OFFICE OF INSPECTOR GENERAL

Coast Guard IT Investments Risk Failure Without Required Oversight

Homeland Security

November 14, 2017

OIG-18-15

DHS OIG Highlights

Coast Guard IT Investments Risk Failure Without Required Oversight

November 14, 2017

Why We Did This Audit

In 2015, the Coast Guard ceased development of an IT system to modernize its electronic health records after the procurement experienced cost and schedule overruns. We performed this audit to determine if the Coast Guard has sufficient controls to ensure IT acquisition programs are properly identified to receive the correct level of acquisition oversight.

What We Recommend

We made four recommendations that, when implemented, should strengthen the Coast Guard's identification and designation process for non-major IT acquisition programs.

For Further Information:
Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

Although the United States Coast Guard approved approximately $1.8 billion of information technology (IT) procurements between fiscal years 2014 and 2016, it does not know if almost 400 information systems are receiving proper acquisition oversight. This occurred because the Coast Guard's controls over IT investments lack synergy and create weaknesses that affect its ability to adequately identify, designate, and oversee non-major IT acquisition programs. Specifically:

- acquisition and IT review processes operate independent of each other, creating inefficiencies and weaknesses that can compromise the success of an IT acquisition program;
- there are insufficient controls to ensure that IT investments are reviewed to identify and designate the appropriate level of acquisition oversight;
- lack of reliable or non-existent information hinders efforts to determine what information systems may require additional acquisition oversight; and
- the Coast Guard has not updated its acquisition and IT manuals, which currently provide insufficient guidance.

These control weaknesses affect the Coast Guard's ability to effectively oversee non-major IT programs. Programs that do not receive adequate oversight are at risk of wasting money, missing milestones, and not achieving performance requirements. For instance, the Coast Guard spent approximately $68 million on the Integrated Health Information System in a failed attempt to modernize its electronic health records system.

Coast Guard Comments

The Coast Guard concurred with all four recommendations and described corrective actions it has taken and plans to take. We consider all recommendations resolved and open.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

November 14, 2017

MEMORANDUM FOR: Vice Admiral Sandra L. Stosz
Deputy Commandant for Mission Support
United States Coast Guard

FROM: John E. McCoy II
Acting Assistant Inspector General for Audits

SUBJECT: *Coast Guard IT Investments Risk Failure Without Required Oversight*

Attached for your action is our final report, *Coast Guard IT Investments Risk Failure Without Required Oversight*. We incorporated the formal comments provided by your office.

The report contains four recommendations aimed at improving the Coast Guard's IT investment process. Your office concurred with all four recommendations. Based on information provided in your response to the draft report, we consider all recommendations open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination. Please call me with any questions, or your staff may contact Donald Bumgardner, Deputy Assistant Inspector General for Audits, at (202) 254-4100.

Attachment

Table of Contents

Appendixes

Abbreviations

C4IT	Command, Control, Communications, Computers and Information Technology
DHS	Department of Homeland Security
ECD	estimated completion date
GAO	Government Accountability Office
IT	information technology
ITAR	Information Technology Acquisition Review
OIG	Office of Inspector General
NMAP	Non-Major Acquisition Process
SDLC	System Development Life Cycle

Background

Between fiscal years 2014 and 2016, the Coast Guard approved approximately $1.8 billion of information technology (IT) procurements to help execute its mission of ensuring the Nation's maritime safety, security, and stewardship.[1] These procurements range in scope from major acquisitions to non-major acquisitions and simple procurements. Major acquisition programs receive Department-level oversight and have historically received a greater level of review. In contrast, non-major acquisition oversight is primarily delegated to the component and generally receives less scrutiny than major acquisition programs; yet, these programs also encompass investments that have significant systems integration, high risk, or require high performance parameters. In fact, according to a recent Government Accountability Office (GAO) report,[2] Department of Homeland Security components indicated that managing non-major acquisitions has historically been a lower priority than managing major acquisitions or other component activities.

The Coast Guard recognizes the requirements of the *Clinger Cohen Act of 1996*, enacted by Congress to reform and improve the way Federal agencies acquire and manage IT resources. Thus the Coast Guard's own policies state that Federal agencies are required to be responsible for treating acquisition, planning, and management of technology as "capital investments." Within the Coast Guard, IT systems are a common type of IT investment[3] requiring acquisition oversight and are generally categorized as capital assets. There are three levels of acquisition programs for capital assets. Table 1 provides a breakdown of the tiers based on acquisition life cycle cost estimates.

Table 1. Capital Asset Acquisition Tiers

Dollar Threshold	Acquisition Tier	Acquisition Decision Authority
≥ $1Billion	Major Acquisition (Level 1)	Under Secretary For Management
$300 Million ≤ $1 Billion	Major Acquisition (Level 2)	Under Secretary For Management
$0 ≤ $300 Million	Non-Major Acquisition (Level 3)	Component Acquisition Executive

Source: Office of Inspector General (OIG) analysis of Department of Homeland Security acquisition guidance

[1] U.S. Coast Guard officials provided a listing of information technology procurements they said they approved between FYs 2014 and 2016. We were unable to validate the accuracy of this information and are presenting the information as provided.
[2] *Identifying All Non-Major Acquisitions Would Advance Ongoing Efforts to Improve Management* (GAO-17-396)
[3] Coast Guard policies do not define the term "IT investment." For purposes of this report, the term "IT investment" is used to refer to the cost, outlay, or expenditures of money to obtain and support IT resources that the Coast Guard may or may not have designated as an acquisition program.

Our audit focused on Level 3 non-major IT acquisition investments that may require a higher level of governance to ensure budget, milestones, and program objectives are met.

Information Technology Directorate

The Coast Guard Command, Control, Communications, Computers and Information Technology (C4IT) Directorate, designs, develops, deploys, and maintains IT solutions for the entire Coast Guard. The C4IT Directorate also establishes, monitors, and approves technical standards, tools, and processes. In addition, the directorate certifies acquisition projects in conformance with statute, policy, requirements, architectures, and standards.

