Department of Homeland Security
Office of Inspector General

DHS' Strategy and Plans to Counter Small Vessel Threats Need Improvement

OIG-09-100

September 2009

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

September 10, 2009

Preface

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report assesses the efficacy of the Department of Homeland Security's strategy to secure our ports, waterways, and maritime borders from small vessel threats. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all who contributed to the preparation of this report.

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendixes

Abbreviations

CBP	Customs and Border Protection
DHS	Department of Homeland Security
GAO	Government Accountability Office
OIG	Office of Inspector General

Executive Summary

A small vessel, such as a commercial fishing vessel or recreational boat, can be used as a waterborne improvised explosive device, as a platform for conducting an attack, or to smuggle weapons or terrorists into the United States. Recognizing the threat, in mid-2006, the Department of Homeland Security initiated a working group to develop a small vessel security national strategy. In April 2008, the department published the Small Vessel Security Strategy to address these potential threats. The department is also developing an Implementation Plan, which is intended to provide direction to federal, state, and local agencies on achieving the major goals outlined in the Strategy. We reviewed the Small Vessel Security Strategy and the draft Implementation Plan to determine whether the department has developed a comprehensive approach for securing our ports, waterways, and maritime borders from small vessel threats.

Overall, the department has made progress, but more remains to be done to provide effective guidance and operate effective programs to address small vessel threats. The Strategy addresses two desirable characteristics of an effective national strategy as it defines the problem, and uses risk assessments to analyze the threats. However, the Strategy only partially addresses the remaining four characteristics. It partially addresses elements such as strategic priorities and milestones, and roles and responsibilities of state and local sectors, but it does not address performance measures, associated costs or human capital, or accountability and oversight frameworks.

Additionally, critical programs intended to support small vessel security may not be operating effectively. Although the department recognizes the need to raise public awareness and take action to mitigate the risk of small vessel threats, its approach was hindered because its components are not fully integrated. As a result, the nation's ports, waterways, and maritime borders remain vulnerable to small vessel threats. The department partially concurred with our recommendation that it address the missing elements in its strategy. The department nonconcurred with our recommendation that it evaluate the effectiveness of the programs it intends to use to meet the strategy's goals.

Background

The Department of Homeland Security (DHS) recognizes the need to address the threats that small vessels pose to the United States. Small vessels are categorized as any watercraft of less than 300 gross tons and used for recreational or commercial purposes, regardless of method of propulsion. Small vessels include commercial fishing vessels, recreational boats and yachts, towing vessels, uninspected passenger vessels, and any other personal or commercial vessels involved in U.S. or foreign voyages. With 95,000 miles of shoreline, 300,000 square miles of waterways, 360 ports of call, 12,000 marinas, and an estimated 17 million small vessels presently operating in U.S. waters, it is extremely difficult to distinguish friend from foe.

DHS has identified four scenarios of gravest concern regarding the potential use of small vessels in terrorist-related activities: using a small vessel (1) as a waterborne improvised explosive device, (2) to smuggle weapons (including weapons of mass destruction) into the United States, (3) to smuggle terrorists into the United States, and (4) as a waterborne platform for conducting an attack.

These four scenarios are based on terrorist acts that have involved small vessels. For example, in October 2000, Al-Qaeda attacked the *USS Cole* by navigating an explosive-laden small boat alongside the destroyer as it was refueling pier side at the port of Aden in Yemen. Seventeen U.S. Navy sailors were killed in the explosion. (See figure 1.)

Figure 1. The *USS Cole* with a large hole in her left side after being struck by an Al-Qaeda waterborne improvised explosive device. Photo – Department of Defense.

In October 2002, Al-Qaeda directed an attack by an explosive-laden small boat against the French oil tanker M/V *Limburg* off the coast of Yemen. The attack resulted in a large oil spill and fires on board the tanker, and killed one and injured four crew members. (See figure 2.)

Figure 2. M/V *Limburg* on fire off the coast of Yemen after being struck by an Al-Qaeda waterborne improvised explosive device. Photo – DHS.

In a recent surge of international piracy, terrorists have used small vessels to hijack cruise ships, tankers, and other vessels. In 2007, 206 acts of piracy were committed, and 76 others attempted. In September 2008, Somali pirates used three small vessels to surround and seize the *MV Faina*, which was carrying 33 Russian

T-72 tanks and other weapons and ammunition. The captain of the vessel died during the assault, and the pirates demanded $35 million for the release of the ship and the crew. (See figure 3.)

Figure 3. Using small vessels, Somali pirates armed with rocket-propelled grenades and AK-47 assault rifles hijack the *MV Faina* in September 2008. Photo – U.S. Navy.

In November 2008, terrorists hijacked a Pakistani fishing boat, killing the captain and crew. The terrorists then sailed the boat to Mumbai, India, where they went ashore in small inflatable boats and carried out an attack that killed more than 170 people and held India's financial capital hostage for 3 days. (See figure 4.)

Figure 4. Eleven terrorists went ashore in inflatable boats and attacked the Taj Mahal Hotel in Mumbai, India. Photo – Reuters.

As these events demonstrate, the threat posed by terrorists operating small vessels is daunting.

In June 2007, the DHS National Small Vessel Security Summit, held in Arlington, Virginia, brought together approximately 300 small vessel maritime stakeholders and top federal, state, and local government officials to share concerns about small vessel operations, safety, and security. Using recommendations from the National Summit, risk management principles, and previous U.S. Coast Guard (Coast Guard) and U.S. Customs and Border Protection (CBP) analyses of small vessel threats, a DHS working group developed the Small Vessel Security Strategy, which DHS published in April 2008, to address the risks of small vessels to national security.

The overall objective of the Small Vessel Security Strategy is to close security gaps and enhance the small vessel security environment. The Strategy lists four major goals for achieving small vessel security:

1. Develop and leverage a strong partnership with the small vessel community and public and private sectors in order to enhance maritime domain awareness.

2. Enhance maritime security and safety based on a coherent plan with a layered, innovative approach.

3. Leverage technology to enhance the ability to detect, determine the intent of, and when necessary, interdict small vessels.

