

**GAO**

Report to the Subcommittee on Coast  
Guard and Maritime Transportation,  
Committee on Transportation and  
Infrastructure, House of Representatives

---

December 2000

**INFORMATION  
TECHNOLOGY  
MANAGEMENT**

**Coast Guard Practices  
Can Be Improved**



**G A O**

Accountability \* Integrity \* Reliability

---





**United States General Accounting Office**  
**Washington, D.C. 20548**

December 12, 2000

The Honorable Wayne T. Gilchrest  
Chairman  
The Honorable Peter A. DeFazio  
Ranking Democratic Member  
Subcommittee on Coast Guard and Maritime Transportation  
Committee on Transportation and Infrastructure  
House of Representatives

As the U. S. Coast Guard (USCG) strives to achieve its information technology (IT) management vision to “deliver the right information to the right people at the right time to support all USCG missions,” it needs to identify and address operational problems that have agencywide implications. Evaluating USCG’s IT management is a critical part of efforts to assess whether it has a sound foundation for addressing these problems. As you requested, our objective was to evaluate USCG’s IT policies, procedures, and practices in the areas of investment management, architecture, software acquisition and development, information security, and human capital. These five key areas encompass major IT functions and are recognized by the IT industry as having substantial influence over the effectiveness of an organization’s operations.

To fulfill this objective, we reviewed USCG’s policies and procedures in each of the five key IT areas and compared them to applicable laws, regulations, federal guidelines, and industry standards. We also reviewed selected IT projects and activities to determine if USCG’s practices complied with its policies and procedures as well as federal and industry standards. We performed our work from March through August 2000, in accordance with generally accepted government auditing standards. Department of Transportation (DOT) and USCG officials provided us with comments on a draft of this report; they are discussed in the “Agency Comments” section.

On September 8, 2000, we provided a detailed briefing to your office on the results of this work. The briefing slides are included in appendix I. The purpose of this letter is to provide the published briefing slides to you and to officially transmit our recommendations to the Secretary of Transportation.

In brief, we reported that while USCG had many important IT management policies and procedures in place, it did not always implement them

---

consistently. That is, USCG's practices were not always in compliance with its policies. We noted weaknesses in each of the key areas of IT management and made specific recommendations to address these weaknesses. The recommendations we are making to the Secretary of Transportation follow.

---

## Recommendations

To improve USCG's IT management practices, we recommend that the Secretary of Transportation direct the USCG Commandant to ensure that the appropriate officials complete the following actions.

In the investment management area,

- develop written procedures to guide IT Investment Board operations;
- establish an IT oversight process that compares actual cost and schedule data with original estimates for all projects to determine whether investments are proceeding as expected and to take corrective actions as appropriate;
- establish a comprehensive inventory of IT assets that includes up-to-date cost and schedule information;
- establish a process for analyzing, validating, and prioritizing the costs, benefits, schedules, and risks associated with all IT investments; and
- develop and oversee a comprehensive IT investment portfolio.

In the IT architecture area,

- ensure that all system investments are compliant with the IT architecture and
- ensure that legacy systems integration processes are effectively implemented across the agency.

In the area of software acquisition and development,

- initiate software acquisition process improvement efforts to address weaknesses in requirements development and management, and acquisition risk management and
- initiate software development process improvement efforts to address weaknesses in project planning, project tracking and oversight, quality assurance, and configuration management.

In the information security area,

- 
- implement a complete, effective security awareness program;
  - ensure that systems' risk assessments and accreditations are completed;
  - implement appropriate corrective actions on vulnerabilities identified during facilities' physical security evaluations;
  - implement appropriate corrective actions on the network security weaknesses we identified; and
  - develop and implement a centralized mechanism to monitor and enforce compliance with physical security and information systems security policies.

In the human capital management area,

- assess the IT civilian workforce to identify knowledge and skill requirements and any gaps;
- maintain a complete inventory that includes specific IT knowledge and skills; and
- analyze and document the effectiveness of strategies for recruiting, training, and developing IT personnel, and use the results to continually improve human capital strategies.

---

## Agency Comments


We obtained oral comments on drafts of our briefing and this report from DOT and USCG officials, including representatives of the Office of the Secretary of Transportation, and the USCG Office of Quality Management. These officials generally agreed with our recommendations and stated that they are working to implement them.

We are sending copies of this report to the Honorable Rodney E. Slater, Secretary of Transportation; Admiral James M. Loy, USCG Commandant; the Honorable Jacob J. Lew, Director, Office of Management and Budget; and other interested parties. Copies will also be made available to others upon request.

Should you or your staffs have any questions concerning this report, please contact me at (202) 512-6408 or Linda Koontz, Director, Information Management Issues, at (202) 512-6240. We can also be reached by e-mail at

---

*willemsenj@gao.gov* and *koontzl@gao.gov*, respectively. Major contributors to this report are identified in appendix II.

A handwritten signature in black ink that reads "Joel Willemsen". The signature is written in a cursive style with a large, looping initial "J".

Joel C. Willemsen  
Managing Director, Information Technology Issues

---

---

# GAO's September 8, 2000, Briefing



## United States Coast Guard's Management of Information Technology

Briefing for the Subcommittee on Coast Guard  
and Maritime Transportation, Committee on Transportation  
and Infrastructure, House of Representatives

September 8, 2000





## Purpose and Outline

### Briefing purpose:

- To present the results of our review and analysis of the United States Coast Guard's (USCG) management of information technology (IT)

### Briefing outline:

### Slide:

- |   |    |
|---|----|
| • Objective                                     | 3  |
| • Scope and Methodology                         | 4  |
| • USCG's IT Profile                             | 5  |
| • USCG's IT Policies, Procedures, and Practices | 12 |
| • Investment Management                         | 16 |
| • Architecture                                  | 29 |
| • Software Acquisition and Development          | 37 |
| • Information Security                          | 50 |
| • Human Capital                                 | 58 |



## Objective

To evaluate USCG's information technology policies, procedures, and practices in the areas of investment management, architecture, software acquisition and development, information security, and human capital



## Scope and Methodology

- We reviewed USCG's IT policies and procedures for investment management, architecture, software acquisition and development, information security, and human capital and compared them with applicable laws and regulations, federal guidelines, and industry standards.
- We reviewed selected IT projects and activities to determine if practices complied with the agency's policies and procedures and industry standards, and sought work products documenting these practices, where applicable. The selected projects represent a mix of ongoing and completed IT projects of various costs and durations. We also reviewed activities related to current investments.
- We conducted the review at USCG headquarters in Washington, D.C.; at the Operations Systems Center in Martinsburg, West Virginia; and at the Telecommunications and Information Systems Command in Alexandria, Virginia. We conducted our work from March through August 2000, in accordance with generally accepted government auditing standards.
- We obtained comments from USCG on a draft of this briefing.



