United States Government Accountability Office

GAO

Report to the Subcommittee on Readiness and Management Support, Committee on Armed Services, U.S. Senate

September 2008

DOD BUSINESS SYSTEMS MODERNIZATION

Planned Investment in Navy Program to Create Cashless Shipboard Environment Needs to Be Justified and Better Managed

GAO-08-922

September 2008

DOD BUSINESS SYSTEMS MODERNIZATION

Planned Investment in Navy Program to Create Cashless Shipboard Environment Needs to Be Justified and Better Managed

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-922, a report to the Subcommittee on Readiness and Management Support, Committee on Armed Services, U.S. Senate

Why GAO Did This Study

GAO has designated the Department of Defense's (DOD) multi-billion dollar business systems modernization efforts as high risk, in part because key information technology (IT) management controls have not been implemented on key investments, such as the Navy Cash program. Initiated in 2001, Navy Cash is a joint Department of the Navy (DON) and Department of the Treasury Financial Management Service (FMS) program to create a cashless environment on ships using smart card technology, and is estimated to cost about $320 million to fully deploy. As requested, GAO analyzed whether DON is effectively implementing IT management controls on the program, including architectural alignment, economic justification, requirements development and management, risk management, security management, and system quality measurement against relevant guidance.

What GAO Recommends

GAO recommends that investment of modernization funding in Navy Cash be limited until a basis for informed decision making is established, and that other program management weaknesses be corrected, as appropriate. DOD agreed with most of GAO's recommendations and described actions underway or planned to address them, while FMS committed to supporting DON in implementing them. Both provided other comments that GAO addresses in the report.

To view the full product, including the scope and methodology, click on GAO-08-922. For more information, contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov.

What GAO Found

Key IT management controls have not been effectively implemented on Navy Cash, to the point that further investment in this program, as it is currently defined, has not been shown to be a prudent and judicious use of scarce modernization resources. In particular, Navy Cash has not been (1) assessed and defined in a way to ensure that it is not duplicative of programs in the Air Force and the Army that use smart card technology for electronic retail transactions and (2) economically justified on the basis of reliable analyses of estimated costs and expected benefits over the program's life. As a result, DON cannot demonstrate that the investment alternative that it is pursuing is the most cost-effective solution to satisfying its mission needs.

Moreover, other management controls, which are intended to maximize the chances of delivering defined and justified system capabilities and benefits on time and within budget, have not been effectively implemented.

- System requirements have not been effectively managed. For example, neither policies nor plans that define how system requirements are to be managed, nor an approved baseline set of requirements that are justified and needed to cost-effectively meet mission needs, exist. Instead, requirements are addressed reactively through requests for changes to the system based primarily on the availability of funding.
- Program risks have not been effectively managed. In particular, plans, processes, and procedures that provide for identifying, mitigating, and disclosing risks have not been defined, nor have risk-related roles and responsibilities for key stakeholders.
- System security has not been effectively managed, thus putting the confidentiality, integrity, and availability of deployed and operating shipboard devices, applications, and data at increased risk of being compromised. For example, the mitigation of system vulnerabilities by applying software patches has not been effectively implemented.
- Key aspects of system quality are not being effectively measured. For example, data for determining trends in unresolved system change requests, which is an indicator of system stability, as well as user feedback on system satisfaction, are not being collected and used.

Program oversight and management officials acknowledged these weaknesses and cited turnover of staff in key positions and their primary focus on deploying Navy Cash as reasons for the state of some of these IT management controls. Collectively, this means that, after investing about 6 years and $132 million on Navy Cash and planning to invest an additional $60 million to further develop the program, the department has yet to demonstrate through verifiable analysis and evidence that the program, as currently defined, is justified. Moreover, even if further investment was to be demonstrated, the manner in which the delivery of program capabilities is being managed is not adequate. As a result, the program is at risk of delivering a system solution that falls short of cost, schedule, and performance expectations.