4. Enhance coordination, cooperation, and communications between federal, state, local, and tribal partners and the private sector, as well as international partners.

Results of Audit

Improvements Needed in DHS' Small Vessel Security Strategy

DHS has not provided a comprehensive strategy for addressing small vessel threats. Neither its Small Vessel Security Strategy nor its draft Implementation Plan effectively addresses all the desirable characteristics and elements of a national strategy. In addition, the department has not evaluated the effectiveness of critical programs that are expected to serve

as a foundation for small vessel security and may not be providing anticipated results.

Desirable Characteristics of an Effective National Strategy

In 2004, the Government Accountability Office (GAO) published guidance identifying six desirable characteristics of an effective national strategy for combating terrorism.[1] With each characteristic, GAO provided examples of elements that national strategies might include to ensure that agencies properly address them. Table 1 summarizes these desirable characteristics and their elements.

Table 1. Desirable Characteristics and Their Elements

Desirable Characteristic	Brief Description of Elements
1. Purpose, scope, and methodology	Why the strategy was produced, the scope of its coverage, and the process by which it was developed.
2. Problem definition and risk assessment	The particular national problems and threats that the strategy is designed to mitigate.
3. Goals, subordinate objectives, activities, and performance measures	The goals that a strategy is trying to achieve and steps to accomplish those goals, as well as the priorities, milestones, and performance measures to gauge results.
4. Resources, investments, and risk management	The cost, sources, and types of resources and investments needed to carry out a strategy, as well as where resources and investments should be targeted by balancing risk reductions and costs.
5. Organizational roles, responsibilities, and coordination	Who will be implementing the strategy, what their respective roles will be, and how they will coordinate their efforts.
6. Integration and implementation	How the strategy relates to other strategies' goals, objectives, and activities, as well as to subordinate levels of government and their plans for implementing the strategy.

[1] *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism* (GAO-04-408T, February, 2004).

These characteristics are intended to help shape the policies, programs, priorities, resource allocations, and standards that federal agencies and other stakeholders use to implement their national strategies. The guidance is also designed to assist agencies in evaluating progress, ensuring accountability, and achieving anticipated results from strategy implementation. GAO emphasized that it would be useful for agencies to address in their strategies all of the characteristics, which logically flow from conception to implementation. Appendix C provides additional details on each characteristic.

DHS' Strategy Does Not Address All Desirable Characteristics

DHS' Small Vessel Security Strategy does not effectively address all the desirable characteristics in GAO's guidance for providing an effective national strategy, even when supported by the draft Implementation Plan. (See Appendix D.) Of the six desirable characteristics, the Strategy and Implementation Plan together address the first two and partially address the remaining four.

Characteristics Addressed

The first two desirable characteristics, which the Strategy addresses, provide the foundation for developing specific actions to address the problems and risks posed by small vessels. Specifically, the DHS Small Vessel Security Strategy addresses the following:

Purpose, scope, and methodology The intent of the Small Vessel Security Strategy is to reduce potential security and safety risks from small vessels by adopting and implementing a coherent system of regimes, awareness, and security operations that strike the proper balance between fundamental freedoms, adequate security, and continued economic stability. The Strategy describes the scope of coverage, identifying the stakeholders involved and the Strategy's relationships to other strategies and plans. The Strategy also addresses the DHS working group's methodology for developing the Strategy.

Problem definition and risk assessment The Small Vessel Security Strategy addresses the complexities in managing the risks posed by small vessels. The Strategy notes that small vessels are not centrally registered, are not always proficiently operated, and the ability to screen or detect vessel-borne hazards is extremely limited. Furthermore, small vessel operators have a tradition and expectation of largely unrestricted access to U.S. waterways.

These complexities present unique challenges in assessing the risks posed by small vessels.

The Strategy identifies four scenarios of gravest concern regarding the potential use of small vessels as:

- A waterborne improvised explosive device;
- A conveyance for smuggling weapons, including weapons of mass destruction, into the United States;
- A conveyance for smuggling terrorists into the United States; or
- A waterborne platform for conducting attacks.

By defining the problem and assessing the risk, responsible parties could tailor approaches to address the needs of specific regions or sectors.

Characteristics Partially Addressed

The Small Vessel Security Strategy and draft Implementation Plan partially address the remaining four desirable characteristics of an effective strategy.

Goals, objectives, activities, and performance measures The draft Implementation Plan provides short-term and long-term actions for fulfilling the goals outlined in the Small Vessel Security Strategy; however, it does not address priorities, milestones, performance measures, or progress indicators. Without these elements, it is difficult to effectively monitor progress, establish accountability, and ensure program success.

Resources, investments, and risk management The Small Vessel Security Strategy only partially addresses this characteristic, as it does not sufficiently address detailed information regarding strategic costs, human capital, resources, or economic principles. Furthermore, the draft Implementation Plan simply categorizes funding levels as high, medium, or low without providing any dollar amounts, stating only whether an action is or is not currently funded. A strategy should address the sources and types of resources and investments needed, consider the actual costs associated with implementing the strategy, and define where resources and investments should be targeted. Without addressing these elements, DHS cannot coordinate implementation efforts effectively and efficiently across its numerous components.

Organizational roles, responsibilities, and coordination The Small Vessel Security Strategy addresses the roles and responsibilities of specific federal agencies in some detail, but it only partially addresses the roles and responsibilities of state, local, private, and international sector partners. Furthermore, the Strategy partially addresses the lead, support, and partner roles and responsibilities, but does not address any accountability and oversight framework, or how conflicts will be resolved. The draft Implementation Plan identifies lead federal agencies for each proposed action; however, it does not address how the implementing agencies will coordinate their efforts. As directed by Section 801(b) of the *Homeland Security Act of 2002* (Public Law 107-296), DHS is required to develop a process for receiving meaningful input from states and localities to assist in the development of a national strategy "for combating terrorism and other homeland security activities." The Small Vessel Security Strategy provides a generic list of functional responsibilities, but it does not provide the mechanisms needed to coordinate and collaborate on these responsibilities.