## IT Profile

### USCG Missions and Budget

---

USCG is a multi-mission agency and military service dedicated to ensuring America's maritime safety and security. Key mission areas:

- Maritime safety--eliminating deaths, injuries, and property damage associated with maritime transportation, fishing, and recreational boating
- Maritime security--protecting U.S. borders by halting the flow of illegal drugs, migrants, and other contraband through maritime routes; preventing illegal fishing; and enforcing federal law at sea
- Protection of natural resources--eliminating environmental damage and natural resource degradation associated with maritime transportation, fishing, and recreational boating
- Maritime mobility--facilitating maritime commerce and eliminating impediments to the movement of goods and people
- National defense--enhancing regional stability in support of the national security strategy



**IT Profile**  
**IT Environment**

In August 2000, USCG estimated that it would spend about \$197 million on 81 IT initiatives in FY 2000

- **54 operational systems and projects**, totaling about \$117.4 million (60 percent of the IT budget)
  
- **27 system acquisition or development projects**, totaling about \$79.9 million (40 percent of the IT budget)
  - USCG closely tracks four of these, which are considered “major IT acquisitions” because their total acquisition or development costs exceed \$50 million
  
  - The four major IT acquisitions represent about 25 percent of the FY 2000 IT budget



**IT Profile**  
**IT Environment (continued)**

Estimated costs for major IT acquisitions as of August 2000  
(dollars in millions)

	Estimated FY 2000 Budget	Estimated Total Life Cycle Costs
<b>MAJOR IT ACQUISITIONS</b>		
National Distress and Response System	\$22.0	\$717.1
Ports and Waterways Safety System	\$9.7	\$125.4
Marine Information for Safety and Law Enforcement	\$12.5	\$118.7
Fleet Logistics System	\$5.5	\$57.5
<b>TOTAL</b>	<b>\$49.7</b>	<b>\$1,018.7</b>



## IT Profile

### IT Environment (continued)

---

Specific USCG systems initiatives presenting particular challenges:

- **Marine Information for Safety and Law Enforcement (MISLE)**
    - Initiated in the mid-1980s to replace the aging Marine Safety Information System, USCG awarded a development contract in 1995
    - In 1999, after spending about \$35 million, USCG terminated the contract and moved MISLE development to its systems development center
    - USCG expects to complete development of two key subsystems in May 2001
    - Total life cycle costs are expected to be \$118.7 million
  - **Deepwater Capability Replacement Project**
    - A planned, 20-year, \$10-billion initiative to replace aging aircraft, ships, and supporting systems in the deepwater environment
    - In 1998, USCG awarded contracts for conceptual design to three vendors
    - USCG expects to select a design in early 2002
-



## IT Profile

### IT Roles and Responsibilities

---

In July 2000, USCG established an Information and Technology Directorate, headed by the Chief Information Officer (CIO), who reports to the Chief of Staff.

This organization has responsibility for USCG-wide IT strategy and oversight, including

- managing a **comprehensive IT investment process** to ensure all IT investments support desired mission outcomes
- defining and directing **architectural compliance and IT standards** across the organization
- ensuring that **information security** is included in all phases of an IT system's life cycle

This organization also oversees the **Operations Systems Center**--a government-owned, contractor-operated facility--which develops, fields, and maintains critical systems and data networks.





## IT Profile

### IT Roles and Responsibilities (continued)

USCG's Systems Directorate is responsible for IT systems management and support throughout the agency. Key supporting units include:

#### **Telecommunications and Information Systems Command**

- Supports communication/computer system test and development

#### **Command and Control Engineering Center**

- Supports command and control systems on all ships and shore units
- Develops and maintains new navigation systems

#### **Office of Force Management**

- Manages IT staffing throughout the agency

USCG's Acquisition Directorate is responsible for major acquisitions throughout the agency.



**IT Profile**  
**IT Staffing**

- As of May 2000, USCG reported having 2,355 IT positions in its 40,000-person workforce:
  - 325 Officers
  - 243 Warrant Officers
  - 1505 Enlisted
  - 282 Civilian



## IT Policies, Procedures, and Practices

### IT Areas Evaluated

To evaluate IT management, we focused on five key areas that encompass major IT functions and are recognized by the industry as having substantial influence over the effectiveness of operations:

- **IT investment management** has three essential phases--project selection, control, and evaluation--each supported by critical organizational processes. We recently issued a common framework for assessing federal agencies' IT investment management practices.<sup>1</sup> This framework takes the organizational processes supporting selection, control, and evaluation efforts, and extends them into a growth and maturity framework. The framework's five maturity stages represent steps toward achieving a stable and mature IT investment process. By determining the current stage of maturity of an organization, managers are better able to identify specific steps that would contribute to improving IT management performance.
- **IT architecture** helps align the requirements for agency-sponsored information systems with the processes that support the agency's mission and goals, achieve interoperability and security of information systems, and promote the application and maintenance of standards by which the agency evaluates and acquires systems. The information architecture has operational, systems, and technical components that delineate the business processes, information flows and relationships, systems, technology infrastructure, and standards. To implement and maintain the architecture, an agency should have processes for change management and legacy systems integration.

<sup>1</sup>Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity, Exposure Draft (GAO/AIMD-10.1.23, May 2000). This guide builds upon the investment management guidance provided in our prior guide, *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making* (GAO/AIMD-10.1.13, February 1997).



## IT Policies, Procedures, and Practices

### IT Areas Evaluated (continued)

- **Software acquisition and development** activities help produce information systems within the cost, budget, and schedule goals set by the investment management process, while complying with the guidance and standards of the information architecture. Key processes for software acquisition are acquisition planning, solicitation, contract tracking and oversight, evaluation, transition to support, and acquisition risk management. Key processes for software development include requirements management, project planning, project tracking and oversight, quality assurance, and configuration management.
- **Information security** helps protect the integrity, confidentiality, and availability of the agency's data and systems it relies on by reducing the risks of tampering, unauthorized intrusions and disclosures, and serious disruptions of operations. Information security activities include conducting risk assessments, promoting awareness, implementing controls, performing evaluations, and providing centralized coordination and oversight of all security activities.
- **IT human capital management** helps provide employees with the appropriate knowledge and skills to effectively execute critical IT functions. Key processes for human capital management involve assessing IT knowledge and skills requirements, inventorying existing staff's knowledge and skills and assessing them against requirements, developing strategies and plans to fill the gap between requirements and existing staffing, and evaluating and reporting on progress in filling the gap in knowledge and skills.



## IT Policies, Procedures, and Practices

### Evaluation Indicators

In evaluating the five key IT areas at USCG, we assessed applicable policies, procedures, and practices. We use three broad indicators to depict our results:



**Blank circle** indicates that policies and procedures do not exist or are substantially obsolete or incomplete; and practices are not performed or are predominantly ad hoc.