The C4IT Directorate uses the System Development Life Cycle (SDLC) to oversee the development of IT systems. SDLC has seven phases listed in appendix C that include the conceptual planning, planning and requirements, and design. The SDLC team must prepare documentation to present to the Phase Exit Review Board to receive approval to move to the next phase in the system's development. According to the SDLC manual, the board comprises the Chief Information Officer, Chief Financial Officer, and representatives from the acquisition directorate, among others. Appendix D provides an excerpt of the Coast Guard's organizational chart, specific to the C4IT and Acquisition Directorates.

The Coast Guard Chief Information Officer manages and administers all IT resources and assets to meet mission and enterprise goals. The Chief Information Officer also approves the acquisition of all IT equipment, software, services, hardware, communications, infrastructure, and programs prior to contract award. Any IT investment larger than or equal to $100,000 is subject to the Information Technology Acquisition Review (ITAR) process, a review and approval process overseen by the IT directorate.

Acquisition Directorate

The Coast Guard's Acquisition Directorate is responsible for efficiently and effectively delivering capabilities needed to execute the full range of Coast Guard missions. This is accomplished by acquiring needed capabilities following a structured acquisition process that is most adequate for the type of acquisition. To that end, the Coast Guard updated its policies in December 2012 to better align with the Department's guidance in Management Directive 102, and began requiring that non-major IT acquisition programs also follow the Non-Major Acquisition Process (NMAP) and receive governance by the Acquisition Directorate.

The NMAP manual's purpose is to define a structured process for the designation, management, and oversight of non-major acquisitions through three phases or decision events — (1) analyze/select; (2) obtain; and (3) produce/deploy and support. The NMAP phases are also listed in appendix C. Phase one begins when the decision authority — the Deputy Commandant for Mission Support — designates the procurement as a non-major acquisition program. If the designation does not occur, the acquisition would not receive Acquisition Directorate governance. Each subsequent phase ensures that the designated acquisition completes specific activities and documentation before receiving approval for the next phase. According to the NMAP manual, C4IT non-major acquisitions are required to follow both NMAP for acquisition oversight and SDLC for systems engineering. Prior to the 2012 NMAP manual, only the C4IT Directorate provided oversight to IT acquisitions using SDLC.

Results of Audit

Although the Coast Guard approved the approximately $1.8 billion of IT procurements between fiscal years 2014 and 2016, it does not know if almost 400 information systems are receiving proper acquisition oversight. This occurred because the Coast Guard's controls lack synergy and create weaknesses that affect its ability to adequately identify, designate, and oversee non-major IT acquisition programs. Specifically:

- acquisition and IT review processes operate independent of each other, creating inefficiencies and weaknesses that can compromise the success of an IT acquisition program;
- there are insufficient controls to ensure that IT investments are reviewed to identify and designate the appropriate acquisition oversight;
- lack of reliable or non-existent information hinders efforts to determine what information systems may require additional acquisition oversight; and
- the Coast Guard has not updated its acquisition and IT manuals, which currently provide insufficient guidance.

In addition to hindering proper identification and designation of non-major IT acquisition programs, these control weaknesses may also affect the Coast Guard's ability to effectively oversee IT acquisition programs. The Coast Guard's management of IT investments risks wasting money, missing milestones, and not achieving performance requirements.

Coordination among the Coast Guard Directorates is Limited

The Coast Guard's current culture creates an environment in which related

acquisition and IT review processes are operating independent of each other and limiting collaboration among directorates. For example, although non-major IT acquisition programs should follow NMAP, SDLC, and ITAR, the SDLC and ITAR processes can also operate independently. When IT investments follow the SDLC and ITAR processes independent of NMAP, the Acquisition Directorate lacks visibility over ongoing non-major IT investments. Additionally, these processes rely on much of the same information for approval; yet, the Coast Guard is not leveraging the information to assist in the identification of potential non-major acquisition programs. The Coast Guard should strengthen its controls by integrating these reviews and increasing the collaboration among the directorates.

SDLC and NMAP

The Acquisition Directorate lacks visibility over ongoing non-major IT investments that are not designated. SDLC and NMAP provide IT systems engineering and acquisition oversight, respectively, to non-major IT acquisition programs. However, a sponsoring office may enter the SDLC process and initiate an IT system without ever presenting the system to the acquisition directorate for review and designation.

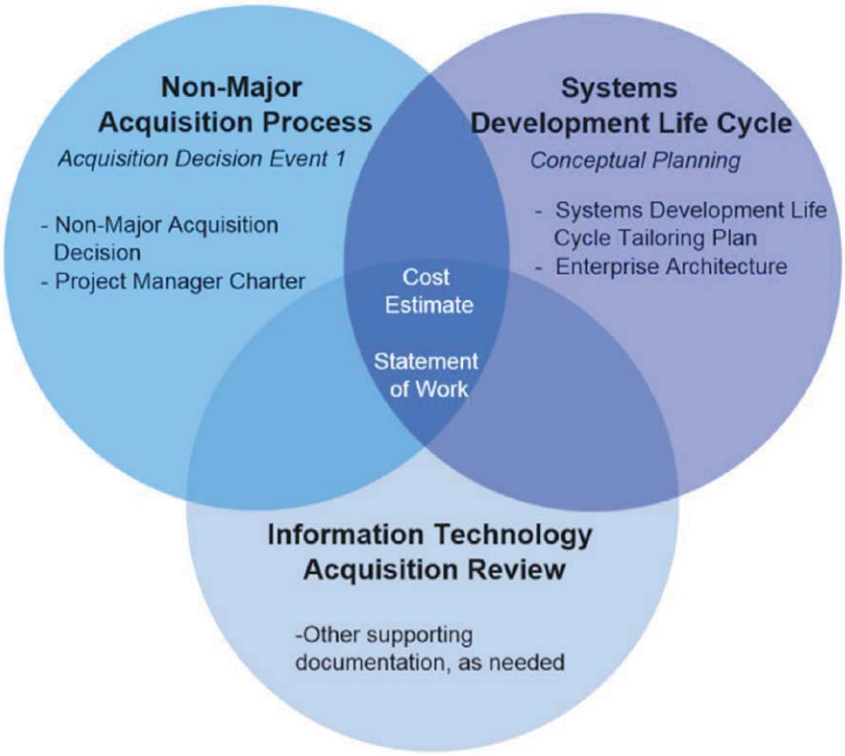
The sponsor is the designated official or program office that has the lead for documenting the capital investment. Because each process operates independently, the Acquisition Directorate could be unaware of ongoing non-major IT investments. Similarly, the SDLC process does not require that sponsoring offices show evidence of compliance with NMAP prior to approving the first and second SDLC Phases. See appendix C for an illustration of the Coast Guard's IT acquisition guidance that includes both SDLC and NMAP. The SDLC process conducts Phase Exit Review Board meetings in which an Acquisition Directorate representative may attend. We obtained either Phase Exit Decision Memos or SDLC Designation Memos for six information systems following the SDLC process and noted that none of the memos were routed to the Acquisition Directorate.