Integration and implementation The Strategy addresses how it integrates with other national strategies, but it only partially addresses details on specific federal, state, local, or private strategies and plans. It does not address and provide implementation guidance for state, local, or private strategies and plans. By not providing integration guidance, DHS risks ineffective and inefficient Strategy implementation.

Programs and Processes Supporting the Strategy

The Small Vessel Security Strategy and draft Implementation Plan identify existing programs and processes that DHS plans to use to combat the risks posed by small vessels. They include America's Waterway Watch, Pleasure Boat Reporting System, and various information-sharing processes that the department did not evaluate before including them in the solution to the small vessel security threat. These programs and processes need improvement to ensure that they are operating effectively and providing anticipated results.

America's Waterway Watch

The Small Vessel Security Strategy and draft Implementation Plan identify America's Waterway Watch as a key program to support the goal of developing and leveraging strong partnerships with the small vessel community to enhance maritime domain awareness. The program is intended to serve as a tool for the maritime

industries, recreational boating communities, and the public to report suspicious and unusual maritime activity via a 24-hour hotline. (Appendix E provides a more detailed description of these programs and processes.) However, the effectiveness of America's Waterway Watch is limited because it is not widely known to the maritime and boating communities, calls are not tracked, and it does not fully leverage public participation.

- America's Waterway Watch is not widely known. Of the estimated 13 million registered boaters within the United States, only 440,000 received informational brochures sent inside national vessel documentation packets. An additional 1 million boaters received information on America's Waterway Watch when they renewed their vessel's state registration.[2] Therefore, the Coast Guard may not have reached out to more than 90% of the estimated registered boaters. According to representatives from recreational vessel interest groups and national associations, the program is not widely known because the Coast Guard has not conducted sufficient public outreach. In 2007, the America's Waterway Watch hotline received 197 calls from the public. This limited public awareness inhibits the usefulness of the program.

- America's Waterway Watch calls are not tracked. Calls to the America's Waterway Watch hotline are routed through the National Response Center, where they are screened and forwarded to the appropriate authorities in the area where the suspicious activity was reported. The National Response Center is staffed by Coast Guard personnel who monitor the hotline 24 hours a day, 365 days a year. However, the National Response Center does not have the capability to record the phone numbers that call in, the frequency of calls, or the results of the information provided. As a result, the Coast Guard is unable to determine the overall effectiveness of the America's Waterway Watch program. A method to track the calls and their outcome is essential to monitor and evaluate the program's efficiency and effectiveness.

- Citizen's Action Network. In addition to the America's Waterway Watch, the draft Implementation Plan identifies the Citizen's Action Network as a program that could

[2] *America's Waterway Watch–U.S. Coast Guard's Maritime Homeland Security Outreach Program* (U.S. Coast Guard presentation, October 2008).

support the Strategy's goal of developing and leveraging a strong partnership with the small vessel community. The Citizen's Action Network seeks to leverage the general public's active participation. It differs from America's Waterway Watch in that it acquires information from vetted, trained members in addition to the general public.

The Citizen's Action Network can track both the outcomes of the information provided and the degree of member participation, and therefore can evaluate the overall effectiveness of the program. The draft Implementation Plan states that the Coast Guard has plans for a pilot program to expand and combine public outreach programs, but the pace of development is slow due to resource constraints. Coast Guard officials in the field, however, conducted a cost-benefit analysis to support the conclusion that the Citizen's Action Network program could be implemented nationwide with few to no additional resources.

Because of minimal public awareness, inability to track calls, and limited participation, the America's Waterway Watch program is unable to effectively support the Small Vessel Security Strategy's goals. DHS should evaluate the Citizen's Action Network program and its usefulness as a possible best practice to better leverage the public's participation and maritime domain awareness.

Pleasure Boat Reporting System

The Small Vessel Security Strategy states that DHS should use data gathered from the Pleasure Boat Reporting System program to improve data analysis capabilities to target high-risk small vessels. CBP administers the Pleasure Boat Reporting System program, which requires small vessel boaters traveling from a foreign country to self-report their arrival to the United States immediately. However, both the Strategy and CBP officers state that the Pleasure Boat Reporting System is ineffective and the data it gathers are not accurate. Specifically, the Strategy states,

During Fiscal Year 2006, only 70,000 boater foreign arrivals were recorded in the U.S. Customs and Border Protection (CBP) Pleasure Boat Reporting System (PBRS), based on boater self-reporting. Conservative estimates suggest that these reporting figures represent only a

fraction of the actual international boater traffic, especially given the ease with which boaters operate in these waters.

In January 2009, CBP provided OIG with total small vessel arrival data for the past 3 fiscal years pulled directly from the Pleasure Boat Reporting System (see table 2).

Table 2. PBRS Small Vessel Arrivals

Fiscal Years	Small Vessel Arrivals
2006	50,304[3]
2007	56,277
2008	52,595

Previously, CBP analyzed the Pleasure Boat Reporting System program and determined that only 10% to 25% of boaters actually self-report their arrivals when returning from foreign ports. Based on a conservative estimate of 25% and the total number of arrivals recorded in 2008, approximately 160,000 vessels did not self-report in 2008. This results in a large amount of unrecorded data; more important, these undocumented arrivals could lead to a potentially large number of dangerous people and things illicitly entering the country using small vessels.

Boaters may not be self-reporting because: (1) they are unaware of reporting requirements, (2) they experience extended waits and processing times, and (3) they experience inconsistent consequences regarding the failure to report.

According to CBP Office of Field Operations officials, current outreach efforts do not reach millions of small vessel boaters, and many boaters may not be aware of the self-reporting requirements. In one city, outreach efforts include CBP officers visiting local yacht clubs and marinas and attending local boat shows to promote the Pleasure Boat Reporting System program, as well as updating signs posted at 600 marinas. Despite these efforts to increase public outreach, the number of reported arrivals remains low.

[3] CBP Office of Field Operations, Planning, Program Analysis and Evaluation Measurements Branch provided small vessel arrival data as of January 15, 2009. For FY 2006, the Small Vessel Security Strategy states that 70,000 arrivals were recorded. CBP officials were unable to explain the difference between the Pleasure Boat Reporting System data provided to OIG and the data presented in the Strategy.