**Half circle** indicates that policies or procedures facilitate key functions; and selected key practices have been implemented.



**Solid circle** indicates that policies and procedures are current and comprehensive for key functions; and practices adhere to policies, procedures, and generally accepted standards.

For each of the five key IT areas reviewed, we selected indicators based on our judgment on the current state of USCG policies, procedures, and practices. There is no basis to judge how USCG is performing in relation to other agencies because we have evaluated only one other agency using this approach, and we continue to refine our approach and the elements we assess.



## IT Policies, Procedures, and Practices Evaluation Summary

Investment Management	IT investment board operation	◐	Software Acquisition	Software acquisition planning	●	Security	Risk assessment	◐
	IT project oversight	◐		Solicitation	●		Awareness	◐
	IT asset tracking	○		Requirements development and management	◐		Information system controls	●
	Business needs identification for IT projects	●		Project management	●		Physical security controls	◐
	IT proposal selection	●		Contract tracking and oversight	●		Network access controls	◐
	Portfolio selection criteria definition	●		Evaluation	●		Evaluation	◐
	Investment analysis	◐		Transition to support	●		Central management	◐
	Portfolio development	◐		Acquisition risk management	◐		Requirements	◐
	Portfolio performance oversight	○		Requirements management	●		Inventory	◐
	Operational component	●		Software project planning	◐		Workforce strategies and plans	◐
Architecture	Systems component	●	Software project tracking and oversight	◐	Human Capital	Progress evaluation	●	
	Technical component	◐	Software quality assurance	◐				
	Change management	●	Software configuration management	◐				
	Legacy systems integration	◐						

○ Incomplete or obsolete policies and procedures; ad-hoc practices

◐ Policies or procedures for key functions; selected key practices

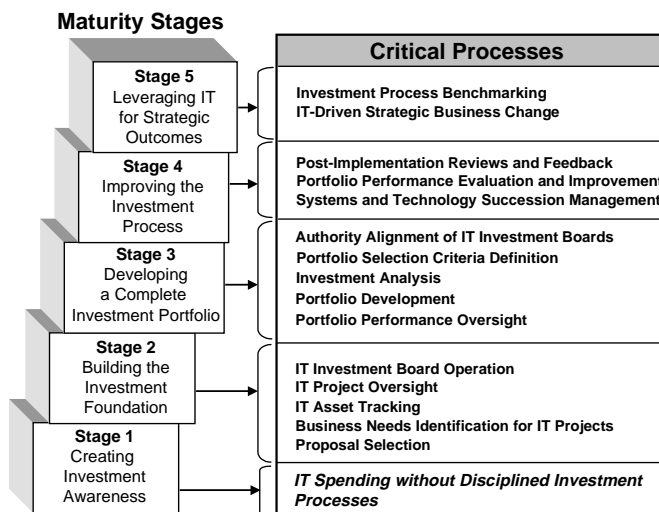
● Comprehensive, current policies and procedures; practices adhere to policies, procedures, and generally accepted standards

15



**IT Policies, Procedures, and Practices**  
**IT Investment Management -- Overview**

IT investment management provides a framework for implementing the processes that are critical to the effective selection, control, and evaluation of a portfolio of IT investments. The maturity stages, listed below, represent steps toward achieving a stable and mature IT investment management process.





## IT Policies, Procedures, and Practices IT Investment Management -- Overview (continued)

Descriptions of Critical Processes:

### STAGE 1

- **IT Spending without Disciplined Investment Processes**--there are no critical processes associated with this stage

### STAGE 2

- **IT Investment Board Operation**--creates and defines one or more IT investment boards within the organization, and operates these boards according to written policies and procedures.
- **IT Project Oversight**--the organization monitors all projects relative to cost and schedule expectations, and takes corrective action when milestones are not achieved.
- **IT Asset Tracking**--creates and maintains an IT inventory according to written procedures, in order to assist in managerial decision-making.
- **Business Needs Identification for IT Projects**--ensures that each IT project supports the organization's business needs and meets users' needs. It involves identifying business needs and users for each IT project and having users participate in project management throughout the project's life cycle.
- **Proposal Selection**--ensures that a predefined, structured process is used to select new IT proposals.





## IT Policies, Procedures, and Practices

### IT Investment Management -- Overview (continued)

#### Descriptions of Critical Processes (continued)

##### STAGE 3

- **Authority Alignment of IT Investment Boards**--coordinates the responsibilities and activities of the IT investment boards when an organization uses multiple boards.
- **Portfolio Selection Criteria Definition**--creates and communicates the criteria used by decision-makers to select and fund IT investments to the organization.
- **Investment Analysis**--examines the fundamental cost, benefit, schedule, and risk characteristics of each IT investment before it is funded and combined with other investments into a portfolio. It involves validating data associated with individual investments, then assessing and prioritizing these investments within the complete portfolio.
- **Portfolio Development**--compares worthwhile investments and then combines selected investments into a funded portfolio. It involves examining all investments and making selections for funding and then establishing expectations for each investment.
- **Portfolio Performance Oversight**--involves monitoring the performance of each investment in the portfolio. This process builds upon the Stage 2 IT project oversight process by adding the elements of investment benefit and risk management to the control process activities.



## IT Policies, Procedures, and Practices

### IT Investment Management -- Overview (continued)

Descriptions of Critical Processes (continued)

#### STAGE 4

- **Post-Implementation Reviews and Feedback**--learns from past investments and initiatives by comparing actual results with estimates.
- **Portfolio Performance Evaluation and Improvement**--evaluates portfolio performance and uses this information to improve both current IT investment processes and future investment portfolio performance.
- **Systems and Technology Succession Management**--analyzes and manages the succession of identified IT investments and assets to their higher-value successors.

#### STAGE 5

- **Investment Process Benchmarking**--identifies and implements measurable improvements in IT investment management processes so that the processes meet or exceed those used by best-in-class organizations.
- **IT-Driven Strategic Business Change**--uses information technology to strategically renovate and transform work processes and push the organization to explore new and better ways to execute its mission.



## IT Policies, Procedures, and Practices IT Investment Management Review

We evaluated USCG IT investment management using the Clinger-Cohen Act, OMB's Capital Programming Guide, and GAO's draft guide, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* (see slide 12).

We reviewed IT investment management practices for the current Coast Guard investment portfolio. We also evaluated the investment processes used on the Ports and Waterways Safety System (PAWSS), a major acquisition project, and the Configuration Management+ system (CM+), a non-major acquisition project.

We assessed applicable USCG investment processes at maturity stages 2 and 3.<sup>2</sup> We did not evaluate maturity Stage 1 because it is categorized by a lack of processes, and USCG has passed that stage. We also did not evaluate maturity stages 4 or 5 because USCG officials reported that they have not yet implemented these critical processes.