ITAR Process

Within the ITAR process, sponsoring offices are required to submit, among other things, a cost estimate of the total potential value of the IT investment and a statement of work for Chief Information Officer review and approval.

Figure 1 illustrates common information that Coast Guard stakeholders submit for the respective review processes. Although the process requires these documents, they are not reviewed in collaboration with information that may have been submitted during SDLC or NMAP to determine if the estimates align with the acquisition information.

Figure 1. Non-Major Acquisition Program Planning Documentation



Source: OIG analysis of Coast Guard data

Process collaboration is critical because the Chief Information Officer relies on sponsor-provided information to determine whether to approve the acquisition of IT equipment, software, and services prior to contract award. Furthermore, NMAP requires sponsors to provide several acquisition documents —a project manager charter, an acquisition plan, and a requirements memorandum — and follow two phases before the acquisition is ready for a contract award. ITAR only requires sponsors to submit two acquisition-related sources of information — a cost estimate and a description of the work to be performed to receive approval.

Coordination between Acquisition and IT Review Processes

The Coast Guard lacks coordination between the acquisition and IT review process, which risks redundancy in documentation and does not provide a comprehensive layered review process for IT acquisitions. For example, the Coast Guard does not ensure that documents required by all three processes, such as cost estimates and statements of work, are consistent with each other and receive proper review and approval by all stakeholders for their respective subject areas. Having these three processes interface with each other should provide for better controls and reduces the risk of non-major IT acquisitions from being designated incorrectly. If the ITAR process interfaced with the SDLC process, a full acquisition review of an IT investment could be possible.

Preventive Internal Control Procedures are Needed

The Coast Guard lacks sufficient internal controls to prevent a non-major IT acquisition program from being overlooked. The Acquisition Directorate relies heavily on the sponsoring office to identify potential acquisition programs and notify the C4IT Directorate of these investments. However, sponsoring office officials are not subject matter experts in the area of acquisitions. Acquisition and IT processes operate independently; therefore, if a sponsoring office does not identify a potential non-major acquisition program, there are no processes within the Acquisition or C4IT Directorates to ensure that the investment is reviewed to determine appropriate acquisition oversight. Furthermore, the Coast Guard does not require the sponsors to provide documentation of the assessment performed to determine whether an IT Investment is a potential non-major acquisition.

A high ranking Coast Guard IT official said the C4IT Directorate relies on the Acquisition Directorate to identify and designate non-major IT acquisition programs, but NMAP indicates that the IT Assistant Commandant also has a responsibility. According to NMAP, the IT Assistant Commandant should review the DHS Acquisition Planning Forecast System database to identify any planned procurements that appear to be non-major acquisitions. The DHS Acquisition Planning Forecast System is a publicly accessible database that compiles the Department's available projections of contracting opportunities exceeding $150,000. The C4IT Directorate is not completing this analysis.

Reliable IT Investment Information is Essential

The lack of reliable or non-existent IT investment information hinders the Coast Guard efforts to determine if approximately 400 information systems require additional acquisition oversight. According to Coast Guard officials, most of these information systems follow SDLC. Systems that follow SDLC

generally have characteristics of non-major acquisition programs, such as requirements for design, development and testing, implementation, operations and maintenance, and disposition. However, the Coast Guard only designated 2 of the 397 systems as non-major acquisition programs and is not providing governance over any of the remaining systems as required by NMAP. We attempted to identify those systems initiated since 2013 and their respective Life Cycle Cost Estimates; however, the Coast Guard did not have sufficient information available for us to make this determination.

The C4IT Directorate uses a database called the Enterprise System Inventory to maintain information and documentation of information systems; however, the data is incomplete. It is missing information such as start dates, cost estimates, and current SDLC phases. As such, it does not serve as a reliable source of information. Furthermore, for 4 of the 10 information systems we tested, the Coast Guard IT officials could not provide complete documentation to support system development activities. As of March 2017, the Coast Guard issued the *Information System Management Standard Operating Procedures* that requires a reliable documentation repository system for identifying and accounting for information systems across the Coast Guard. Improved record keeping and documentation maintenance is critical to effectively identify and manage IT systems and comply with this procedure.

Acquisition and IT Guidance Must be Clear

The Coast Guard has not updated its acquisition and IT manuals, and the manuals provide insufficient guidance to ensure that non-major IT acquisitions are properly identified and designated. Non-major IT acquisition programs are required to follow both NMAP and SDLC. Yet Coast Guard SDLC guidance dates back to 2011 and has not been updated to align with NMAP's acquisition requirements. We identified the following five key areas in which updates and clarification are needed.

The NMAP Manual Provides Insufficient Guidance

The NMAP manual provides insufficient guidance to sponsoring offices on the pre-decisional steps the sponsoring offices must take to identify potential non-major IT acquisition programs. NMAP defines a non-major acquisition as,

> *… a procurement greater than $10M in procurement costs and less than $300M in life cycle costs, that is not designated as a major system acquisition. This cost assessment is initially based on a documented rough order of magnitude Life Cycle Cost Estimate (LCCE) that includes all estimated costs from inception through disposal.*

The manual also indicates:

> *In addition, procurements under $10M may be designated as a Non-Major Acquisition upon notification from the Sponsor to Commandant [of the Office of Acquisition Support][4] or Commandant [of the Office of Enterprise Architecture and Governance][5]…*

However, the manual does not explain how the sponsoring offices should notify the Commandants of the IT investments, when in the IT investment process, or what information the sponsoring office should include in its notification. The manual also does not sufficiently define who within the specific offices is responsible for the notification, and respective key roles and responsibilities for the C4IT Directorate and other relevant directorates.