Boaters who know the reporting requirements may be deterred from self-reporting because CBP cannot always quickly and effectively process arrivals, thereby causing long delays. For example, at one of the ports visited, the Pleasure Boat Reporting System office has limited staff. CBP states that because of the limited number of CBP officers manning the phone lines in this office, boaters may experience extended waiting and processing times. These delays deter numerous boaters from calling in to report their arrival, and many who do call hang up without completing the reporting process.

Last, CBP's policies regarding its response to the failure to report foreign boat arrivals may need strengthening. Under the *Tariff Act of 1930,* any operator of a small vessel operator who fails to report immediately the vessel's arrival is liable for a civil penalty of $5,000 for the first violation and $10,000 for each subsequent violation, and the small vessel used in connection with the violation(s) may be seized.[4] Further, under 19 U.S.C. 1436(c), the vessel operator may be subject to criminal penalties if the failure to report the vessel's arrival was intentional. However, CBP's policies allow officers the discretion to issue first time violators a warning letter. CBP officers said that in FY 2008, one port issued 137 warning letters to first-time violators. Without the consistent application of more serious consequences, small vessel boaters may not feel compelled to self-report, and the Pleasure Boat Reporting System will continue to have inaccurate data to target high-risk small vessels.

To improve small vessel operations data, the draft Implementation Plan lists numerous short- and long-term actions for improving the methods of data gathering. One action includes requiring small vessel operators traveling to the United States from a foreign seaport to provide notice of arrival 1 hour prior to departure from an overseas port. Although this may help alert CBP officers of incoming vessels, without addressing the issues of public awareness, processing delays, and inconsistent enforcement of serious consequences, these actions may be ineffective in meeting the Small Vessel Security Strategy's goals.

As a result, the Pleasure Boat Reporting System program is not providing complete data for targeting high-risk small vessels, and may be ineffective for countering small vessel threats as required

[4] 19 U.S.C. 1436(b), *Tariff Act of 1930 – Penalties for violations of arrival, reporting, entry, and clearance requirements.*

in the Small Vessel Security Strategy and draft Implementation Plan.

Information-Sharing Processes

The Small Vessel Security Strategy states that because of the large number of small vessels operating in the maritime domain, it is "virtually impossible for any single government entity at any level to have sufficient information, resources, expertise, or statutory authority to address the spectrum of potential risks related to small vessels."[5] The Strategy calls for leveraging the department's current capabilities for coordinating, cooperating, and communicating information on small vessel threats among all stakeholders in an effective and timely manner. However, some of the DHS systems used to share information may not be accessible to all DHS components, thus limiting their ability to effectively share information.

CBP administers TECS[6], one of the largest law enforcement databases operated by DHS. It provides storage and access to personally identifiable information that is collected through other government databases.

Although TECS is available to many federal, state, and local agencies, it is not readily available to the Coast Guard, the largest maritime law enforcement entity. Currently, the Coast Guard has limited access to the information housed in the database, and it does not regularly add new information obtained through its vessel interdictions. Instead, the Coast Guard uses another database, the Maritime Information for Safety and Law Enforcement system, to store the information it obtains during small vessel interdictions.

Although the Coast Guard shares its data through the Maritime Information for Safety and Law Enforcement among its own offices, CBP and other law enforcement agencies do not have expeditious access to the Coast Guard system. The disconnect between the Maritime Information for Safety and Law Enforcement and TECS, and the department's methods for inputting, storing, and retrieving information, may restrict the ability of CBP, the Coast Guard, and other law enforcement agencies to counter small vessel threats. Without addressing these limitations, the department is not leveraging its capabilities for

[5] *Small Vessel Security Strategy* (DHS, April 2008).
[6] TECS is not an acronym.

coordinating, cooperating, and communicating information effectively.

DHS Components Not Fully Integrated

Although DHS recognized the need to increase public awareness and take action to mitigate the risks posed by small vessels, DHS' approach was hindered because its components are not fully integrated. In addition, the working group tasked with developing the strategy decided not to follow all the guidance available in GAO's desirable characteristic report.

In mid-2006, the DHS Office of Policy set up a working group to develop a small vessel security national strategy. The working group determined that better public outreach was necessary to educate the public and garner its support in combating the small vessel threat. Therefore, they began their efforts to engage stakeholders, and in June 2007, DHS sponsored the first National Small Vessel Security Summit. The summit brought together approximately 300 stakeholders and federal observers to discuss a range of issues involving the security risks posed by small vessels in the U.S. maritime domain. After the summit, the working group continued to develop the Strategy, which was published in April 2008.

The working group's members cut across multiple DHS components and organizations but did not feel empowered to make departmental decisions while developing the Strategy. For example, the working group decided that the Strategy and Draft Implementation Plan would not set specific performance measures on the components, nor would they specifically define costs or human capital requirements associated with the Strategy. Working group members also stated that they considered the GAO desirable characteristics and elements standards but determined that not all the elements applied to the Small Vessel Security Strategy. In some instances the working group determined that it was not the appropriate forum to discuss or address recommended elements.

Although it is difficult to ensure that all national strategies are able to provide details on each and every characteristic, the guidance should be considered a best practice. National strategies that contain all of these characteristics increase their usefulness as guidance for policy and decision-makers in allocating resources and balancing homeland security priorities.

Finally, the working group relied on each component to vet the programs and processes presented to the working group in support of the Strategy. However, the working group did not verify the information to ensure that the programs and processes were operating effectively before including

them as part of an overall solution because they determined that each component was solely responsible for the information they provided.

Until a comprehensive approach is fully evaluated, developed, and implemented, the United States will remain vulnerable to the threats posed by small vessels. Without fully evaluating and mitigating these weaknesses in the programs and processes supporting the Strategy, DHS may not achieve its goal of protecting our nation against dangerous people and addressing critical opportunities to identify and prevent terrorist acts.

Recommendations

We recommend that DHS develop a more comprehensive small vessel security strategy by:

Recommendation #1: Addressing the desirable characteristics and elements missing from its Strategy and draft Implementation Plan.

