and key sources of uncertainty, so that decision makers are informed of the limitations of the risk information provided by the model. In its 2009 review of the risk reduction model, CREATE at the University of Southern California stated that it seemed likely that the model ignored important uncertainties and implied

[76]GAO/GGD-10.1.20.

[77]GAO/GGD-00-52.

[78]The model utilizes judgments as well as actual Coast Guard patrol data, mapping data that show Coast Guard assets in relation to potential targets, as well as consequence models from MSRAM.

incorrectly high precision of risk estimates.[79] Furthermore, OMB's *Updated Principles for Risk Analysis* notes that because of the inherent uncertainties associated with estimates of risk, presentation of a single risk estimate may be misleading and provide a false sense of precision. OMB suggests that when a quantitative characterization of risk is provided, a range of plausible risk estimates should also be provided.[80] From fiscal years 2006 to 2010, the Coast Guard reported the risk reduction measure as a specific risk reduction number rather than as a range of plausible risk reduction estimates. The Coast Guard official responsible for this measure told us this was because the previous risk reduction model was not capable of producing a range of plausible risk reduction estimates. The official noted that while the new risk reduction model—which will be used to report results for fiscal year 2011—is capable of producing a range of estimated risk reduction, the Coast Guard will continue to report the risk reduction measure as a single number because the DHS data system for performance reporting does not accept ranges—only numerical values. However, the official added that there is value in reporting a range of risk reduction and officials are considering a transition to a range of estimated reduction for the PWCS mission in future years. One alternative could be to report the percentage of risk reduced as a single number, but having an explanatory note indicating the range of plausible risk reduction estimates. Using a risk reduction measure that more accurately reflects performance effectiveness can give Coast Guard leaders and Congress a better sense of progress toward goals, which can support efforts to identify areas for improvement.

DHS officials have also raised some questions about the risk reduction measure. Recently, DHS determined that the Coast Guard's risk reduction measure was not appropriate for inclusion as a DHS strategic performance measure and has designated it as a management measure. According to DHS, a strategic measure is designed to communicate achievement of strategic goals and objectives and be readily understandable to the public, and a management measure is designed to

[79]See Barret et al., *Evaluation of U.S. Coast Guard Terrorism Risk and Decision Analysis Models and Processes for Port, Waterways and Coastal Security*. This review examined the Coast Guard's risk reduction model before the model was upgraded and improved in 2010.

[80]OMB, *Updated Principles for Risk Analysis*.

gauge program results and tie to resource requests and be used to support achievement of strategic goals. According to a senior DHS official, in 2010, DHS leadership reviewed all existing department measures and made decisions about which measures they believed were clearly tied to the DHS Quadrennial Homeland Security Review missions and were easily understandable by the public.[81] This official noted that based on this review, DHS leadership did not feel the risk reduction measure and its methodology would be easily understandable by the public and therefore did not designate the measure as a strategic measure. As a result, the risk reduction measure will not be included in DHS's annual performance plan, formally published with the Annual Performance Report, because this report only includes the smaller set of strategic measures.[82] However, this official noted that the risk reduction measure is important as one piece of information to manage risk and is considered to be part of the full suite of DHS performance measures, and will continue to be published in the Coast Guard's strategic context that is submitted with DHS's Annual Performance Report.[83]

Conclusions

The Coast Guard has invested substantial effort incorporating risk management principles into its security priorities and investments, and continues to proactively strengthen its assessment, management, and evaluation practices. As a result, the Coast Guard's risk assessments and risk model are generally sound and in alignment with DHS standards. However, there are some additional actions that the Coast Guard could

[81]In February 2010, DHS issued its first Quadrennial Homeland Security Review report, outlining a strategic framework for homeland security to guide the activities of the department and its homeland security partners, including federal, state, local, and tribal government agencies; the private sector; and nongovernmental organizations. The report identified five homeland security missions—Preventing Terrorism and Enhancing Security, Securing and Managing Our Borders, Enforcing and Administering Our Immigration Laws, Safeguarding and Securing Cyberspace, and Ensuring Resilience to Disasters—and goals and objectives to be achieved within each mission.