Contents

Abbreviations

ATM	automated teller machine
BEA	business enterprise architecture
DOD	Department of Defense
DON	Department of the Navy
FISMA	Federal Information Security Management Act
FMS	Department of the Treasury, Financial Management Service
IT	information technology
NAVSUP	Naval Supply Systems Command
NIST	National Institute of Standards and Technology
NTCSS	Naval Tactical Command Support System
OMB	Office of Management and Budget

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 8, 2008

The Honorable Daniel K. Akaka
Chairman
The Honorable John Thune
Ranking Member
Subcommittee on Readiness and Management Support
Committee on Armed Services
United States Senate

The Honorable John Ensign
United States Senate

For decades, the Department of Defense (DOD) has been challenged in modernizing its business systems.[1] In 1995, we designated the department's modernization effort as high-risk, and we continue to do so today.[2] Among our reasons for doing so are the enormous size and complexity of the effort, and the department's long-standing challenges in implementing effective information technology (IT) management controls on each business system investment.

One of the Department of the Navy's (DON) larger business system modernizations is Navy Cash. Initiated in 2001, the program is to create a cashless environment on ships through the use of smart card technology.[3] It is being executed jointly with the Department of the Treasury's Financial Management Service (FMS), under which DON is responsible for managing the acquisition of Navy Cash, while FMS is responsible for (1) managing the funds distributed through the system and (2) developing and maintaining the system. Navy Cash is expected to cost approximately $320 million to develop and implement over a 14-year period. Of this, $220

[1]Business systems include financial and non-financial systems that support DOD's business operations, such as civilian personnel, finance, health, logistics, military personnel, procurement, and transportation.

[2]GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

[3]Smart cards are plastic devices that are about the size of a credit card and contain an embedded integrated circuit chip capable of storing and processing data. The term "smart card" may also be used to refer to cards with a computer chip, also referred to as an e-purse, that store information to be processed by hardware such as point-of-sale terminals or card access devices.

million is being funded by DON and $100 million is being funded by FMS. The system is to be fully deployed in fiscal year 2011.

As agreed, our objective was to determine whether DON is effectively implementing IT management controls on Navy Cash. To accomplish this, we analyzed a range of program documentation and interviewed cognizant officials relative to the following IT management controls: architectural alignment, economic justification, requirements development and management, risk management, security management, and system quality measurement. In doing so, we compared DON's efforts in each control area to relevant federal and industry requirements and guidance.

We conducted this performance audit between June 2007 and September 2008, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Additional details on our objective, scope, and methodology are in appendix I.

Results in Brief

Key IT management controls have not been effectively implemented on Navy Cash. Collectively, these IT management controls are intended to ensure that a selected system investment alternative represents the most cost-effective option to meeting a mission need and, if it is, that the proposed investment, as defined, is acquired and deployed in a way that maximizes the chances of delivering promised system capabilities and benefits on time and within budget. For Navy Cash, these management controls have largely not been implemented. As a result, investment in the system has not been justified. More specifically,

- Navy Cash has not been assessed to ensure that it is not duplicative of programs in the Air Force and the Army that also provide for the use of smart card technology for electronic retail transactions. As a result, the extent of such duplication, and thus the opportunity for DOD to share and reuse system functions and services across the military departments, is not known. Within DOD, the means for avoiding business system duplication and overlap is the department's process for assessing

compliance with the DOD business enterprise architecture (BEA).[4] However, the BEA does not contain business activities that Navy Cash supports and according to DOD officials, are not planned for inclusion in the architecture. Further, even if the BEA included the business activities that Navy Cash supports, the program's ability to assess architecture compliance would have been limited because the program office did not develop a complete set of system-level architecture products needed to perform a meaningful compliance assessment. As a result, resources are being invested to deliver capabilities that could be potentially duplicative of similar programs in the department; therefore, DOD may not be pursuing the most cost-effective solution to its mission needs.

- Navy Cash has not been economically justified on the basis of reliable analyses of estimated costs and expected benefits over the life of the program. According to the latest economic analysis, the program is expected to produce estimated benefits of about $133 million for an estimated cost of about $100 million. However, the cost estimate is not reliable because it covers only 6 years of costs, while the program's estimated life cycle is now at least 14 years. Moreover, the cost estimate excludes FMS's costs, and it was not derived in accordance with effective estimating practices, such as adjusting the estimate to account for program risks and changes to the program. At the same time, the economic analysis did not consider all relevant alternatives, such as leveraging in part or in total the above mentioned Air Force and Army programs. Further, the benefits projection erroneously counted $40 million as cost savings rather than cost transfers (i.e., shift in the control over spending from one group to another that does not result in an economic gain); therefore, projected benefits should only be $93 million. Additionally, the economic analysis has not been validated using data on actual benefits accrued to date. Without a reliable economic analysis, DON's ongoing and planned investment in Navy Cash lacks adequate justification and may not be a cost-effective course of action.