Recommendation #2: Evaluating the effectiveness of programs intended to support small vessel security before including them as part of a solution to improve security against the small vessel threats.

Management Comments and OIG Analysis

We obtained written comments on our draft from the Assistant Secretary, Office of Policy, the U.S. Coast Guard Commandant, and the Acting Commissioner, U.S. Customs and Border Protection on behalf of DHS. The department submitted technical comments and corrections, and raised the issue that some information within the report may require restricted public access. We reviewed the report and made changes to ensure the accuracy of the information. We also reviewed the report and coordinated with the department to resolve sensitivity comments and to ensure the report was publicly releasable in its entirety. There is no need for the report to be restricted to For Official Use Only (FOUO). We have included a copy of the comments in their entirety at Appendix B. In the comments, DHS partially concurred with recommendation 1 and did not concur with recommendation 2. The following is an evaluation of DHS' comments.

Management Comments to Recommendation #1: DHS partially concurs with the OIG's recommendation to address the desirable characteristics and elements missing from its Strategy and Implementation Plan. DHS acknowledges that some of the six desirable characteristics of an effective national strategy could be

addressed more fully in the Strategy. DHS acknowledges that performance metrics for federal, state, local, tribal, and private sector initiatives as well as associated costs were not addressed in great detail in the Strategy. DHS plans to work to more fully address these elements in the execution of the Implementation Plan. DHS noted that many of the desirable characteristics were indeed addressed in the Strategy.

OIG Analysis: We consider DHS' proposed actions partially responsive to the recommendation. We acknowledged in our report that the Strategy addresses the first two desirable characteristics as it defines the problem, and uses risk assessments to analyze the threats. However, as illustrated at Appendix D, the Strategy only partially addresses the remaining four characteristics because it explicitly cites some, but not all, of the elements of the remaining four characteristics. The designation "partially addresses" can be used for a strategy that addresses few of the elements of a characteristic and a strategy that addresses most of the elements of a characteristic, but not all. To have a more robust and effective strategy, DHS should work to more fully address these elements, as appropriate. This recommendation will remain unresolved and open until DHS provides evidence that it considered the missing elements and addressed them, as appropriate, in the Strategy.

Management Comments to Recommendation #2: DHS does not concur with the recommendation to evaluate the effectiveness of programs intended to support small vessel security before including them as part of a solution to improve security against the small vessel threats. DHS stated that the agencies that submitted specific actions for the implementation plan considered their effectiveness to support small vessel security in view of the Strategy.

OIG Analysis: We consider this recommendation open and unresolved. The interagency working group was unable to provide evidence that the programs or actions submitted by the agencies had been evaluated. Further, during the course of the review, we identified weaknesses in these programs that could hinder their effectiveness in combating the small vessel threat. We ask that DHS reconsider its response to our recommendation and advise us of plans and strategies for its implementation.

Our objective was to determine the effectiveness of DHS' approach for improving national maritime security against small vessel threats. To achieve our audit objective, we reviewed the DHS Small Vessel Security Strategy, draft Implementation Plan, and selected programs used to support the Small Vessel Security Strategy.

We observed operations carried out in support of small vessel security in various ports, and we interviewed personnel at the U.S. Coast Guard Intelligence Coordination Center in Suitland, MD. We interviewed U.S. Coast Guard personnel in the Offices of Vessel Activities, Boating Safety Division, and America's Waterway Watch Program. We also interviewed U.S. Customs and Border Protection personnel in the offices of Pleasure Boat Reporting System Program, Intelligence and Operations Coordination, and Air & Marine Operations. We met with state and local law enforcement officials to discuss communication, coordination, and cooperation efforts regarding small vessel security.

We reviewed prior DHS OIG, GAO, and Homeland Security Institute reports discussing maritime security and national strategies related to terrorism.

We reviewed the Small Vessel Security Strategy and draft Implementation Plan and compared them to the desirable characteristics and supporting elements of an effective national strategy as set forth in GAO's report, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism.*[7] (See Appendix D.)

To ensure consistency, we used GAO's definitions to determine the extent to which the Small Vessel Security Strategy satisfied each of the six desirable characteristics.

We conducted our audit at DHS, Coast Guard, and CBP headquarters in Washington, DC. We also performed fieldwork at two ports. We conducted this performance audit between August 2008 and January 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate

[7] *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism* (GAO-04-408T), February 2004.

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.

We would like to thank the Coast Guard, CBP, and DHS Office of Policy for the cooperation and courtesy they extended to our staff during this audit.

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

August 10, 2009

Richard L. Skinner
Inspector General
Office of the Inspector General
Department of Homeland Security

Dear Mr. Skinner:

RE: Draft OIG Report: "DHS' Strategy and Plans to Counter Small Vessel Threats Need Improvement"

The Department of Homeland Security (DHS) is pleased to comment on the Office of Inspector General's (OIG) draft report on the Small Vessel Security Strategy (the Strategy). DHS appreciates OIG's recognition of our progress made to-date to provide effective guidance and operate robust programs to address small vessel threats. We remain committed to managing and controlling risks posed by the potential threat and possibly dire consequences of small vessel exploitation.

As you noted in your report, DHS developed the Strategy after close consultation with private, commercial and government stakeholders in the small vessel community. DHS convened the National Small Vessel Security Summit (NSVSS) in June 2007 to engage more than 300 stakeholders on the security risks posed by small vessels in the U.S. maritime domain, including the risks of international arrivals. The information developed from the NSVSS, as well as a number of subsequent discussions with stakeholders, informed the development of a strategic-level national small vessel security strategy.

We have restricted our written comments to points that are directly relevant to the two OIG recommendations.

Recommendation 1: OIG recommends that DHS develop a more comprehensive small vessel security strategy by addressing the desirable characteristics and elements missing from its Strategy and draft Implementation Plan.

DHS partially concurs with Recommendation One. DHS acknowledges that some of the six desirable characteristics of an effective national strategy identified by the Government Accountability Office (GAO) in their 2004 report entitled "*Evaluation of Selected Characteristics in National Strategies Related to Terrorism*" *(GAO-04-408T)* could be addressed more fully in the Small Vessel Security Strategy.