[82]According to a DHS official, there are no other risk reduction measures similar to the Coast Guard's risk reduction measure chosen as strategic measures.

[83]For fiscal year 2011, DHS identified 85 strategic measures for assessing its progress in achieving its Quadrennial Homeland Security Review missions and goals. In addition to these strategic measures, DHS also has 130 management measures, which DHS uses for resource allocation and other internal decision-making purposes, such as program evaluation. DHS includes its management measures in the Strategic Context presented to Congress with the department's budget request.

take to further its risk management approach by facilitating a wider use of risk information and making the results more valuable to the users. For example, since risk management is a tool for informing policymakers' decisions about assessing risks, allocating resources, and taking actions under conditions of uncertainty, the Coast Guard could better document and communicate the uncertainty or confidence levels of its risk assessment results, including any implications that the uncertainty may have for decision makers. This added information would allow Coast Guard decision makers to prioritize strategies, tactics, and long-term investments with greater insight about the range of likely results and associated trade-offs with each decision. Additional information would also allow external reviewers of the risk model to reach the most appropriate conclusions or provide the most useful improvement recommendations through periodic reviews. The Coast Guard could also enhance the risk-informed prioritization of its field-level strategies, operations, and tactics by ensuring that risk management training is expanded to multiple levels of Coast Guard decision makers at the sector level, including command-level personnel. Expanding training on how MSRAM could be used at all levels of command for risk-informed decision making—including how MSRAM can assist with the selection of different types of security measures and the evaluation of their impacts—would further the Coast Guard's efforts to implement its risk management framework and meet its goal of institutionalizing MSRAM as the risk management tool for maritime security. Finally, accurately representing performance results is important and the Coast Guard could more accurately convey its risk reduction performance measure by reporting risk reduction results as a range rather than a point estimate. Presenting risk reduction as a single number without a corresponding range of uncertainty could hamper Coast Guard efforts to identify areas for improvement. Taking these steps would make the Coast Guard's risk management approach even stronger.

Recommendations for Executive Action

To help the Coast Guard strengthen MSRAM and better align it with NIPP risk management guidance, as well as facilitate the increased use of MSRAM across the agency, we recommend that the Commandant of the Coast Guard take the following three actions:

(1) Provide more thorough documentation related to key assumptions and sources of uncertainty within MSRAM and inform users of any implications for interpreting the results from the model.

(2) Make MSRAM available to appropriate parties for additional external peer review.

(3) Provide additional training for sector command staff and others involved in sector management and operations on how MSRAM can be used as a risk management tool to inform sector-level decision making.

To improve the accuracy of the risk reduction measure for internal and external decision-making, we recommend that the Commandant of the Coast Guard take action to report the results of the risk reduction measure as a range rather than a point estimate.

Agency Comments and Our Evaluation

We provided a draft of this report to DHS and the Coast Guard on October 17, 2011, for review and comment. DHS provided written comments, which are reprinted in appendix II. DHS and the Coast Guard concurred with the findings and recommendations in the report, and stated that the Coast Guard is taking actions to implement our recommendations.

The Coast Guard concurred with our first recommendation that it provide more thorough documentation related to key assumptions and sources of uncertainty within MSRAM. Specifically, the Coast Guard stated that the documentation of uncertainty is part of the ongoing MSRAM VV&A process, and that the Coast Guard will continue to work with the DHS Office of Risk Management and Analysis in developing a feasible and deployable model that will benefit field-level security operations. These actions should improve the Coast Guard's ability to document and inform MSRAM users of any implications for interpreting results from the model, thereby addressing the intent of our recommendation.

Regarding the second recommendation that the Coast Guard make MSRAM available to appropriate parties for additional external peer review, the Coast Guard concurred. The Coast Guard stated that external peer review is part of the ongoing MSRAM VV&A process, and that additional external peer review will be part of an independent verification and validation of MSRAM expected to be completed in the fall of 2012. Such actions should address the intent of the recommendation.