  Even if investment in Navy Cash were justified, the manner in which the system is being acquired and deployed does not reflect other key IT management controls, and thus introduces considerable cost, schedule, and performance risks.

[4]The BEA defines the department's business priorities, the capabilities required to support those priorities, and the combinations of systems and initiatives that enable those capabilities.

- System requirements have not been adequately developed and managed. In particular, basic requirements documentation does not exist to inform program estimates of the costs and schedule needed to accomplish the work associated with delivering predetermined and economically justified system capabilities. In addition, plans and procedures that define how system requirements are to be managed and who is responsible for doing so do not exist. As a result, ongoing system development is not focused on delivering an approved baseline set of capabilities, but rather is reactive to addressing requirements that emerge through the program's change control process. Under this process, users propose changes to the system and these proposals are approved or disapproved by a joint DON and FMS change control board primarily on the basis of consensus about the need for the change and the availability of funds. The result is an inability to develop and measure performance against meaningful cost, schedule, and capability baselines, and thereby reasonably ensure that Navy Cash is meeting expectations, and that those responsible for it are accountable for the results.

- Program risks have not been effectively managed. In particular, plans, processes, and procedures that provide for identifying, mitigating, and disclosing risks do not exist, and risk management roles and responsibilities have not been assigned to key stakeholders. As a result, the program office is not proactively attempting to avoid the occurrence of cost, schedule, and performance problems, but rather is reacting to the consequences of actual problems.

- The security of deployed and operating Navy Cash shipboard devices, applications, and data has not been effectively managed. Specifically, the program office has not (1) fully implemented a comprehensive patch management process; (2) followed an adequate process for planning, implementing, evaluating, and documenting remedial actions for known information security weaknesses; (3) obtained adequate assurance that FMS has effective security controls in place to protect Navy Cash applications and data; and (4) developed an adequate contingency plan and conducted effective contingency plan testing. As a result, the confidentiality, integrity, and availability of deployed and operating Navy Cash shipboard devices, applications, and financial data are at increased risk of being compromised.

- System quality is not being effectively measured because sufficient data for determining trends in unresolved change requests, which is an indicator of a system's stability and for understanding users' satisfaction with the system, are not being collected and used. To the program's credit, it has (1) established a change control board to review and decide whether

to approve requests for changes to the system and (2) conducted a survey to assess the extent to which users are satisfied with the system. However, the program office has not consistently collected and captured the data needed to analyze trends in significant change requests that have not been resolved, such as the dates that the change requests are opened and closed, and the priority of change requests. In addition, the last user survey was conducted 6 years ago and this survey was limited to a prototype version of the system operating on two ships. Without meaningful data in these areas, the quality of the system is not clear.

Program officials acknowledged the above weaknesses and attributed them to, among other things, turnover of staff in key positions and their focus on deploying the system. Further, they stated that addressing these weaknesses has not been a top program priority because Navy Cash has been deployed to and is operating on about 80 percent of the ships. Given that the department still plans to invest an additional $60 million to further develop the program, it is important to treat all the weaknesses that we have identified as priorities.

Accordingly, we are making recommendations to the Secretary of Defense aimed at limiting further investment of modernization funding in Navy Cash to only (1) deployment of already developed and tested capabilities, (2) correction of information security vulnerabilities and weaknesses on ships where it has been deployed and is operating, and (3) development of the basis for deciding whether further development, as planned, is in the department's best interest to pursue. If further investment in development can be justified, then we are recommending that the IT management control weaknesses related to requirements management, risk management, and system quality measurement discussed in this report be considered program management priorities and that they be addressed before significant system development and modernization activities begin.

We received written comments on a draft of this report from both DOD and FMS. In DOD's comments, signed by the Deputy Under Secretary of Defense (Business Transformation) and reprinted in appendix II, the department stated that it concurred with 9 of our 11 recommendations, partially concurred with 1, and non-concurred with the remaining 1.