DHS did make considerable effort to address all characteristics in the Strategy. However, despite the fact that the OIG report concluded that these elements are desirable characteristics rather than requirements that must be included in a strategy, DHS does acknowledge that performance metrics for Federal, state, local, tribal, and private sector initiatives as well as associated costs were not

U.S. Department of Homeland Security
Washington, DC 20528

addressed in great detail in the Strategy.[1] DHS will work to more fully address these elements as appropriate in the execution of the Implementation Plan and as small vessel security processes and procedures are further developed. The draft Implementation Plan evaluated programs, placed them under the appropriate goals and objectives of the Strategy, and further stratified them based on their short or long-term nature in meeting an objective. DHS will focus efforts on better defining performance measures and associated costs for the Strategy as this Implementation plan is finalized.

DHS notes, however, that many of the desirable characteristics were indeed addressed in the Strategy. Specific references made in the Strategy to each of the six desirable characteristics are provided below:

1. Purpose, Methodology and Scope: covered in pages 1-2.
2. Problem definition and risk assessment: covered in pages 11-14.
3. Goals, subordinate objectives, activities, and performance measures: DHS acknowledges that performance metrics and associated costs were not addressed in great detail in the Strategy. DHS will work to more fully address these elements as small vessel security processes and procedures are further developed.
4. Resources, investments, and risk management: covered in pages 18, 20, 22-27, and A-2 thru A-4. DHS acknowledges that the Strategy lacks details on specific Federal, state, local, tribal, and private sector initiatives from which to calculate a total cost and a breakdown by entity. Therefore, the Implementation Plan categorized costs as high, medium, and low as provided by the relevant government or private organization. While costs associated with some of the newer programs are unavailable, specific dollar amounts for the other programs are covered on page 26.
5. Organizational roles, responsibilities, and coordination: covered in pages 24-28.
6. Integration and implementation: covered in the "Relationship to Other Strategies and Plans" section in pages 1-2, and pages 23, and 29.

Recommendation 2: OIG recommends that DHS evaluate the effectiveness of programs intended to support small vessel security before including them as part of a solution to improve security against the small vessel threats.

DHS does not concur with OIG Recommendation Two. The agencies that submitted specific actions (called programs by OIG) for the Implementation Plan considered their effectiveness to support small vessel security in view of the Strategy. These inputs were then considered by the interagency working group drafting the Implementation Plan. The OIG's assertion that some of these programs, to include America's Waterway Watch (AWW), are ineffective is not substantiated and is beyond the scope of this audit.

Finally, there were a few areas or conclusions in the body of your report that warrant clarifying comments:

- The Pleasure Boat Report System (PBRS) is used as a mechanism to record the arrival of small boats. Small boat operators can report their arrival: 1) telephonically if they possess a valid Canadian Border Boat Landing Permit, a NEXUS card, or are enrolled in the Local Boater

[1] DHS' Strategy and Plans to Counter Small Vessel Threats Need Improvement (OIG Draft Report, August 2009), pg. 16.

U.S. Department of Homeland Security
Washington, DC 20528

Option program; 2) by physically reporting for inspection to the nearest open port-of-entry or designated reporting sites; or 3) by using an Outlying Area Reporting Station.

- All references to the Treasury Enforcement Communication System (TECS) should be changed to "TECS". The Customs and Border Protection (CBP), Office of Information and Technology received approval from the Deputy Commissioner in September 2008 to change the name of the Treasury Enforcement Communication System (TECS) to simply "TECS," with no definition of the acronym. The TECS name change was needed to remove "Treasury" from the name and to recognize that TECS is not a communication system or network. However, due to its universal recognition, CBP retained the use of the 'TECS' acronym.

With regard to the classification of the draft report, DHS has identified information within the report requiring restricted public access based on a designation of "For Official Use Only."

Thank you for the opportunity to review and comment on your report.

Sincerely,

David Heyman
Assistant Secretary
Office of Policy

Admiral Thad W. Allen.
Commandant
U.S. Coast Guard

Jayson P. Ahern
Commissioner (Acting)
Customs and Border Protection

Based on heightened concerns about terrorism and homeland security, GAO published a set of standards containing six desirable characteristics for an effective national strategy.[8] These desirable characteristics are intended to help shape the policies, programs, priorities, resource allocations, and standards that would enable federal agencies and other stakeholders to implement the strategies and achieve the identified results. The six desirable characteristics contain 40 specific supporting elements that, when properly addressed in a national strategy, provide guidance for developing and implementing the strategy, improve management's abilities to set policy and direct resources, and ensure accountability of all stakeholders at all levels of government.

The six desired characteristics are as follows:
(1) Purpose, scope, and methodology
(2) Problem definition and risk assessment
(3) Goals, subordinate objectives, activities, and performance measures
(4) Resources, investments, and risk management
(5) Organizational roles, responsibilities, and coordination
(6) Integration and implementation

We compared the Small Vessel Security Strategy against each desirable characteristic and its supporting elements. (See Appendix D).

The Strategy could obtain one of three potential scores of "addresses," "partially addresses," or "does not address" for each desirable characteristic.

- The Strategy "addresses" a characteristic when it explicitly cites all the elements of a characteristic, even if it lacks specificity and details and thus could be improved.
- The Strategy "partially addresses" a characteristic when it explicitly cites some, but not all, of the elements of a characteristic. The designation "partially addresses" can entail a wide variation between a strategy that addresses most of the elements of a characteristic and a strategy that addresses few of the elements of a characteristic.
- The Strategy "does not address" a characteristic when it does not explicitly cite or discuss any elements of a characteristic, and/or any implicit references to the characteristics or elements are either too vague or too general.

[8] GAO-04-408T, February 2004.