Additionally, the manual does not provide sufficient guidance on factors and considerations the sponsoring office should use to determine which IT procurements to present. Furthermore, the C4IT Directorate was unable to provide any documentation demonstrating any instance when a new IT investment had been presented for review.

The NMAP Manual Provides Ambiguous Information on Non-Major IT Acquisition Programs

The manual states that a non-major acquisition would normally have procurement costs above $10 million. However, some potential acquisitions with initial procurement costs below $10 million may still have significant life cycle costs, have high risk, or may result in significant logistics or personnel impact. Department acquisition guidance asks components to consider several factors to determine if the investment is an acquisition program or a simple procurement, but does not establish procurement cost as a limiting factor. DHS officials said that they did not agree with the inclusion of a lower limit procurement cost threshold. This may result in the misconception that procurements with costs below the $10 million threshold should be treated as simple procurements without consideration of other important factors. Those factors include, among others, capabilities that require modification to meet requirements and those that require development. Appendix E includes the complete list of factors in the DHS acquisition decision matrix.

[4] The Office of Acquisition Support is the Coast Guard's designation title for CG-924.
[5] The Office of Enterprise Architecture and Governance is the Coast Guard's designation title for CG-66.

The NMAP Manual Excludes Service Contracts

The fact that the NMAP manual excludes applicability to "service contracts" further complicates identifying and designating non-major IT acquisitions. Many Coast Guard procurements identified as IT investments were for IT services. However, because service contracts are excluded from following NMAP, the Acquisition Directorate would not have reviewed them to determine whether they required additional governance. Coast Guard and DHS officials said that this type of acquisition should adhere to applicable DHS guidance, yet the NMAP manual does not make reference to the departmental requirement.

The NMAP Manual Does Not Address Preexisting IT Investments

Despite the NMAP manual requiring IT acquisitions to follow the revised process, the Acquisition Directorate only discussed how to identify planned procurements that appear to be non-major acquisitions. The NMAP does not discuss how Coast Guard officials should treat IT investments already in progress.

Guidance Updates Are Needed to Enhance Consistency

The C4IT Directorate has not updated its guidance since 2011, so it is not only inconsistent, but it directly conflicts with the acquisition guidance. According to a high ranking Coast Guard IT official, the Acquisition Directorate did not provide the C4IT Directorate instructions on how it should implement the new NMAP requirements. Prior to the 2012 update to the NMAP manual, IT officials were required to follow only SDLC. In the absence of complete instructions, the C4IT Directorate continued to process IT systems following outdated procedures. Historically, sponsors are aware they need to follow the SDLC process for IT investments, said a Coast Guard official. However, the SDLC manual does not direct them to the NMAP manual for acquisition oversight information.

The SDLC manual notes that although non-major acquisitions will follow NMAP, non-major IT acquisitions will only follow SDLC. This is an outdated statement that is contrary to the NMAP manual, but may be contributing to the lack of compliance with current acquisition policy. In addition, one sponsoring office official and one IT asset manager also said that they follow the SDLC process and were unaware as to whether IT investments were required to follow the NMAP process.

There is an additional example of guidance issued prior to the December 2012 NMAP update. According to the *Coast Guard Handbook of Acquisition Logistics*

and Templates, all IT acquisitions not following the *Major Systems Acquisition Manual* should follow the SDLC policy, and that NMAP excludes IT acquisitions.

Coast Guard Took Corrective Actions During Audit

Coast Guard officials recognize that challenges exist in identifying and designating IT investments as non-major acquisition programs. As such, in January 2017, it established the Non-Major Acquisition Oversight Council to begin screening acquisition program candidates and provide recommendations for designation. In addition, GAO found that identification of non-major acquisition programs was a concern across DHS components.[6] As of March 2017, the Department requires that components develop a repeatable methodology to identify non-major acquisition programs and that these programs are identified by October 31, 2017. Implementation of these changes will improve DHS's visibility over all non-major acquisition programs and address the GAO recommendation.

These changes are positive initial steps the Coast Guard needs to take to correct its control weaknesses and ensure it properly identifies IT investments. However, the Coast Guard must take additional steps to change the Coast Guard's culture and improve collaboration among directorates for lasting success.

Integrated Health Information System

Programs that do not receive adequate oversight are at risk of wasting money, missing milestones, and not achieving performance requirements, such as the Integrated Health Information System.

In 2010, the Coast Guard bought a commercial off-the-shelf system for less than $10 million to replace its existing electronic health records system. Coast Guard officials decided to expand the system and in FY 2011, began reengineering the project to integrate other

***Source*:** OIG analysis of Coast Guard contracts

[6] GAO-17-396

functions, such as safety and work-life modules for Coast Guard personnel, retirees, and their dependents. The reengineered system, known as the Integrated Health Information System, was estimated to cost approximately $30.5 million. Despite the initial cost estimates, significant impact on personnel, and significant systems integration, the reengineered system was not designated as a non-major IT acquisition program. Designated acquisition programs receive a higher level of acquisition governance, as denoted in table 1.

After experiencing cost and schedule overruns and spending almost $68 million for the design of this system, in 2015, the Coast Guard cancelled the effort. As a result, the Coast Guard had to return to a paper-based system.

Conclusion

The Coast Guard does not know if all IT investments within its $1.8 billion in approved procurements are receiving proper acquisition oversight since it has not been able to identify all non-major IT acquisition programs from its pool of nearly 400 information systems. To prevent system failures, such as the Integrated Health Information System, the Coast Guard must strengthen its controls for identifying and designating non-major IT acquisition programs. This includes correcting weaknesses in its guidance, improving coordination between directorates, and implementing preventive controls.

Recommendations

Recommendation 1: We recommend the Deputy Commandant Mission Support conduct a comprehensive analysis of related acquisition and information technology review processes to identify redundancies, gaps, and potential improvements; and make improvements accordingly.

Recommendation 2: We recommend the Deputy Commandant Mission Support evaluate all existing information technology investments to (1) identify and designate non-major information technology acquisitions programs, and (2) implement a verifiable process to identify non-major information technology acquisition programs. At a minimum, the process should:

a. state the frequency of the review;
b. identify the criteria used to identify procurements for review; and
c. denote the type of documentation that should be maintained.