- In non-concurring with our recommendation for limiting further investment in the program, the department actually concurred with two out of three aspects of the recommendation. Nevertheless, for the aspect of our recommendation aimed at limiting further investment in the program to certain types of spending, it stated that it did not concur with

limiting investment to the exclusion of needed maintenance (e.g., technology refresh) of operational systems. We agree with this comment, as it is consistent with statements in our report, including the recommendation on the report's highlights page and the report's conclusions, which focus on limiting investment of modernization funding only, and not operations and maintenance funding. To avoid any misunderstanding as to our intent, we have clarified our report.

- With respect to our recommendation for optimizing the relationships among DOD's programs that provide smart card technology for electronic retail and banking transactions, the department stated that while it concurs with the overall intent of the recommendation, it believes that the Office of the Under Secretary of Defense (Comptroller) is the appropriate organization to implement it. Since our intent was not to prescribe the only DOD organization that should be responsible for implementing the recommendation, we have slightly modified the recommendation to provide the department flexibility in this regard.

In FMS's comments, signed by the Commissioner and reprinted in appendix III, the service stated that our recommendations will help strengthen the Navy Cash program and that it has begun to address several of our findings and recommendations. Further, it stated that it will work with and support DOD in implementing the recommendations, and consistent with DOD's comments, stated that it did not agree with limiting investment in the program to the exclusion of maintenance of deployed systems. As noted above, this is not the intent of our recommendation, and we have slightly modified the report to avoid any possible confusion as to our intent. Notwithstanding FMS's agreement with our recommendations, it provided additional comments on the findings that underlie several of the recommendations. For various reasons discussed in detail in the agency comments section of this report, we either do not agree with most of these additional comments or do not find most of them to be germane to our findings and recommendations.

Background

DON's primary mission is to organize, train, maintain, and equip combat-ready naval forces capable of winning the global war on terror and any other armed conflict, deterring aggression by would-be foes, preserving freedom of the seas, and promoting peace and security. To support this mission, DON performs a variety of interrelated and interdependent business functions (e.g., acquisition and financial management), relying heavily on IT systems. In fiscal year 2008, DON's IT budget was about $2.7 billion, of which $2.2 billion was allocated to operations and maintenance

of existing systems and the remaining $500 million to systems in development and modernization. Of the approximately 3,000 business systems that DOD reports in its current inventory, DON accounts for 904, or about 30 percent, of the total. The Navy Cash system is one such system investment.

Navy Cash: A Brief Description

In 2001, DON initiated Navy Cash in partnership with Treasury's FMS to enable sailors and marines to use smart cards that store monetary value, also known as stored value cards, to make retail purchases and conduct banking transactions while on ships and ashore. The program builds upon capabilities that have been incrementally introduced from previously deployed systems. (Table 1 summarizes these systems and their capabilities and limitations.)

Table 1: Capabilities and Limitations of Navy Cash Predecessor Systems

System	Year deployed	Capabilities	Limitations
Automated Teller Machines (ATMs)-At-Sea	1988	Localized, shipboard ATMs that received and accounted for a portion of sailors' and marines' paycheck to be available through ATMs. According to DON, this reduced disbursing office workload and provided a more secure means of storing personal funds. This system was replaced by ATMs-at-Sea/Commercial Banking Afloat.	User accounts were limited to a particular ship; no direct access to personal bank accounts ashore.
ATMs-At-Sea/ Commercial Banking Afloat	1996	Sailors and marines had access to ship-based ATM account or personal bank accounts ashore via satellite communication.	Communication link not always available to smaller ships.

Source: GAO analysis of DON data.

According to DOD, Navy Cash's key objectives include introducing workload efficiencies and improving the quality of life for sailors and marines by

- reducing the amount of currency on ships, which lowers costs associated with cash handling activities;
- enabling sailors and marines to conduct ashore banking transactions from ships; and
- enabling sailors and marines to conduct banking or retail transactions while ashore (wherever these branded debit cards are accepted).