Appendix C
Desirable Characteristics and Elements of an Effective National Strategy

Desirable Characteristic	Brief Description	Example of Elements
Purpose, scope, and methodology	Addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed.	• Statement of broad or narrow purpose, as appropriate • How it compares and contrasts with other national strategies • Major functions, mission area, or activities it covers • Principles or theories that guided its development • Impetus for strategy (e.g., statutory requirement or event) • Process to produce strategy (e.g., interagency task force; state, local, or private input) • Definition of key terms
Problem definition and risk assessment	Addresses the particular national problems and threats toward which the strategy is directed.	• Discussion or definition of problems, their causes, and operating environments • Risk assessment, including an analysis of threats and vulnerabilities • Quality of data available (e.g., constraints, deficiencies, and "unknowns")
Goals, subordinate objectives, activities, and performance measures	Addresses what the strategy is trying to achieve and steps to achieve those results, as well as the priorities, milestones, and performance measures to gauge results.	• Overall results desired (i.e., "end state") • Hierarchy of strategic goals and subordinate objectives • Specific activities to achieve results • Priorities, milestones, and outcome related performance measures • Specific performance measures • Process for monitoring and reporting on progress • Limitations on progress indicators
Resources, investments, and risk management	Addresses what the strategy will cost, the sources and types of resources and investments needed, and where resources and investments should be targeted by balancing risk reductions and costs.	• Resources and investments associated with the strategy • Types of resources required (e.g., budgetary, human capital, information technology, research and development, contracts) • Sources of resources (e.g., federal, state, local, and private) • Economic principles (e.g., balancing benefits and costs) • Resource allocation mechanisms (e.g., grants, in kind services, loans, or user fees) • "Tools of government" (e.g., mandates or incentives to spur action) • Importance of fiscal discipline • Linkage to other resource documents (e.g., federal budget) • Risk management principles
Organizational roles, responsibilities, and coordination	Addresses who will be implementing the strategy, what their roles will be compared to others, and mechanisms for them to coordinate their efforts.	• Roles and responsibilities of specific federal agencies, departments, or offices • Roles and responsibilities of state, local, private, and international sectors • Lead, support, and partner roles and responsibilities • Accountability and oversight framework • Potential changes to current organizational structure • Specific processes for coordination and collaboration • How conflicts will be resolved
Integration and implementation	Addresses how a national strategy relates to other strategies' goals, objectives, and activities, and to subordinate levels of government and their plans to implement the strategy.	• Integration with other national strategies (horizontal) • Integration with relevant documents from implementing organizations (vertical) • Details on specific federal, state, local, or private strategies and plans • Implementation guidance • Details on subordinate strategies and plans for implementation (e.g., human capital and enterprise architecture)

Source: GAO-04-408T, February 2004.

Appendix D
Small Vessel Security Strategy and Draft Implementation Plan Compared Against Desirable Characteristics and Elements

Desirable Characteristics and Elements	Not Addressed	Partially Addressed	Addressed
Purpose, scope, and methodology–Addressed			
Statement of broad or narrow purpose, as appropriate			X
How it compares and contrasts with other national strategies			X
Major functions, mission areas, or activities it covers			X
Principles or theories that guided its development			X
Impetus for strategy (e.g., statutory requirements or event)			X
Process to produce strategy (e.g., interagency task force; state, local, or private input)			X
Definition of key terms			X
Problem definition and risk assessment–Addressed			
Discussion or definition of problems, their causes, and operation environment			X
Risk assessment, including an analysis of threats and vulnerabilities			X
Quality of data available (e.g., constraints, deficiencies, and "unknowns")			X
Goals, subordinate objectives, activities, and performance measures–Partially Addressed			
Overall results desired (i.e., "end-state")			X
Hierarchy of strategic goals and subordinate objectives			X
Specific activities to achieve results			X
Priorities, milestones, and outcome-related performance measures		X	
Specific performance measures	X		
Process for monitoring and reporting on progress		X	
Limitation on progress indicators		X	
Resources, investments, and risk management–Partially Addressed			
Costs associated with strategy	X		
Human capital associated with strategy	X		
Information technology associated with the strategy			X
Research and development associated with the strategy			X
Sources of resources (e.g., federal, state, local, and private)		X	
Economic principles (e.g., balancing benefits and costs)	X		
Resource allocation mechanisms (e.g., grants, in-kind services, loans or user fees)	X		
"Tools of government" (e.g., mandates or incentives to spur action)			X
Importance of fiscal discipline	X		
Linkage to other resource documents (e.g., federal budget)	X		
Risk management principles			X

Appendix D
Small Vessel Security Strategy and Draft Implementation Plan Compared Against Desirable Characteristics and Elements

Desirable Characteristics and Elements	Not Addressed	Partially Addressed	Addressed
Organizational roles, responsibilities, and coordination–Partially Addressed			
Roles and responsibilities of specific federal agencies, departments, or offices			X
Roles and responsibilities of state, local, private, and international sectors		X	
Lead, support, and partner roles and responsibilities		X	
Accountability and oversight framework	X		
Potential changes to current organizational structure	X		
Specific process for coordination and collaboration		X	
How conflicts will be resolved	X		
Integration and implementation–Partially Addressed			
Integration with other national strategies (horizontal)			X
Integration with relevant documents from implementing organizations (vertical)	X		
Details on specific federal, state, local, or private strategies and plans		X	
Implementation guidance	X		
Details on subordinate strategies and plans for implementation (e.g., human capital and enterprise architecture)	X		
Totals	**13**	**8**	**19**

America's Waterway Watch

U.S. Coast Guard Commandant Instruction 16618.8 established the America's Waterway Watch program on February 10, 2005. The program's purpose is to raise national awareness among those who work, live, or recreate on or near the water of suspicious activity that might indicate threats to our country's homeland security. Individuals can report suspicious and unusual activity via the 24-hour hotline, 1-877-24WATCH (1-877-249-2824). Calls to the hotline are routed through the National Response Center, where they are screened and forwarded to the appropriate authorities in the area where the suspicious activity was reported. The National Response Center is staffed by Coast Guard personnel who monitor the hotline 24 hours a day, 365 days a year.