---

<sup>2</sup>Because USCG has only one investment board, the Stage 3 critical process involving authority alignment of IT investment boards was not applicable, and thus, it was not assessed.



**IT Policies, Procedures, and Practices**  
**IT Investment Management -- Evaluation**

Activity (Critical process)	Assessment	Comments
<b>IT investment board operation</b>		USCG's Investment Board charter defines membership that incorporates both IT and business knowledge. The board meets annually to select and recommend investments. However, there are no written procedures guiding the Board's operations.
<b>IT project oversight</b>		USCG's Acquisition Review Council oversees major acquisition projects. This oversight includes monthly status reports on cost, schedule, and performance; semiannual reviews; and special reviews for under-performing projects, which include approving and overseeing corrective actions. However, neither the Council nor the Investment Board oversees non-major acquisition projects or any operational system projects, which comprise most of its IT budget.
<b>IT asset tracking</b>		USCG has no policy for developing or maintaining an IT asset inventory. In practice, USCG has several different lists of assets, but they are not consistent or comprehensive. One key list, the Agency Capital Plan, summarizes the IT systems in development and in operation, but does not capture and track the assets--such as hardware, software, and human capital--comprising these systems.

Incomplete or obsolete policies and procedures; ad-hoc practices

Policies or procedures for key functions; selected key practices

Comprehensive, current policies and procedures; practices adhere to policies, procedures, and generally accepted standards



**IT Policies, Procedures, and Practices**  
**IT Investment Management -- Evaluation**

Activity (Critical process)	Assessment	Comments
<b>Business needs identification for IT projects</b>		Business needs and specific users are clearly identified for IT projects. Identified users participate in project management during the project's life cycle.
<b>Proposal selection</b>		USCG uses a structured process to solicit new IT proposals. Resource proposals are submitted for investment board consideration during the annual budget development process. Working groups analyze and prioritize IT proposals according to predefined selection criteria. The investment board makes funding recommendations for the new IT proposals according to a predefined process.
<b>Portfolio selection criteria definition</b>		USCG approves the IT portfolio selection criteria based on the agency's mission, strategies, and priorities. The criteria are reviewed, modified, and distributed throughout the agency each year, as part of the budget development process.

Incomplete or obsolete policies and procedures; ad-hoc practices

Policies or procedures for key functions; selected key practices

Comprehensive, current policies and procedures; practices adhere to policies, procedures, and generally accepted standards



**IT Policies, Procedures, and Practices**  
**IT Investment Management -- Evaluation (continued)**

Activity (Critical process)	Assessment	Comments
<b>Investment analysis</b>		USCG analyzes and prioritizes--according to portfolio selection criteria--system acquisition investments and any operational system investments that have funding-level changes from the prior year. However, inconsistent data, such as the lack of life-cycle cost and risk data, hinder the effective analysis and prioritization of these investments; USCG does not analyze or prioritize operational system investments which did not have funding level changes from the prior year; and USCG does not validate data for any investment.
<b>Portfolio development</b>		The Investment Board examines, and makes funding decisions on all system acquisition investments and any operational system investments which had funding-level changes from the prior year. Cost and schedule expectations are established for these investments. However, benefit and risk expectations are generally not established for these investments, and operational system investments which did not have funding level changes from the prior year are not examined. They are funded without examination.


Incomplete or obsolete policies and procedures; ad-hoc practices

Policies or procedures for key functions; selected key practices

Comprehensive, current policies and procedures; practices adhere to policies, procedures, and generally accepted standards



**IT Policies, Procedures, and Practices**  
**IT Investment Management -- Evaluation (continued)**

Activity (Critical process)	Assessment	Comments
<p><b>Portfolio performance oversight</b></p>		<p>USCG does not oversee a complete investment portfolio. The Acquisition Review Council monitors the performance of major system acquisition investments. However, USCG does not monitor the performance of non-major system acquisition investments or any operational system investments.</p>



Incomplete or obsolete policies and procedures; ad-hoc practices



Policies or procedures for key functions; selected key practices



Comprehensive, current policies and procedures; practices adhere to policies, procedures, and generally accepted standards



## IT Policies, Procedures, and Practices

### Impact of IT Investment Management Weaknesses

- **IT Investment Board Operation:**

Without written procedures, USCG lacks assurance that the investment board will provide investment management oversight and decision-making in a repeatable and consistent manner.

- **IT Project Oversight:**

Project oversight is performed on only a small portion of the agency's projects, the major acquisition projects. Without an oversight process that compares actual cost and schedule data to original estimates for all projects, USCG management lacks assurance that all projects are under control and being developed on time, within budget, and according to requirements.

- **IT Asset Tracking:**

Without up-to-date information on a comprehensive inventory of IT assets, USCG lacks assurance that decisionmakers have the information they need to effectively manage IT investments.





## IT Policies, Procedures, and Practices

### Impact of IT Investment Management Weaknesses

- **Investment Analysis:**  
Without analysis and validation of all IT investments' costs, benefits, schedules, and risks, USCG cannot be certain that it is selecting and funding the IT investments that will best result in mission-focused benefits.
- **Portfolio Development:**  
By not examining--and establishing cost, benefit, risk, and schedule expectations on--all IT investments, USCG lacks assurance that it is effectively selecting and funding an optimal portfolio with manageable risks and returns.
- **Portfolio Performance Oversight:**  
By not overseeing the performance of a complete investment portfolio, USCG lacks assurance that its portfolio will achieve cost, benefit, schedule, and risk expectations.



## IT Investment Management Recommendations

USCG should:

- Develop written procedures to guide IT Investment Board operations.
- Establish an IT oversight process that compares actual cost and schedule data with original estimates for all projects to determine whether investments are proceeding as expected and to take corrective actions as appropriate.
- Establish a comprehensive inventory of IT assets that includes up-to-date cost and schedule information.
- Establish a process for analyzing, validating, and prioritizing the costs, benefits, schedules, and risks associated with all IT investments.
- Develop and oversee a comprehensive IT investment portfolio.



## IT Policies, Procedures, and Practices

### Plans to Address IT Investment Management Weaknesses

USCG officials stated that the agency plans to

- reassess and revise its investment management processes
- incorporate lessons learned and our recommendations in its efforts to revise USCG investment management policy
- identify funds for all IT investments as part of future oversight activities
- implement control phase activities next year



## IT Policies, Procedures, and Practices

### IT Architecture -- Overview

An IT architecture serves as a blueprint to guide and constrain the development and evolution of a collection of related information systems.