Regarding the third recommendation that the Coast Guard provide additional training for sector command staff and others involved in sector management on how MSRAM can be used as a risk management tool,

the Coast Guard concurred. Specifically, the Coast Guard stated that MSRAM is part of the Coast Guard's contingency planning course, and the Coast Guard will explore other opportunities to provide risk training to sector command staff, including online and webinar training opportunities. Such actions, once implemented, should address the intent of the recommendation.

Finally, the Coast Guard also concurred with the fourth recommendation to take action to report the results of the risk reduction measure as a range rather than a point estimate. The Coast Guard stated that it is currently limited by the DHS data reporting system with regard to the format of presenting performance targets and results, but noted that it is currently working with DHS to determine options for reporting risk as a range. Such action, when fully implemented, should address the intent of the recommendation.

DHS and the Coast Guard also provided us with technical comments, which we incorporated as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the Secretary of Homeland Security, appropriate congressional committees, and other interested parties. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

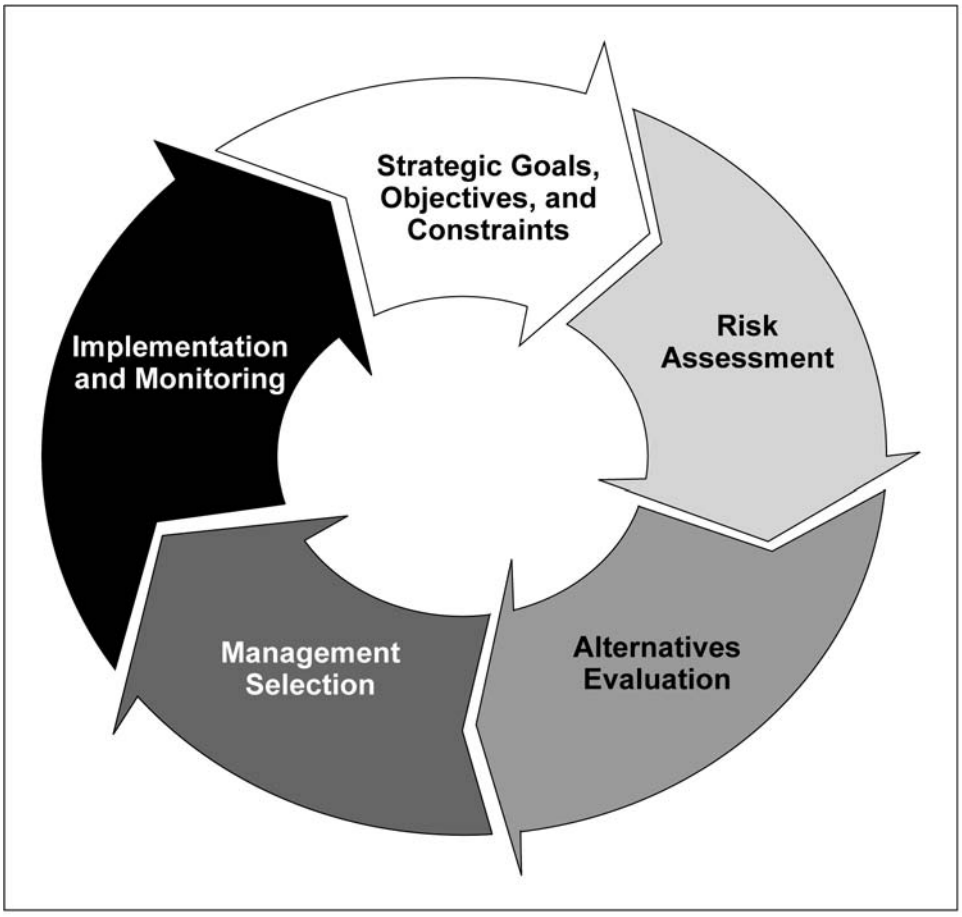
If you or your staff have any further questions about this report, please contact me at (202) 512-9610 or caldwells@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors are listed in appendix III.

Stephen L. Caldwell
Director, Homeland Security
and Justice Issues

Appendix I: Risk Management Framework

To provide guidance to agency decision makers, we developed a risk management framework which is intended to be a starting point for applying risk-informed principles.[1] Our risk management framework, shown in figure 2, 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.

Figure 2: GAO's Risk Management Framework



Source: GAO.