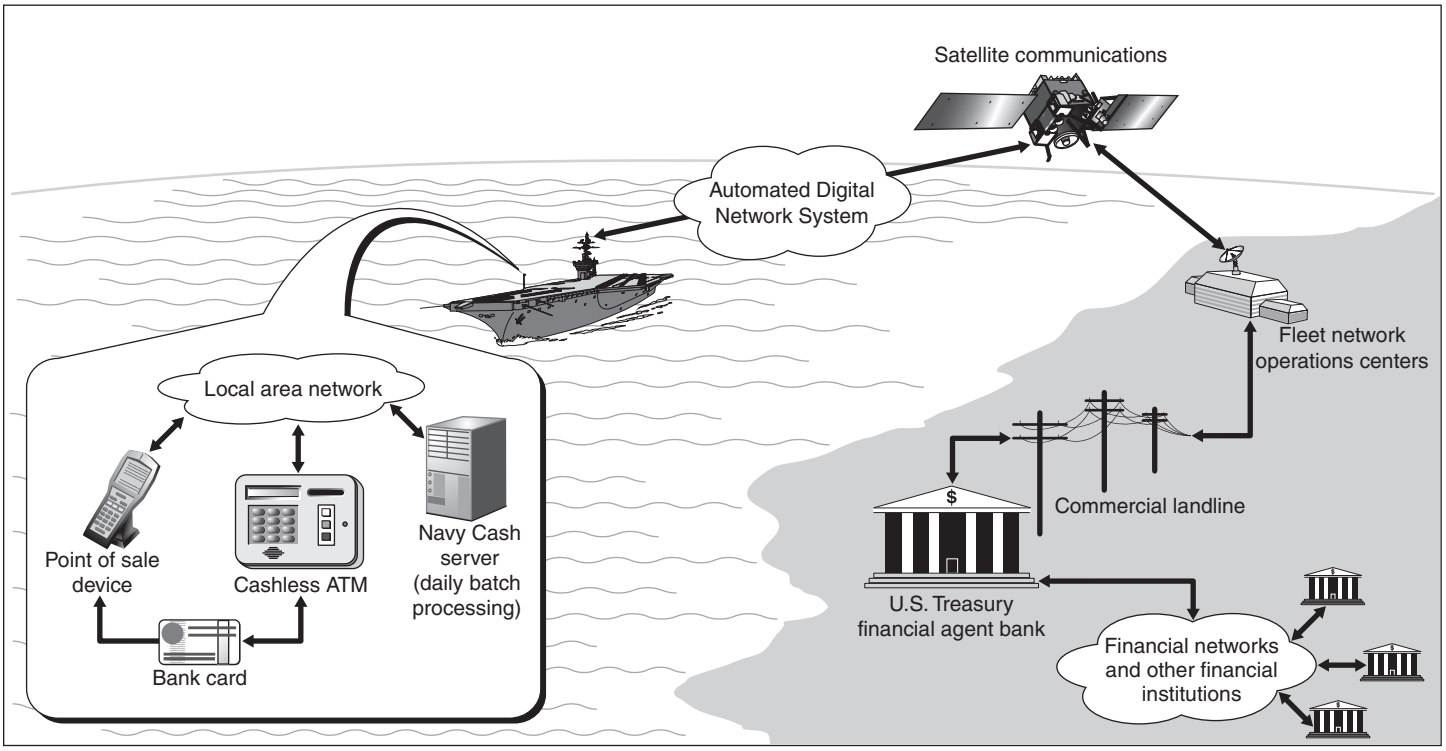
Navy Cash consists of various equipment and devices, including servers that connect to the ship's local area network as well as point-of-sale terminals and ATMs that communicate with Navy Cash smart cards. These cards contain an electronic chip that stores monetary value and interacts with the various devices for conducting electronic retail purchases and personal banking transactions on the ships. On shore, cardholders can access their Navy Cash accounts via ATMs worldwide or conduct retail purchases using the card's magnetic stripe, which provides a debit card feature. According to program officials, while ashore, sailors and marines have access to over 1,000,000 ATMs and 23 million merchants worldwide.

Navy Cash uses a ship's Automated Digital Network System to access satellite communications systems, and then transmits transaction files off the ship through fleet network operations centers to a financial agent (i.e., bank) ashore. To do so, it uses a store-and-forward process[5] to batch transactions together and transmit them off the ship typically during non-peak evening hours. These transactions are then processed in a manner similar to personal check processing through the Automated Clearing House.[6] Figure 1 is a simplified illustration of the Navy Cash network used to transmit these transactions.

[5]The Navy Cash shipboard server stores individual transactions, groups them into a single compressed file, and then transmits the file of daily transactions for processing.

[6]The Automated Clearing House is a network that allows banking institutions to clear, or validate, electronic transactions.