Recommendation 3: We recommend the Deputy Commandant Mission Support ensure that the Command, Control, Communications, Computers and

Information Technology Directorate develop and maintain an up-to-date system for managing and tracking information technology investments.

Recommendation 4: We recommend the Deputy Commandant Mission Support review acquisition and information technology guidance to ensure it establishes a clear process to identify and designate non-major information technology acquisition programs. At a minimum, all guidance should:

a. identify stakeholders and define respective roles and responsibilities;
b. include clear factors and considerations that sponsors should use to identify potential non-major information technology acquisitions;
c. establish documentation and review requirements of sponsor assessments; and
d. be consistent with current Department and Coast Guard acquisition and information technology requirements.

USCG Comments and OIG Analysis

In its response to our draft report, the Coast Guard concurred with all four of our report recommendations. We incorporated the Coast Guard's comments, responses to our recommendations, and our analysis with the applicable recommendations in the report. We also included a copy of the management comments in their entirety in appendix B.

U.S. Coast Guard Comments: Coast Guard officials reported that their respective program offices have developed or will develop corrective measures to alleviate the OIG audit team's concerns. These offices are working toward implementing the recommendations and estimate completion by September 30, 2018.

Coast Guard Response to Recommendation 1: Concur. Coast Guard staffs are reviewing the related acquisition and IT processes to identify gaps and overlaps, and recommend improvements to implement. Specifically, the Coast Guard established a Command, Control, Computers, Communications, Cyber and Intelligence (C5I) Program Management Office (PMO) to overhaul the way the Coast Guard acquires and manages information technology. The C5I PMO's overhaul includes transitioning processes from the Coast Guard's System Development Life Cycle management for IT to the DHS System Engineering Life Cycle management for acquisitions, as well as aligning IT with acquisition and sustainment activities. The estimated completion date (ECD) is: September 30, 2018.

OIG Analysis: The Coast Guard's corrective action is responsive to the recommendation. The recommendation will remain open and resolved until the department provides evidence to support that corrective actions are completed.

Coast Guard Response to Recommendation 2: Concur. The Coast Guard acknowledges that its processes for acquisition management and information technology have developed in parallel to each other without consistently intersecting. The Coast Guard recognizes the need to revisit its impacted programs as recommended. Accordingly, the Coast Guard will revise its acquisition processes, methodology, and guidance to account for requisite programs below $300 million in life cycle cost. The ECD is: September 30, 2018.

OIG Analysis: The Coast Guard's corrective action is responsive to the recommendation. The recommendation will remain open and resolved until the department provides evidence to support that corrective actions are completed.

Coast Guard Response to Recommendation 3: Concur. The Coast Guard is refining its Capital Planning and Investment Control process, management, and oversight, in accordance with Department directives; to further align portfolio management of systems, IT investments, acquisition management and operational assessments. ECD is: September 30, 2018.

OIG Analysis: The Coast Guard's corrective action is responsive to the recommendation. The recommendation will remain open and resolved until the department provides evidence to support that corrective actions are completed.

Coast Guard Response to Recommendation 4: Concur. As noted in the Coast Guard response to Recommendation #2, the Coast Guard acknowledges its parallel processes with uncoordinated non-major thresholds existing between IT and acquisition management, which contributed to disparate documentation and oversight. The Coast Guard commits to establish a clear process to identify non-major IT for nominating to non-major acquisition designation. To that end, the Coast Guard is revising its acquisition methodology and guidance to ensure improved oversight and accountability of its IT investments. The estimated release of the updated guidance is: September 30, 2018.

OIG Analysis: The Coast Guard's corrective action is responsive to the recommendation. The recommendation will remain open and resolved until the department provides evidence to support that corrective actions are completed.

Appendix A
Objective, Scope, and Methodology

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*.

The United States Coast Guard spent almost $68 million in a failed attempt to modernize its electronic health records system. To determine if this occurrence was unique or due to systemic weaknesses, we held interviews with Coast Guard program and investigative officials and reviewed related program, oversight, investigative, and corrective action documentation. As a result, we decided to conduct an audit of the Coast Guard's controls related to IT acquisitions.

Our audit objective was to determine whether the Coast Guard has sufficient controls to adequately identify IT acquisition programs. The scope of our review was October 2013 to September 2016. To answer the objective, we:

- obtained and reviewed pertinent Federal laws and regulations, departmental and component regulations, policies, procedures, and guidance relevant to the Coast Guard's acquisitions and IT Investments;
- reviewed and analyzed GAO and DHS OIG prior audit reports related to acquisitions and IT investments; and
- interviewed Coast Guard officials responsible for the management, oversight, and execution of non-major IT acquisitions, procurements, and contracts.

To assess the effectiveness of Coast Guard's internal controls we reviewed applicable steps within NMAP, SDLC, and ITAR as they relate to the identification of non-major IT acquisitions.

We identified information systems that follow SDLC recorded in the Coast Guard's Enterprise Systems Inventory. The database had 397 recorded information systems as of March 2017. We attempted to identify systems initiated between FYs 2014 and 2016, but the database did not have sufficient information to make that determination. We selected a sample of 10 information systems and requested supporting documentation to verify if they were following SDLC. We also reviewed one of these systems to determine whether it had the characteristics of an acquisition program. The Coast Guard could not provide supporting documentation for all the sampled items. In addition, we tested the reliability of the data, and because it was incomplete, we determined the Enterprise System Inventory is unreliable. Because essential

information was unavailable, we were precluded from completing all planned tests as they relate to SDLC compliance and acquisition program identification.

To gain an understanding of the ITAR process, we reviewed a sample of ITARs. The Coast Guard provided a listing of ITAR packages approved between FYs 2014 and 2016. The listing contained 1,006 ITARs totaling approximately $1.8 billion of IT procurements. We reviewed 66 randomly selected ITAR packages for completeness, compliance, and relevant information to aid in the identification of non-major IT acquisitions.

To determine ITAR policy compliance, we reviewed a sample of randomly selected contract files. We identified 6,260 IT-related contracts and modifications that Coast Guard executed between FYs 2014 and 2016 in the Federal Procurement Database System-Next Generation. We tested 30 contract files. All contract files tested included an approved ITAR and we noted no exceptions.