Citizen's Action Network

Coast Guard District 13 created the Citizen's Action Network program in 1999 to formally engage waterfront citizens, businesses, and organizations in providing a homeland security resource. In the Puget Sound area, the Citizen's Action Network is composed of more than 300 vetted members, including citizen, business, tribal, Canadian, and Coast Guard Auxiliary partners. The Coast Guard actively trains and educates Citizen's Action Network members and recruits many into the ranks of the Coast Guard Auxiliary. Citizen's Action Network members can contact the Coast Guard to report suspicious activity by calling the Coast Guard Auxiliary office, the America's Waterway Watch hotline, or the District 13 office directly. Coast Guard District 13 can contact Citizen's Action Network members through phone calls, pagers, text messages, e-mails, and a web community.

Pleasure Boat Reporting System

CBP administers the Pleasure Boat Reporting System. This program was designed to process the arrival of small vessels to the United States from foreign ports, as required by law.[9] The Pleasure Boat Reporting System program requires small vessel operators to telephone the local office to report the operator's personal identifying information, the vessel name, and the vessel registration number, as well as any passengers' personal identifying information.

[9] 19 U.S.C. 1433, 1434, *Tariff Act of 1930* – Entry; vessels.

CBP officers operating the Pleasure Boat Reporting System program can either clear small vessel operators and their passengers verbally on the telephone or require them to report in person within 24 hours to a Private Vessel Designated Reporting Location for a face-to-face inspection. These reporting locations include official CBP ports of entry, Pleasure Boat Reporting System call-in centers, and certain locations to which CBP officers will travel to meet and process small vessel operators as necessary. Boaters may be asked to report to one of these locations if a CBP officer deems it necessary based on the information provided.

The Tariff Act of 1930 requires that any small vessel operator arriving from a foreign port who fails to report as required be liable for a fine of $5,000 for the first violation and $10,000 for each subsequent violation, and any small vessel used in connection with any such violation to be subject to seizure and forfeiture

Currently, CBP officers operate the Pleasure Boat Reporting System program in 20 field offices, with 128 Private Vessel Designated Reporting Locations throughout the continental United States, Hawaii, and Alaska.

Maritime Information for Safety and Law Enforcement

The Maritime Information for Safety and Law Enforcement system is an internal Coast Guard database used to record all Coast Guard activities. Personnel enter data manually into the system, but information from other law enforcement databases cannot be cross-linked or automatically downloaded into the Coast Guard system. Coast Guard personnel can search records in the Maritime Information for Safety and Law Enforcement system, providing users with vessel details, owner information, and past vessel interdiction records. "Lookout reports" can be added to the records of previously stopped vessels to alert boarding officers with information obtained during past interdictions. These "lookout reports" are added only by Coast Guard personnel and are not shared with any other law enforcement databases.

TECS

TECS is a Department of the Treasury legacy system now managed by CBP Office of Field Operations. It connects thousands of databases and provides controlled access to personally identifiable information that is collected through other government databases.

Appendix F
Major Contributors to This Report

Paul Wood, Director
Yesi Starinsky, Audit Manager
Andrew Smith, Auditor in Charge
Christopher Byerly, Program Analyst
Mathew Noll, Program Analyst
Gwendolyn Priestman, Program Analyst
Marissa Weinshel, Program Analyst
Corneliu Buzesan, Program Analyst
Gary Alvino, Independent Referencer

Department of Homeland Security

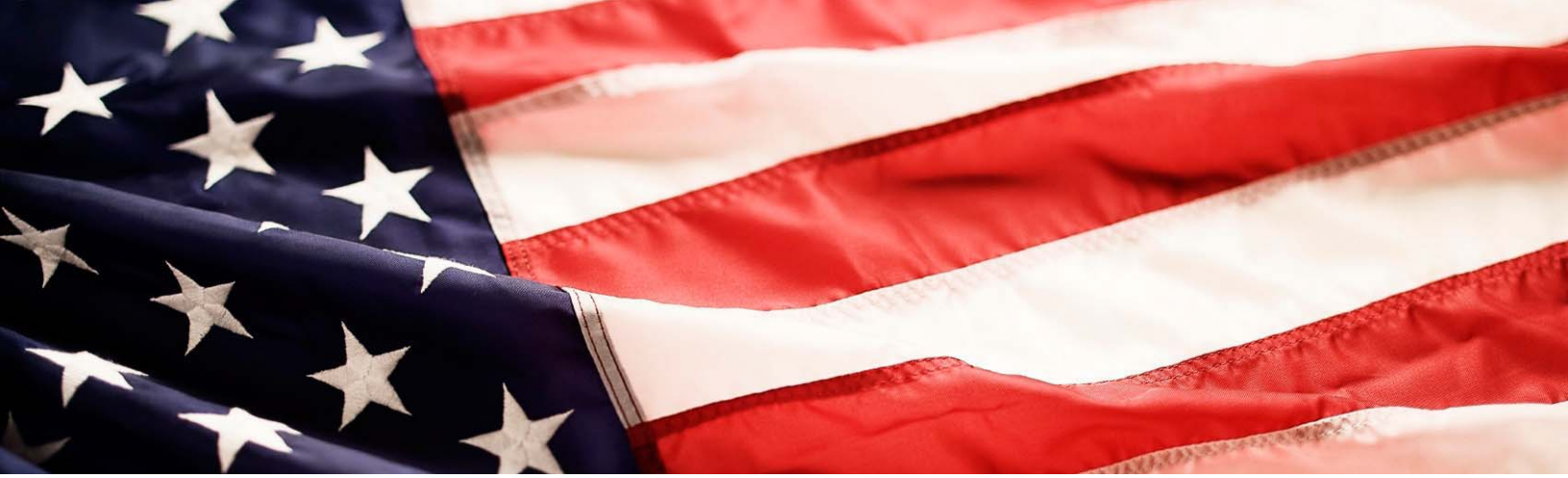
Secretary
Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Acting General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Respective Under Secretary
U.S. Coast Guard Director
CBP Director
U.S. Coast Guard Liaison
CBP Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate



ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

• Call our Hotline at 1-800-323-8603;

• Fax the complaint directly to us at (202) 254-4292;

• Email us at DHSOIGHOTLINE@dhs.gov; or

• Write to us at:
DHS Office of Inspector General/MAIL STOP 2600,
Attention: Office of Investigations - Hotline,
245 Murray Drive, SW, Building 410,
Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.