Three typical components of an IT architecture are:

- **Operational component**--describes the operational elements (business functions), assigned tasks and activities, and information flows required to support an operation
- **Systems component**--describes and graphically depicts how multiple systems link and interoperate to support an operation, and may describe the internal construction and operation of individual systems within the architecture
- **Technical component**--provides the technical system implementation guidelines upon which engineering specifications are based and common building blocks are established, and provides a set of tools that facilitate integration of legacy and new systems



## IT Policies, Procedures, and Practices

### IT Architecture -- Overview (continued)

OMB guidelines require agencies to include certain key elements in their IT architectures. These elements can be generally grouped into the three component categories as follows:

#### **Operational component**

- Business or operational processes
- Information flows and relationships in those processes

#### **Systems component**

- Activities or systems that capture, manipulate, and manage the information to support operations
- Data descriptions and relationships and how data are maintained, accessed, and used

#### **Technical component**

- Technology standards, services, and infrastructure



## IT Policies, Procedures, and Practices

### IT Architecture -- Overview (continued)

OMB guidelines also require agencies to establish two key processes to maintain and implement the architecture:

#### **Change management**

- Manages and documents changes to the architecture that are needed as business functions evolve

#### **Legacy systems integration**

- Develops and implements a strategy for integrating existing and new systems that will permit them to interoperate cost-effectively

We evaluated the Coast Guard's Command, Control, Communications, Computer and Intelligence (C4I) architecture using the Clinger-Cohen Act, OMB guidance, and the Defense Department Architecture Working Group's Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework, version 2.0. We also reviewed USCG's efforts to ensure compliance with its IT architecture through the investment decision-making process. We did not evaluate USCG's actions to develop an enterprise-wide architecture.



**IT Policies, Procedures, and Practices**  
**IT Architecture-- Evaluation**

Activity	Assessment	Comments
<b>Operational component</b>		USCG's C4I Baseline Architecture describes the agency's operational functions, including waterway management, search and rescue, ice operations, commercial vessel safety, marine environmental protection, port safety and security, law enforcement, defense operations, and recreational boating safety. It also describes information flows.
<b>Systems component</b>		USCG's Information Architecture contains a mapping of systems to business functions. The Systems Plan describes critical information systems such as MISLE, FLS, and the Aviation Logistics Management Information System. The Objective Architecture and Transition Plan provides a framework for attaining systems integration in the areas of command, control, communications, and computers.



Incomplete or obsolete policies and procedures; ad-hoc practices



Policies or procedures for key functions; selected key practices



Comprehensive, current policies and procedures; practices adhere to policies, procedures, and generally accepted standards



**IT Policies, Procedures, and Practices**  
**IT Architecture-- Evaluation (continued)**

Activity	Assessment	Comments
<b>Technical component</b>		USCG's Common Operating Environment, Baseline Product List, and Technology Architecture describe the technical architecture, technical standards, platforms, interfaces, and security standards. However, USCG does not ensure that all system investments are compliant with the architecture infrastructure and standards.
<b>Change management</b>		USCG policies provide configuration control over the C4I Baseline Architecture. In practice, we found changes to the architecture were documented and controlled.
<b>Legacy systems integration</b>		USCG has guidelines for legacy systems integration. However, internal assessments show that legacy systems have not been effectively integrated in the past, resulting in limited information sharing and redundant data.

Incomplete or obsolete policies and procedures; ad-hoc practices

Policies or procedures for key functions; selected key practices

Comprehensive, current policies and procedures; practices adhere to policies, procedures, and generally accepted standards





## IT Policies, Procedures, and Practices Impact of IT Architecture Weaknesses

- Without ensuring that all system investments are compliant with the architecture, USCG lacks assurance that its investments are compatible and cost-effective
- Without effective legacy system integration, USCG lacks assurance that new software and hardware will be compatible with existing systems.



## IT Architecture Recommendations

- USCG should ensure that all system investments are compliant with the IT architecture
- USCG should ensure that legacy systems integration processes are effectively implemented across the agency



## IT Architecture

### Plans To Address IT Architecture Weaknesses

---

- USCG recognizes that IT acquisition review and approval processes do not adequately address compliance with its IT standards, policy, and guidance.
  - In June 2000, USCG established an IT Life Cycle and Configuration Management Working Group (LCCMWG) to address gaps, redundancies, and conflicts in USCG IT standards, policy, and guidance.
- USCG recognizes a need to improve information sharing and eliminate redundant data.
  - In September 1999, USCG began exploring the use of an enterprise decision support system and data warehousing technology in order to optimize data-sharing and eliminate redundant data.



## IT Policies, Procedures, and Practices

### Software Acquisition and Development -- Overview

Many organizations rely on software-intensive systems to perform their missions. The quality of these systems' software is governed largely by the quality of the processes involved in acquiring or developing the software, and in maintaining it. Carnegie Mellon University's Software Engineering Institute (SEI), recognized for its expertise in software processes, has developed models and methods for determining an organization's software process maturity.

SEI's Capability Maturity Model (CMM) provides a framework of five maturity levels that can be used to identify an organization's current process strengths and weaknesses, and to develop a structured plan for incremental process improvement. The five maturity levels are:

1. **Initial:** the software process is characterized as ad hoc and few processes are defined.
2. **Repeatable:** basic project management processes are established; the necessary process discipline is in place to repeat earlier successes.
3. **Defined:** software processes are documented and standardized; all projects use an approved, tailored version of the organization's standard software processes for acquiring or developing software products and services.
4. **Managed/Quantitative:** detailed measures of the software processes, products, and services are collected; the software processes and products are quantitatively understood and controlled.
5. **Optimizing:** continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.



## IT Policies, Procedures, and Practices

### Software Acquisition and Development -- Overview (continued)

The CMM's maturity levels 2 through 5 require the verifiable existence and use of certain software processes, known as key process areas (KPA).

SEI has developed separate maturity models, with supporting KPAs, for both software acquisition and software development.

We evaluated USCG's policies and procedures on software acquisition and development using SEI's Software Acquisition and Software Development Capability Maturity Models and SEI's Software Capability Evaluation (SCE) methodology. We conducted SCEs on two software acquisition projects (Fleet Logistics System--FLS and Marine Information for Safety and Law Enforcement--MISLE) at USCG headquarters, and on two software development projects (Marine Safety Information System--MSIS and MISLE) at USCG's Operations Systems Center. Our evaluation teams were led by, and staffed with, SEI-trained software specialists.

We evaluated USCG's software acquisition processes against all applicable level 2 KPAs and one level 3 KPA--acquisition risk management--because it is considered by software experts to be a very important process area.

We evaluated USCG's software development processes against all applicable level 2 KPAs.