To verify C4IT Directorate's compliance with the NMAP manual, we requested documentation supporting review of the DHS Acquisition Planning Forecast System database. The NMAP manual requires the C4IT Directorate to perform bi-annual reviews of the planned procurements to identify potential non-major IT acquisition programs.

We conducted site visits in Coast Guard Headquarters, Washington, DC; DHS Headquarters, Washington, DC; and Coast Guard C4IT, Alexandria, VA.

We conducted interviews with the following departmental and Coast Guard entities:

- Assistant Commandant for Command, Control, Communications, Computers & IT
- Assistant Commandant for Acquisition
- Assistant Commandant for Resources
- Assistant Commandant for Capability
- Coast Guard Investigative Service
- Department of Homeland Security Office of Program Accountability and Risk Management

We conducted this performance audit between June 2016 and June 2017, pursuant to the *Inspector General Act of 1978,* as amended, and according to 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 upon our

audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

Appendix B
Coast Guard Comments to the Draft Report

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

Commander
United States Coast Guard

2703 Martin Luther King, Jr. Ave SE
Washington, DC 20593-7000
Staff Symbol: CG-8
Phone: (202) 372-3533
Fax: (202) 372-4960

7500
OCT 1 2 2017

MEMORANDUM

From: A. J. Tiongson RDML
COMDT (CG-8)

Reply to Attn of: Audit Manager
Mark Kulwicki
(202) 372-3535

To: John V. Kelly
Deputy Inspector General

Subj: DHS OIG REPORT: "COAST GUARD IT INVESTMENTS RISK FAILURE WITHOUT REQUIRED OVERSIGHT"

Ref: (a) OIG Project No. OIG-16-074-AUD-USCG, of September 2017

1. This memorandum transmits the Coast Guard's response to the draft report identified in reference (a).

2. The Coast Guard concurs with all of the recommendations listed in the draft report. Our response in enclosure (1) demonstrates that the Coast Guard respective program offices have developed or will develop corrective measures to alleviate the audit team's concerns.

3. If you have any questions, my point of contact is Mr. Mark Kulwicki who can be reached at 202-372-3533.

#

Enclosure: (1) USCG Response to OIG Draft Report on IT Investments

COAST GUARD IT INVESTMENTS RISK FAILURE WITHOUT REQUIRED OVERSIGHT
OIG Project No. OIG-16-074-AUD-USCG

Recommendation #1: We recommend the Deputy Commandant Mission Support conduct a comprehensive analysis of related acquisition and information technology review processes to identify redundancies, gaps, and potential improvements; and make improvements accordingly.

Response: Concur. Coast Guard staffs are reviewing the related acquisition and IT (information technology) processes to identify gaps and overlaps, and recommend improvements to implement. With that, the Coast Guard established a Command, Control, Computers, Communications, Cyber and Intelligence (C5I) Program Management Office (PMO) to overhaul the way the Coast Guard acquires and manages information technology. The C5I PMO's overhaul includes transitioning processes from the Coast Guard's System Development Life Cycle management for IT to DHS System Engineering Life Cycle management for acquisitions, as well as aligning IT with acquisition and sustainment activities.

The C5I PMO implementation team works closely with the Assistant Commandant for Command, Control, Communications, Computers & Information Technology (CG-6) and Assistant Commandant for Acquisition (CG-9) staffs to fully review the related processes to identify gaps and overlaps, and implement improvements. The estimated completion date (ECD) is: September 30, 2018.

Recommendation #2: We recommend the Deputy Commandant Mission Support evaluate all existing information technology investments to (1) identify and designate non-major information technology acquisitions programs and (2) implement a verifiable process to identify non-major information technology acquisition programs. At a minimum, the process should:

a. state the frequency of the review;
b. identify the criteria used to identify procurements for review; and
c. denote the type of documentation that should be maintained.

Response: Concur. The Coast Guard acknowledges that its processes for acquisition management and information technology have developed in parallel to each other without consistently intersecting. The Coast Guard recognizes the need to revisit its impacted programs as recommended. Accordingly, the Coast Guard will be revising its acquisition processes, methodology and guidance to account for requisite programs below $300M LCC (life cycle cost).

The C5I PMO will ensure that individual PMs comply with acquisition governance to validate procurements against the approved program and project management plans. The ECD is: September 30, 2018.

Recommendation #3: We recommend the Deputy Commandant Mission Support ensure that the Command, Control, Communications, Computers and Information Technology Directorate develop and maintain an up-to-date system for managing and tracking information technology investments

Response: Concur. The Coast Guard is refining its Capital Planning and Investment Control (CPIC) process, management and oversight, in accordance with Department directives, to further align portfolio management of systems, IT investments, acquisition management and operational assessments. ECD is: September 30, 2018

Enclosure (1)