[1]See GAO-06-91.

Setting strategic goals, objectives, and constraints is a key first step in applying risk management principles and helps to ensure that management decisions are focused on achieving a purpose. Risk assessment, an important element of a risk-informed approach, helps decision makers identify and evaluate potential risks so that countermeasures can be designed and implemented to prevent or mitigate the effects of the risks. Risk assessment is a qualitative determination, quantitative determination, or both of the likelihood of an adverse event occurring and the severity, or impact, of its consequences. Risk assessment in a homeland security application involves assessing three key components—threat, vulnerability, and consequence. A threat assessment is the identification and evaluation of adverse events that can harm or damage an asset. A vulnerability assessment identifies weaknesses in physical structures, personal protection systems, processes, or other areas that may be exploited. A consequence assessment is the process of identifying or evaluating the potential or actual effects of an event, incident, or occurrence. Information from these three assessments contributes to an overall risk assessment that characterizes risks, which can provide input for evaluating alternatives and prioritizing security initiatives. The risk assessment element in the overall risk management cycle informs each of the remaining steps of the cycle. Alternatives evaluation addresses the evaluation of risk reduction methods by consideration of countermeasures or countermeasure systems and the costs and benefits associated with them. Management selection addresses such issues as determining where resources and investments will be made, the sources and types of resources needed, and where those resources would be targeted. The next phase in the framework involves the implementation of the selected countermeasures. Following implementation, monitoring is essential to help ensure that the entire risk management process remains current and relevant and reflects changes in the effectiveness of the alternative actions and the risk environment in which it operates. Program evaluation is an important tool for assessing the efficiency and effectiveness of the program. As part of monitoring, consultation with external subject area experts can provide a current perspective and an independent review in the formulation and evaluation of the program.

The *National Infrastructure Protection Plan* (NIPP), originally issued by the Department of Homeland Security (DHS) in 2006 and updated in 2009, includes a risk analysis and management framework, which, for the most part, mirrors our risk management framework. This framework includes six steps—set goals and objectives; identify assets, systems, and networks; assess risks; prioritize; implement programs; and measure

effectiveness. The NIPP is DHS's base plan that guides how DHS and other relevant stakeholders should use risk management principles to prioritize protection activities. In 2009, DHS updated the NIPP to, among other things, increase its emphasis on risk management, including an expanded discussion of risk management methodologies and discussion of a common risk assessment approach that provided core criteria for these analyses. Beyond the NIPP, DHS has issued additional risk management guidance and directives. For example, in January 2009 DHS published its *Integrated Risk Management Framework*, which, among other things, calls for DHS to use risk assessments to inform decision making. In April 2011, DHS issued its *Risk Management Fundamentals*, which establishes specific doctrine and guidance for risk management across DHS.

Appendix II: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, D.C. 20528

Homeland Security

November 7, 2011

Steven Caldwell
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO-12-14, "COAST GUARD: Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations"

Dear Mr. Caldwell:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

As the lead federal agency for maritime security, including the protection of U.S. ports, coasts, and inland waterways, the U.S. Coast Guard's mission involves protecting the maritime domain and marine transportation system, including preventing terrorists attacks, and responding to and recovering from attacks. To assist with this mission, since 2005, the Coast Guard has been using its Maritime Security Risk Analysis Model (MSRAM) as its primary approach for assessing and managing security risks, which has provided the Coast Guard with a standardized way of assessing risk of the maritime infrastructure.

The Department is pleased to note GAO's positive acknowledgement of the substantial efforts the Coast Guard had made incorporating risk management principles into its security priorities and investments. The draft report also recognizes that the Coast Guard continues to proactively strengthen its assessment, management and evaluation practices and, as a result, MSRAM generally meets DHS criteria for being complete, reproducible, documented, and defensible. The Coast Guard is taking action and developing long-term strategies to further improve MSRAM methodology and risk assessment process. It is important to note that related challenges are not unique to MSRAM or the Coast Guard, but faced by many others in the Homeland Security risk assessment community.