## IT Policies, Procedures, and Practices

### Software Acquisition and Development -- Overview (continued)

Applicable software acquisition KPAs:

- **Software acquisition planning**--identifies and organizes the work elements necessary for the contractor to perform the software engineering, and the organization's support and oversight of the contractor.
- **Solicitation**--details the solicitation and selection of contractors qualified to satisfy the contract's requirements for the project's software-related products and services. The solicitation package includes the contractual software requirements, proposal evaluation criteria, and product-acceptance criteria.
- **Requirements development and management**--establishes a common and unambiguous definition of software-related contractual requirements that is understood by the project team, end user, and contractor team.
- **Project management**--manages the activities of the project office to ensure timely, efficient, and effective software acquisition.



## IT Policies, Procedures, and Practices

### Software Acquisition and Development -- Overview (continued)

Applicable software acquisition KPAs, continued:

- **Contract tracking and oversight**--ensures that the contractor's software engineering is managed and complies with contract requirements, and adheres to relevant laws, policies, regulations, and other guidance.
- **Evaluation**--evaluates contractor products against technical requirements throughout the total period of the acquisition to provide an integrated approach that takes advantage of all evaluation results.
- **Transition to support**--ensures that the software support organization has the capacity and capability to provide the required support upon assumption of responsibility for the support of the software products.
- **Acquisition risk management**--identifies risks as early as possible, adjusts the acquisition strategy to manage those risks, and develops and implements a risk management process as an integral part of the acquisition organization's standard software acquisition process.



## IT Policies, Procedures, and Practices

### Software Acquisition and Development -- Overview (continued)

Applicable software development KPAs:

- **Requirements management**--establishes and documents common understandings of the customer's requirements between the customer and the software project team.
- **Software project planning**--identifies and organizes the work elements for performing the software engineering and managing the project.
- **Software project tracking and oversight**--measures and controls the performance, cost, and schedule objectives of the project throughout its life. It provides visibility into actual progress so that management can act effectively when the software project's performance deviates significantly from plans.
- **Software quality assurance**--determines if the process being used by the project and the resulting products comply with the organization's policies and procedures.
- **Software configuration management**--establishes and maintains the integrity of the products throughout the project's software life cycle, through a structured process for documenting proposed and approved changes in requirements and plans.





**IT Policies, Procedures, and Practices**  
**Software Acquisition-- Evaluation**

Activity (Key process area)	Assessment	Comments
<b>Software acquisition planning</b>		USCG's Systems Acquisition Manual (SAM) provides policy guidance for acquisition planning. USCG adhered to the policy and related procedures when planning the software acquisitions we reviewed.
<b>Solicitation</b>		USCG has a policy for conducting the solicitation. The software acquisition projects we reviewed generally followed the policy and related procedures when conducting the solicitation.
<b>Requirements development and management</b>		USCG has a policy for developing and managing requirements, but some practices, such as assessment of requirements changes and bidirectional traceability, were lacking.
<b>Project management</b>		The SAM provides the policy for project management; USCG generally followed the policy and procedures in managing the software acquisition projects we reviewed.



Incomplete or obsolete policies and procedures; ad-hoc practices



Policies or procedures for key functions; selected key practices



Comprehensive, current policies and procedures; practices adhere to policies, procedures, and generally accepted standards



**IT Policies, Procedures, and Practices**  
**Software Acquisition-- Evaluation (continued)**

Activity (Key process area)	Assessment	Comments
<b>Contract tracking and oversight</b>		USCG has current policies for contract tracking and oversight and it has generally followed these policies and practices in recent acquisition projects.
<b>Evaluation</b>		USCG has generally followed its current policies and procedures in evaluating contractor deliverables and software products on recent software acquisition projects.
<b>Transition to support</b>		USCG has generally followed its current policies and procedures in planning the transition of software products being acquired to the software support organization.
<b>Acquisition risk management</b>		USCG has policies for risk management. However, we found cases in which there was no evidence that risks were tracked and controlled until mitigated.



Incomplete or obsolete policies and procedures; ad-hoc practices



Policies or procedures for key functions; selected key practices



Comprehensive, current policies and procedures; practices adhere to policies, procedures, and generally accepted standards



**IT Policies, Procedures, and Practices**  
**Software Development-- Evaluation**

Activity (Key process area)	Assessment	Comments
<b>Requirements management</b>		USCG has current policies and procedures for requirements management that were generally being used to establish and maintain the requirements baseline of the major software projects we reviewed.
<b>Software project planning</b>		USCG has a systems development methodology that provides software project planning guidance. However, it lacks documented procedures for estimating a software project's effort, cost, and schedules.
<b>Software project tracking and oversight</b>		USCG has a policy for project tracking and oversight. Some tracking and oversight activities were performed, but documented procedures were lacking for key activities such as formal reviews to address the project's accomplishments and results.
<b>Software quality assurance</b>		USCG has a quality assurance policy, but many quality assurance practices were not performed.



Incomplete or obsolete policies and procedures; ad-hoc practices




Policies or procedures for key functions; selected key practices



Comprehensive, current policies and procedures; practices adhere to policies, procedures, and generally accepted standards



**IT Policies, Procedures, and Practices**  
**Software Development-- Evaluation (continued)**

Activity (Key process area)	Assessment	Comments
<b>Software configuration management</b>		USCG's configuration management plan provides guidance for configuration identification, change control, configuration status accounting, configuration management audits, data management and library functions, interface management, and contractor control. However, configuration management practices were lacking in a recent project.



Incomplete or obsolete policies and procedures; ad-hoc practices



Policies or procedures for key functions; selected key practices



Comprehensive, current policies and procedures; practices adhere to policies, procedures, and generally accepted standards



## IT Policies, Procedures, and Practices

### Impact of Software Acquisition and Development Weaknesses

#### Software Acquisition

- Without adequate requirements development and management, USCG lacks assurance that its software requirements are unambiguously defined and are clearly understood by the project team, the software's end users, and the contractor team.
- Without a fully implemented and documented acquisition risk management process, USCG lacks assurance that it is successfully identifying the risks posed to the system being acquired and that risk mitigation strategies are initiated, implemented, and tracked in a timely manner.



## IT Policies, Procedures, and Practices

### Impact of Software Acquisition and Development Weaknesses

#### Software Development

- Without adequate software project planning, USCG lacks assurance that reasonable plans for performing the software engineering and for managing the software project have been developed and are in use.
- Without adequate software project tracking and oversight, USCG lacks assurance that management can effectively oversee the project's actual progress and can take effective action when the project's performance deviates significantly from software plans.
- Without an adequate software quality assurance process, USCG lacks assurance that management can effectively oversee the processes being used on the software project and the quality of the resulting products.
- Without adequate configuration management, USCG lacks assurance that the integrity of the products of the software project are maintained throughout the project's life cycle.