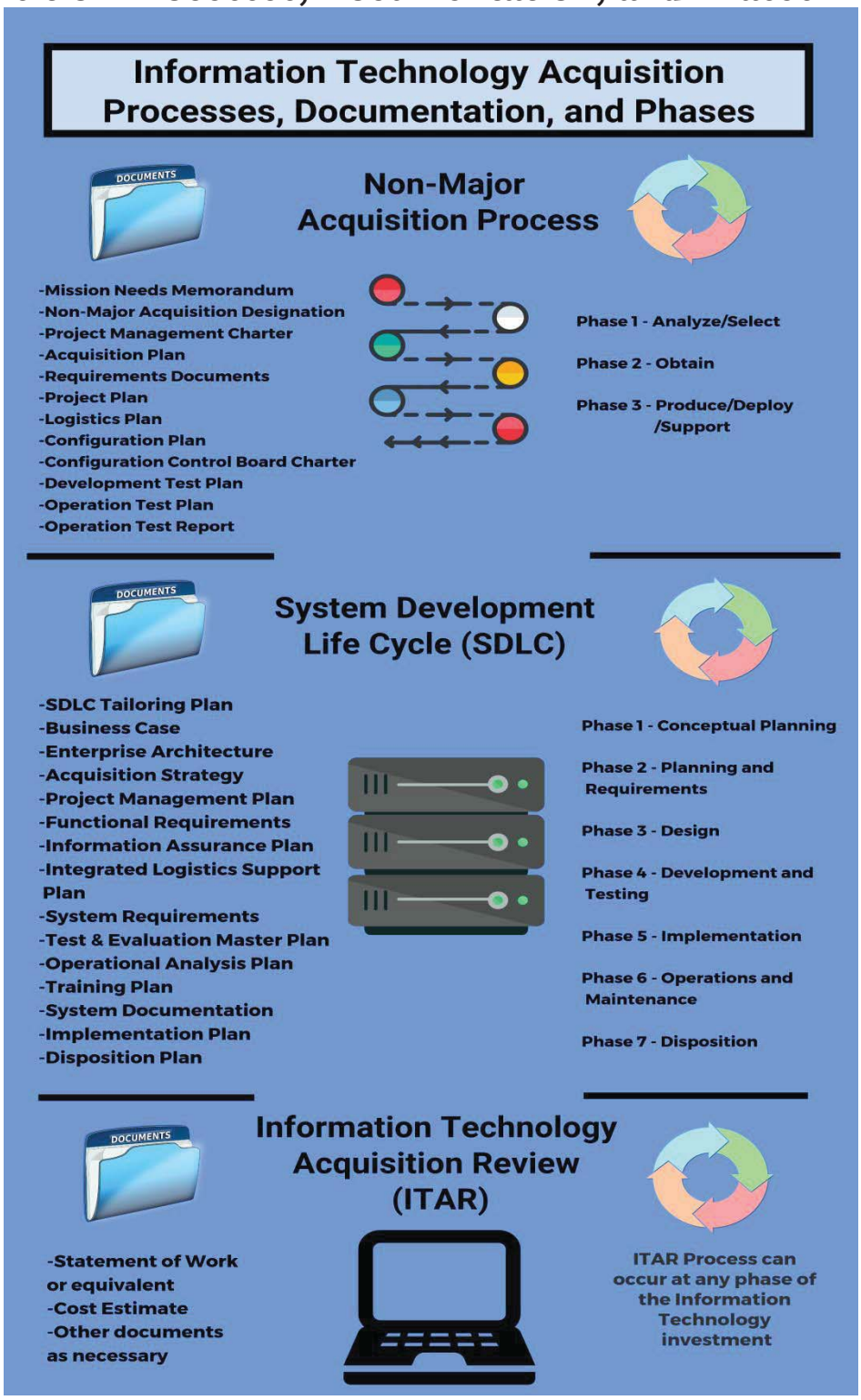
Recommendation #4: We recommend the Deputy Commandant Mission Support review acquisition and information technology guidance to ensure it establishes a clear process to identify and designate non-major information technology acquisition programs. At a minimum, all guidance should:

a. identify stakeholders and defines respective roles and responsibilities;
b. include clear factors and considerations that sponsors should use to identify potential non-major information technology acquisitions;
c. establish documentation and review requirements of sponsor assessments; and
d. be consistent with current Department and Coast Guard acquisition and information technology requirements

Response: Concur. As noted in the Coast Guard response to Recommendation #2, the Coast Guard acknowledges its parallel processes with uncoordinated non-major thresholds existing between IT and acquisition management, which contributed to disparate documentation and oversight. The Coast Guard commits to establish a clear process to identify non-major IT for nominating to non-major acquisition designation. To that end, the Coast Guard is revising its acquisition methodology and guidance to ensure improved oversight and accountability of its IT investments. The estimated release of the updated guidance is: September 30, 2018.

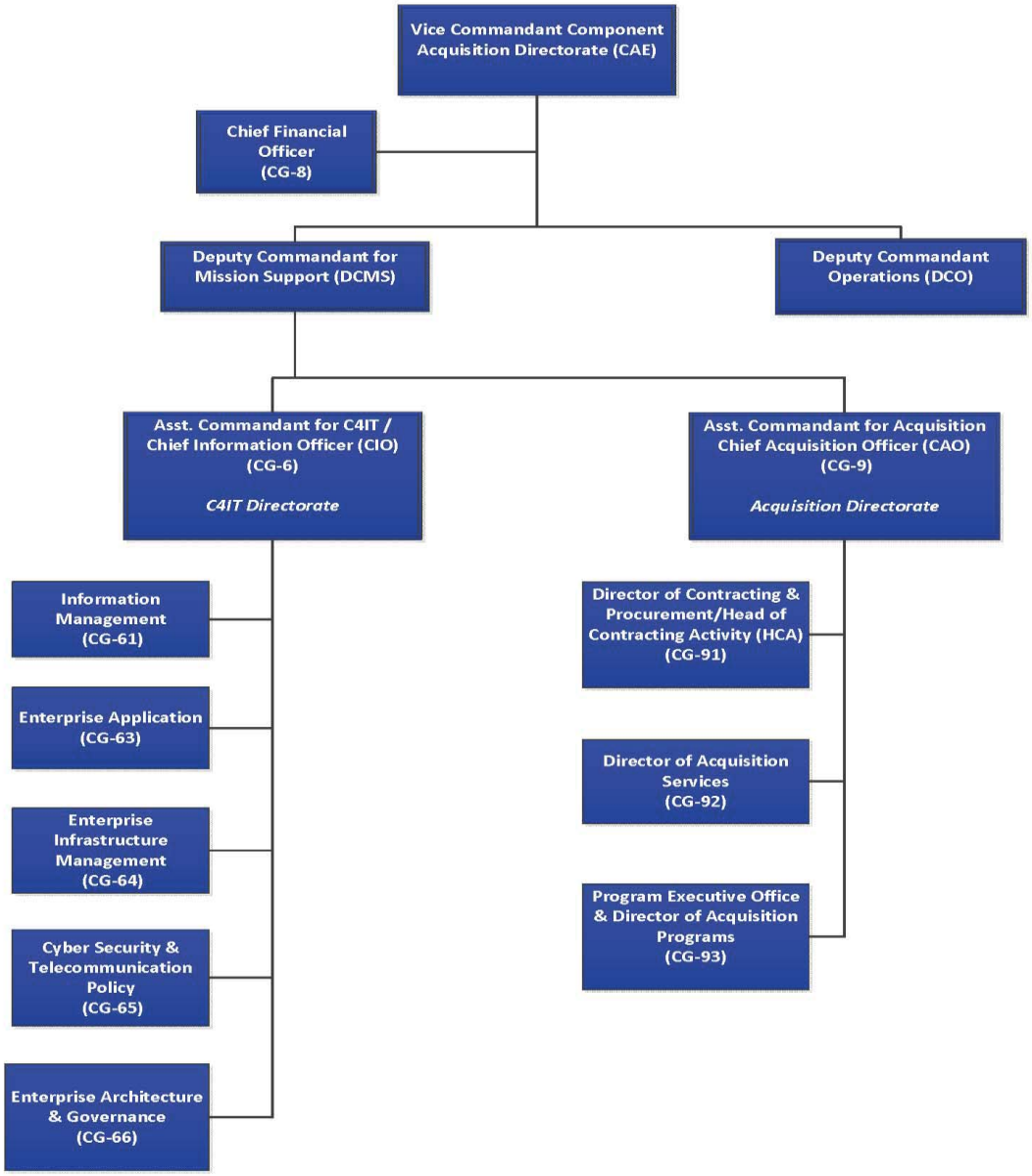
Enclosure (1)