Figure 1: Simplified Diagram of Navy Cash Network



Sources: GAO based on DON data (analysis), ArtExplosion (clipart).

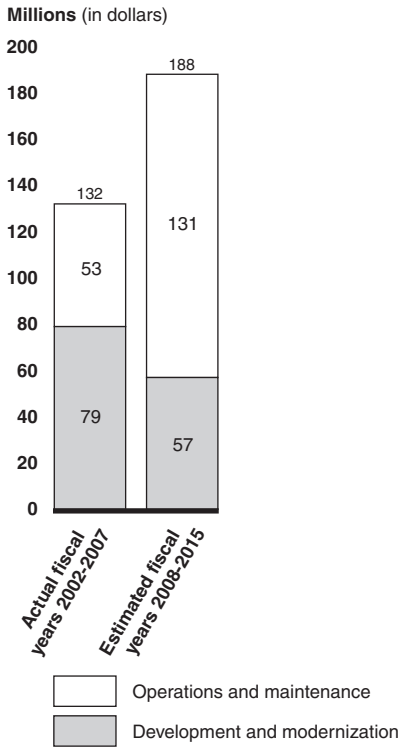
Originally, the program was expected to be fully deployed and reach full operational capability by December 2008 at an estimated cost of about $100 million over a 6-year life cycle.[7] The program office now expects the program to reach full operational capability in fiscal year 2011, and it estimates the program's 14-year life cycle cost[8] to be about $320 million, of which about $100 million is to be funded by FMS. Of the $320 million, about $136 million is for development and modernization, and about $184 million is for operations and maintenance. From fiscal year 2002 to 2007, DON and FMS reported that approximately $132 million has been spent on the program, of which $47 million is FMS's cost. Of the $188 million

[7]This estimate, reported in DON's 2002 economic analysis, did not include FMS's costs for the program.

[8]According to program documentation, Navy Cash has a 14-year expected life. However, program officials stated that this life cycle is being reconsidered and a new life cycle has yet to be established.

expected to be spent (fiscal years 2008-2015), about $57 million is for development and modernization. (See fig. 2 for a breakdown of the actual and planned costs.)

Figure 2: Actual and Estimated Development and Operations and Maintenance Costs for Navy Cash



Source: DON and FMS.

When fully deployed, the program office estimates that Navy Cash could process over $350 million annually in transactions initiated by about 170,000 sailors and marines worldwide on approximately 160 ships. As of April 2008, the program has been deployed to approximately 130 ships.

Navy Cash Oversight and Management Roles and Responsibilities

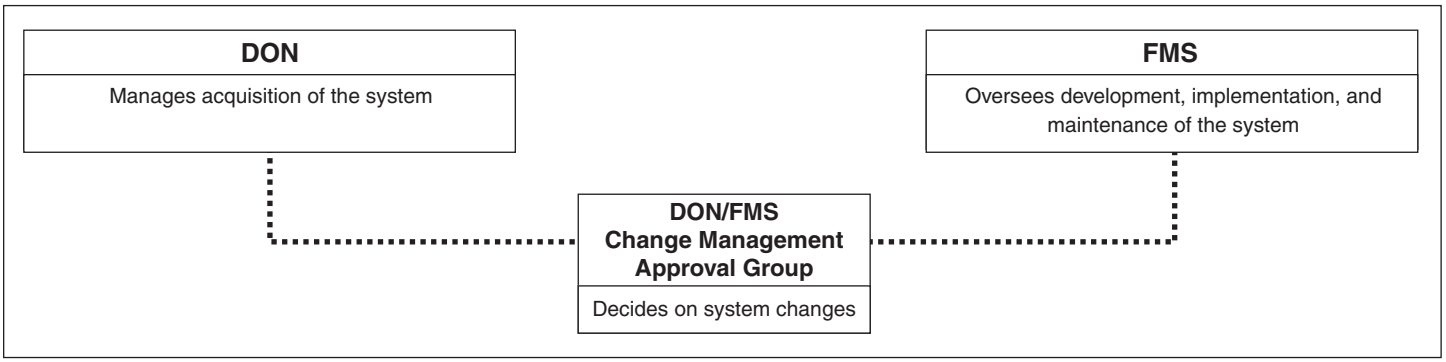
To manage the acquisition and deployment of Navy Cash, DON established a program management office within the Naval Supply Systems Command (NAVSUP).[9] As authorized by statute[10] and because of its experience in developing stored value card programs for other military departments, NAVSUP has partnered with FMS to develop Navy Cash. In February 2001, NAVSUP and FMS signed a memorandum of agreement that, among other things, delineated their respective program roles and responsibilities. According to the agreement, NAVSUP, through the Navy Cash program office, is responsible for managing the acquisition of the program, including managing system requirements and developing program cost and benefit estimates. According to DOD and other relevant guidance, acquisition management includes, among other things, such key IT management control areas as architectural alignment, economic justification, requirements management, risk management, security management, and system quality measurement.