## IT Software Acquisition and Development Recommendations

USCG should initiate a process improvement effort to address weaknesses in the following key process areas:

### Software Acquisition

- requirements development and management
- acquisition risk management

### Software Development

- project planning
- project tracking and oversight
- quality assurance
- configuration management



## IT Policies, Procedures, and Practices

### Plans to Address Software Acquisition and Development Weaknesses

USCG officials stated that they plan to improve the agency's documentation of software acquisition and development practices in order to ensure that these practices are adequately performed.

USCG officials at the Operations Systems Center stated that they plan to improve their software quality assurance processes.





## IT Policies, Procedures, and Practices

### Information Security -- Overview

Information security protects an organization's computer-supported resources and assets. Such protection ensures the integrity, appropriate confidentiality, and availability of an organization's data and systems. **Integrity** means that data have not been altered or destroyed in an unauthorized manner. **Confidentiality** means that information is not made available or disclosed to unauthorized individuals, entities, or processes. **Availability** means that data will be accessible or usable upon demand by an authorized entity.

Key activities for managing information security risks include:

- **Risk assessment** -- identifying security threats and vulnerabilities to information assets and operational capabilities, ranking risk exposures, and identifying cost-effective controls
- **Awareness** -- promoting awareness concerning security risks and educating users about security policies and procedures
- **Controls** -- implementing controls necessary to deal with identified risks to information systems, physical facilities, and networks in order to protect them



## IT Policies, Procedures, and Practices Information Security -- Overview (continued)

- **Evaluation** -- monitoring effectiveness of controls and awareness activities through periodic evaluation
- **Central management** -- coordinating security activities through a centralized group

We evaluated USCG's policies and procedures on information security using the Clinger-Cohen Act, the Computer Security Act, and guidelines issued by OMB, ourselves, and the National Institute of Standards and Technology. We reviewed facilities' security plans, physical security evaluation reports, and system risk assessments. We evaluated key security controls on a USCG network. We also reviewed a Department of Transportation Office of the Inspector General report involving information security.



**IT Policies, Procedures, and Practices**  
**Information Security-- Evaluation**

Activity	Assessment	Comments
<b>Risk assessment</b>		USCG's Automated Information Systems (AIS) Security Manual requires system owners to conduct periodic system risk assessments as part of the system accreditation process, and after a major system alteration. Further, USCG provided comprehensive risk assessments for several systems. However, USCG was unable to report on whether all systems had this required assessment because it does not track systems' status.
<b>Awareness</b>		USCG AIS Security Manual has a requirement for security awareness training. Information security personnel receive security awareness training during an annual security awareness workshop and USCG recently began to provide awareness briefings to high-level officials. USCG also provides security briefings to all new system users. However, many of the system risk assessments we reviewed noted the need for periodic refresher training on security awareness. Such refresher training would focus on emerging issues, threats, and technologies.




Incomplete or obsolete policies and procedures; ad-hoc practices

Policies or procedures for key functions; selected key practices

Comprehensive, current policies and procedures; practices adhere to policies, procedures, and generally accepted standards



**IT Policies, Procedures, and Practices**  
**Information Security-- Evaluation (continued)**

Activity	Assessment	Comments
<b>Information system controls</b>		USCG's AIS Security Manual requires system owners to assess systems risks, address any identified weaknesses, and then to obtain accreditation of each system in order to ensure that the systems are adequately protected. However, in response to our query, a USCG security official determined that only 3 of 38 operational systems have this accreditation.
<b>Physical security controls</b>		USCG Physical Security policy requires biennial physical security evaluations of its facilities to determine the facility's ability to protect against loss of property. However, USCG does not ensure facility owners to implement corrective actions to address identified weaknesses. Consequently, weaknesses that are not corrected are simply reported again during the subsequent evaluation.
<b>Network access controls</b>		USCG's AIS Security Manual addresses network security and USCG has been proactive in implementing network security access controls. For example, USCG has both intrusion-detection on its network and emergency-response capabilities. Despite these efforts, our review identified several access control weaknesses that make the network more vulnerable to intrusion.



Incomplete or obsolete policies and procedures; ad-hoc practices





Policies or procedures for key functions; selected key practices





Comprehensive, current policies and procedures; practices adhere to policies, procedures, and generally accepted standards




**IT Policies, Procedures, and Practices**  
**Information Security-- Evaluation (continued)**

Activity	Assessment	Comments
<b>Evaluation</b>		USCG policies assign responsibility for overseeing facility and systems security controls to two headquarters offices. These offices are to ensure that evaluations of facilities' physical security reviews and systems risk assessments are conducted. However, neither office routinely acts to ensure that corrective actions identified during evaluations are implemented or are effective.
<b>Central management</b>		USCG's Office of Security Policy and Management is responsible for overseeing security activities across the agency. This office also manages and enforces physical and personnel security, but not information systems security. The Office of Information Management is responsible for managing and enforcing information systems security. However, neither office routinely tracks systems' security status or ensures that corrective actions to address security weaknesses are implemented.

 Incomplete or obsolete policies and procedures; ad-hoc practices

 Policies or procedures for key functions; selected key practices

 Comprehensive, current policies and procedures; practices adhere to policies, procedures, and generally accepted standards



## IT Policies, Procedures, and Practices

### Impact of Information Security Weaknesses

- Without a comprehensive security awareness program, USCG lacks assurance that staff will be cognizant of, and adhere to, established information security policies and procedures.
- Without enforced processes for systems' risk assessments and accreditations, USCG lacks assurance that its information systems are protected against identified vulnerabilities.
- Without resolution of corrective actions identified during physical security evaluations, USCG lacks assurance that the facilities that house critical information systems are adequately protected.
- Without resolution of identified weaknesses in its network controls, USCG lacks assurance that these controls will adequately protect its networks.
- Without effective central oversight and coordination, USCG lacks assurance that established information security policies and procedures are implemented and that identified vulnerabilities are addressed throughout the agency.



## Information Security Recommendations

- USCG should implement a complete, effective security awareness program.
- USCG should ensure that systems' risk assessments and accreditations are completed.
- USCG should implement appropriate corrective actions on vulnerabilities identified during facilities' physical security evaluations.
- USCG should implement appropriate corrective actions on the network security weaknesses we identified.
- USCG should develop and implement a centralized mechanism to monitor and enforce compliance with physical security and information systems security policies.



## IT Policies, Procedures, and Practices Plans to Address Information Security Weaknesses

USCG officials reported that they are:

- working to improve USCG's security awareness program by providing contractor support to Information Systems Security Officers in the field, and through the development of a web-enabled awareness program
- obtaining contractor support to help achieve the certification and accreditation of major financial systems and major applications at OSC
- seeking funds to improve facilities' physical security
- working to 1) mitigate the network access control vulnerabilities we identified, 2) re-certify USCG's wide area network, and 3) re-accredit key local area networks
- re-instituting a requirement for system owners to perform and report on annual self-audits
- planning to assess the feasibility of identifying other agencies' methods of obtaining information on system risk assessments, accreditations, and training





## IT Policies, Procedures, and Practices

### IT Human Capital -- Overview

Human capital centers on viewing people as assets whose value to an organization can be enhanced through investment. As the value of people increases, so does the performance capacity of the organization, and therefore its value to clients and other stakeholders.