Appendix C
IT Acquisition Processes, Documentation, and Phases



Source: OIG analysis of Coast Guard acquisition and information technology guidance

Appendix D
Excerpt of Coast Guard Organizational Chart



Source: OIG analysis of Coast Guard data

Appendix E
Acquisition Decision Matrix

Simple Procurement, Services Acquisition, or Capital Asset Acquisition				
		Simple Procurement	Services Acquisition	Capital Asset Acquisition
1	The items obtained do not require modification, integration, or development.	Y/N		
2	The items obtained are only to replenish existing or expended supplies.	Y/N		
3	Contract establishes a blanket purchase agreement for goods or services, but does not execute against the contract.	Y/N		
4	The items obtained do not provide new capabilities.	Y/N		
5	The services obtained provide human resources only to perform work (i.e. landscaping and cleaning services)	Y/N		
6	Services are obtained through contract to provide mission capabilities.		Y/N	
7	Services are obtained through contract that requires lifecycle support not inherent in the contract.		Y/N	
8	Services are obtained through interagency agreement or intergovernmental service agreement to provide mission capabilities.		Y/N	
9	The services obtained are part of a larger acquisition program. (**Note:** The service is included in larger acquisition, not established as a separate service program.			Y/N
10	Specific mission requirements or capabilities (i.e. key performance parameters) must be met through operational testing to be considered successful.			Y/N
11	The items/capabilities obtained require modification to meet mission requirements.			Y/N
12	The items/capabilities obtained require integration with existing or new systems to meet mission requirements.			Y/N
13	The items/capabilities obtained require development to meet mission requirements.			Y/N
14	The Items/capabilities obtained require lifecycle support that is not inherent in a contract.			Y/N
	Total Count of Yes answers:	**Total**	**Total**	**Total**
1. If Simple Procurement Count = 1 or more and Services Acquisition and Capital Asset Acquisition = 0, then the activity is a Simple Procurement 2. If Services Acquisition = 1 or more and Capital Asset Acquisition = 0, then the activity is a Services Acquisition (regardless of the count for Simple Procurement) 3. If Capital Asset = 1 or more, then the activity is a Capital Asset Acquisition, regardless of the count for Simple Procurement or Simple Acquisition				
Note: Once an activity is determined to be an acquisition, further analysis is required to determine how the acquisition is structured and executed.				

Source: Excerpt from *DHS Acquisition Management Instruction 102-01-001*

Appendix F
Useful Terms and Definitions

Acquisition: the conceptualization, initiation, design, development, test, production, deployment, logistics support, modification, and disposal of an asset or system.

Capital Investment: refers to the planning, development, and acquisition of a capital asset; and the management and operation of that asset through its usable life after the initial acquisition.

Executive Oversight Council: a Flag/SES level forum that monitors major risks, addresses emergent issues, and provides direction to cross-directorate teams as require to support successful execution of major acquisition projects; and reviews planned procurements, and follows specific guidelines and processes as specified in the NMAP for the non-major acquisition selection process in identifying procurements to recommend for designation as non-major acquisitions.

Information System: the set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information/data. Information systems may include general support systems, major applications, minor applications, and external information systems.

Information Technology (IT): any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Information Technology Acquisition Review (ITAR): a review and approval process that is required to the award of any IT procurement.

Life Cycle Cost Estimate: provides an exhaustive and structured accounting of all resources and associated cost elements required to develop, produce, deploy, and sustain a particular program.

Major Acquisitions Program: an acquisition program with life cycle cost estimates of $300 million or more. These are categorized into either Level 1 acquisitions, if greater than $1 billion, or Level 2 acquisitions programs that are greater than $300 million and less than or equal to $1 billion.

Non-Major Acquisition Process (NMAP): a structured disciplined process for the designation, management, and oversight of non-major acquisitions.

Non-Major Acquisition Program: an investment less than $300 million in estimated life cycle costs, which is not designated as a major system acquisition and is of relatively high visibility, high risk, complex, essential to mission execution, or requires significant integration. These investments warrant a disciplined project management process to include oversight through formal milestone reviews.

Sponsor: the designated official or program office that has the lead for documenting the business case, translating functional requirements into capabilities, and accepting the capability.

System Development Life Cycle (SDLC): a comprehensive life cycle management framework that applies to all C4&IT systems. The SDLC Practice provides a consistent framework for C4&IT project management, including definition of the phases and the decision points for review by leadership to evaluate risks.

Appendix G
Office of Audit Major Contributors to This Report

Yesi Starinsky, Director
Christine Haynes, Director
Armando Lastra, Lead Auditor
Patricia Benson, Program Analyst
Douglas Campbell, Program Analyst
Ardeth Savery, Auditor
Oluwabusayo Sobowale, Auditor
Danny Urquijo, Program Analyst
Kevin Dolloson, Communications Analyst
Matt Noll, Independent Referencer

Appendix H
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Executive Secretary
Commandant of the U.S. Coast Guard
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
USCG Audit Liaison
DHS Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305