The draft report contained four recommendations with which the Department concurs. Specifically, GAO recommended that the Commandant of the Coast Guard:

Recommendation 1: Provide more thorough documentation related to key assumptions and sources of uncertainty within MSRAM and inform users of any implications for interpreting the results from the model.

Response: Concur. Documentation of uncertainty is part of the ongoing MSRAM Verification, Validation & Accreditation (VV&A) process, in coordination with DHS. The Coast Guard is analyzing how best to incorporate uncertainty estimates as part of the MSRAM risk results. As many of the assumptions and sources of uncertainty stem from a lack of existing functional, rather than theoretical, security risk models, the Coast Guard will continue to work with the DHS National Protection and Programs Directorate (NPPD) Office of Risk Management and Analysis (RMA) personnel in developing a feasible and deployable model that will benefit field-level security operations.

Recommendation 2: Make MSRAM available to appropriate parties for additional external peer review.

Response: Concur. External peer review is part of the ongoing MSRAM VV&A process, in coordination with NPPD RMA. The Coast Guard has already conducted an independent verification and validation (IV&V) of MSRAM, completed in March 2010, and is in the process of conducting a second IV&V as part of the MSRAM VV&A accreditation process. External peer reviews were included in the first IV&V and will be part of the second IV&V, which is expected to be completed in the fall of 2012.

Recommendation 3: Provide additional training for sector command staff and others involved in sector management and operations on how MSRAM can be used as a risk management tool to inform sector-level decision making.

Response: Concur. MSRAM is currently part of the "Risk-Based Decision Making" lesson taught within the Coast Guard's Contingency Planning Course. The lesson objectives are to identify how risk-based decision making will impact preparedness planning, and demonstrate the uses of MSRAM to develop preparedness plans. The Coast Guard will also continue to explore other opportunities to provide risk training to Sector command staff, including online and Webinar training opportunities.

Recommendation 4: Take action to report the results of the risk reduction measure as a range rather than a point estimate.

Response: Concur. The Coast Guard is currently limited by the DHS data reporting system with regard to the format (i.e. performance targets and results). The Coast Guard is currently working with DHS OCFO/Program Analysis &Evaluation to determine options for reporting risk as a range vice a single number.

2

Again, thank you for the opportunity to review and comment on this draft report. Technical and sensitive comments were provided under separate cover. We look forward to working with you on future Homeland Security issues.

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

3

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Stephen L. Caldwell, (202) 512-9610 or caldwells@gao.gov

Staff Acknowledgments

In addition to the contact named above, Dawn Hoff, Assistant Director and Adam Hoffman, Analyst-in-Charge, managed this assignment. Chuck Bausell, Charlotte Gamble, and Grant Sutton made significant contributions to this report. Colleen McEnearney provided assistance with interviews and data analysis. Michele Fejfar assisted with design, methodology, and data analysis. Jessica Orr provided assistance with report development, and Geoff Hamilton provided legal assistance.

Related GAO Products

Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened. GAO-12-47. Washington, D.C.: November 17, 2011.

Maritime Security: Progress Made but Further Actions Needed to Secure the Maritime Energy Supply. GAO-11-883T. Washington, D.C.: August 24, 2011.

Maritime Security: DHS Progress and Challenges in Key Areas of Port Security. GAO-10-940T. Washington, D.C.: July 21, 2010.

Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain. GAO-10-400. Washington, D.C.: April 9, 2010.

Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience. GAO-10-296. Washington, D.C.: March 5, 2010.

Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation. GAO-09-492. Washington, D.C.: March 27, 2009.

Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions. GAO-07-454. Washington, D.C.: August 17, 2007.

Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure. GAO-06-91. Washington, D.C.: December 15, 2005.

Managing for Results: Enhancing Agency Use of Performance Information for Management Decision Making. GAO-05-927. Washington, D.C.: September 9, 2005.

Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection. GAO-04-557T. Washington D.C.: March 31, 2004.

Managing for Results: Challenges Agencies Face in Producing Credible Performance Information. GAO/GGD-00-52. Washington, D.C.: February 4, 2000.

The Results Act: An Evaluator's Guide to Assessing Agency Annual Performance Plans. GAO/GGD-10.1.20. Washington, D.C.: April 1998.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548