To maintain and enhance the capabilities of IT staff, the organization should conduct four basic activities:

- **Requirements**--assess the knowledge and skills needed to effectively perform IT operations to support agency mission and goals
- **Inventory**--determine the knowledge and skills of current IT staff to identify gaps in needed capabilities
- **Workforce strategies and plans**--develop strategies and implement plans for hiring, training, and professional development to fill the gap between requirements and current staffing
- **Progress evaluation**--evaluate progress made in improving IT human capital capability, and use the results of these evaluations to continuously improve the organization's human capital strategies



## IT Policies, Procedures, and Practices



### IT Human Capital -- Overview (continued)

We evaluated USCG's policies and procedures on IT human capital using the Clinger-Cohen Act and our guide *Human Capital: A Self-Assessment Checklist for Agency Leaders*.<sup>3</sup> We reviewed IT human capital practices on the following projects: the Marine Safety Information System, the Marine Information For Safety and Law Enforcement, and the Fleet Logistics System.

<sup>3</sup>GAO/GGD-99-179, September 1999.



**IT Policies, Procedures, and Practices**  
**IT Human Capital-- Evaluation**

Activity	Assessment	Comments
<b>Requirements</b>		USCG's Office of Force Management is responsible for identifying, evaluating, and analyzing all IT personnel requirements and ensuring that performance qualifications meet mission needs. The office conducted assessments of the knowledge and skills needed by IT officers and enlisted personnel throughout the Coast Guard. The office has not assessed the knowledge and skills needed by its civilian IT workforce.
<b>Inventory</b>		USCG does not have a complete inventory of IT knowledge and skills. The agency maintains a profile on each of its officers and enlisted personnel that includes general information on knowledge and skills (such as training and assignment history), and uses this profile to match individuals to new assignments. However, in a mid-1998 assessment, enlisted IT personnel and their commanding officers expressed concern that the profiles did not adequately capture their IT knowledge and skills, and USCG efforts to address this concern are ongoing. USCG does not maintain an inventory of IT knowledge and skills for its civilian workforce.



Incomplete or obsolete policies and procedures; ad-hoc practices





Policies or procedures for key functions; selected key practices





Comprehensive, current policies and procedures; practices adhere to policies, procedures, and generally accepted standards




**IT Policies, Procedures, and Practices**  
**IT Human Capital-- Evaluation (continued)**

Activity	Assessment	Comments
<p><b>Workforce strategies and plans</b></p>		<p>USCG has policies and procedures that address gaps in its IT workforce. In practice, USCG addresses gaps through recruiting, retention, and professional development programs. For example, it offers recruiting incentives and is creating a new IT career field for enlisted personnel. It also uses reservists on extended active duty contracts in order to meet critical IT officer shortages. However, because USCG has not yet fully defined the IT knowledge and skills needed by its civilian workforce, it has not yet defined its strategy for filling those needs.</p>
<p><b>Progress evaluation</b></p>		<p>USCG's Office of Force Management is responsible for evaluating the agency's progress in improving its IT human capital capabilities. The office tracks its progress in filling IT officer and enlisted positions. However, the office has not analyzed or reported on the effectiveness of its specific recruiting, training, and incentive programs.</p>

 Incomplete or obsolete policies and procedures; ad-hoc practices

 Policies or procedures for key functions; selected key practices

 Comprehensive, current policies and procedures; practices adhere to policies, procedures, and generally accepted standards



## IT Policies, Procedures, and Practices

### Impact of IT Human Capital Weaknesses

- Until it assesses the knowledge and skills needed by its civilian IT workforce, USCG lacks assurance that it has effectively identified the IT knowledge and skills needed to sustain its operations and developed strategies to fill these needs.
- Without a complete inventory of IT knowledge and skills, USCG lacks assurance that it is optimizing the use of its current IT workforce and fully understanding the extent of its IT skill gaps.
- Without analyzing and documenting the effectiveness of its workforce strategies, senior decisionmakers lack assurance that they are effectively addressing IT knowledge and skill gaps.



## IT Human Capital Recommendations

- USCG should assess its IT civilian workforce to identify its knowledge and skill requirements, and any gaps.
- USCG should maintain a complete inventory that includes specific IT knowledge and skills.
- USCG should analyze and document the effectiveness of its strategies for recruiting, training, and developing IT personnel, and use the results to continuously improve its human capital strategies.



## IT Policies, Procedures, and Practices Plans to Address IT Human Capital Weaknesses

The Office of Force Management

- is working to improve the precision and number of descriptions it uses to describe IT knowledge and skills of enlisted personnel
- plans to work with other offices to analyze and document the effectiveness of workforce strategies



## Agency Comments

In commenting on a draft of this briefing, USCG officials

- generally agreed with our findings and recommendations
- planned to implement many of our recommendations
- offered specific comments, which have been incorporated in this briefing as appropriate



# GAO Contact and Staff Acknowledgments

---

---

## GAO Contact

Colleen Phillips, (202) 512-6326

---

## Acknowledgments

Individuals making key contributions to the briefing and this report included Nabajyoti Barkakati, William G. Barrick, Timothy E. Case, John T. Christian, Ronald E. Famous, Barbarol J. James, Tonia L. Johnson, William Lew, Anna T. Nguyen, Thomas F. Noone, and Madhav Panwar.

---

---

## Ordering Information

The first copy of each GAO report is free. Additional copies of reports are \$2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

***Orders by mail:***

U.S. General Accounting Office  
P.O. Box 37050  
Washington, DC 20013

***Orders by visiting:***

Room 1100  
700 4th St. NW (corner of 4th and G Sts. NW)  
U.S. General Accounting Office  
Washington, DC

***Orders by phone:***

(202) 512-6000  
fax: (202) 512-6061  
TDD (202) 512-2537

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

***Orders by Internet:***

For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

[info@www.gao.gov](mailto:info@www.gao.gov)

or visit GAO's World Wide Web home page at:

<http://www.gao.gov>

---

## To Report Fraud, Waste, or Abuse in Federal Programs

***Contact one:***

- Web site: <http://www.gao.gov/fraudnet/fraudnet.htm>
- e-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)
- 1-800-424-5454 (automated answering system)



---

**United States  
General Accounting Office  
Washington, D.C. 20548-0001**

**Official Business  
Penalty for Private Use \$300**

**Address Correction Requested**

---

<p><b>Bulk Rate Postage &amp; Fees Paid GAO Permit No. GI00</b></p>
---