Also according to the agreement, FMS, through a designated financial agent, is to (1) provide for all financial services (i.e., manage the funds distributed through Navy Cash) and (2) develop, test, operate, and maintain the system's software (e.g., terminal and accounting applications) and hardware (e.g., accounting servers, smart cards). In short, the financial agent acts as the depository bank, holding and managing the pool of sailor and marine funds, including accounting for the funds and settling transactions processed. FMS is also responsible for tracking and overseeing the financial agent's provision of services, as defined in a financial agency agreement between FMS and the agent. (See fig. 3 for DON and FMS roles and relationships for Navy Cash.)

[9]NAVSUP is one of five system commands within DON. Its mission includes, among other things, providing DON quality supplies and services on a timely basis.

[10]Financial agent services are authorized under a number of statutes, including but not limited to, 12 U.S.C. § 265 and 12 U.S.C. § 332.

Figure 3: DON and FMS Roles and Relationships for Navy Cash



Source: GAO analysis of DON and FMS data.

In addition, various other organizations share program oversight and review activities. A listing of key entities and their roles and responsibilities can be found in table 2.

Table 2: Organizations Responsible for Navy Cash Oversight and Management

Entity	Roles and responsibilities
DOD Under Secretary of Defense, Comptroller	Serves as the Navy Cash investment review board and performs annual or milestone reviews of the planning, programming, budgeting, and execution processes.
DON Chief Information Officer	Ensures that the program's goals are achievable and executable; conformance to financial management regulations, and DON, DOD, and federal IT policies in several areas (e.g., security, architecture, and investment management); and recommends to the Secretary of DON whether to continue, modify, or terminate IT programs based on its ability to meet these regulations.
NAVSUP (Vice Commander)	Serves as the milestone decision authority, which according to DOD, has overall responsibility for the program, to include approving the program to proceed through its acquisition cycle on the basis of, for example, the life cycle cost-and-benefits estimate, acquisition strategy, and acquisition program baseline.
Navy Cash Program Office	Manages the acquisition by performing activities such as assessing compliance with the DOD's BEA; preparing cost and benefit estimates; developing and managing program requirements; managing program risks; ensuring the confidentiality, integrity, and availability of shipboard devices, applications, and financial data; measuring system quality; and providing infrastructure for installation of system hardware and software.
Treasury, FMS	Manages and oversees the designated financial agent, including holding and accounting for funds distributed throughout the system; developing, implementing, and maintaining the financial software and hardware; and providing life cycle support for the maintenance of the financial software, hardware, and other services, and ensures controls are adequate to protect transactions processed through the designated financial agent's network and equipment and that these controls comply with applicable rules and regulations issued by regulatory and private organizations.[a]

Entity	Roles and responsibilities
Change Management Approval Group	Comprised of representatives from the Navy Cash program office and FMS that jointly review and approve changes to system functionality.
Disbursing Officer	Processes transactions from the ship to the appropriate DON network operations center; produces system related reporting on transactions for accounting purposes; distributes and reports lost or stolen cards; monitors and reports on negative (i.e., insufficient) account balances; maintains shipboard cash reserve; and resolves system-related issues while deployed with assistance from the financial agent.

Source: GAO based on DON and FMS data.

[a]According to FMS, the regulatory organizations include the Office of the Comptroller of the Currency, Federal Reserve Board, and Federal Deposit Insurance Corporation, and the private organizations are the National Automated Clearing House Association, as well as the corporation whose name is branded on the Navy Cash smart card.

Use of IT Management Controls Maximizes Chances for Success

Effective IT management controls are grounded in tried and proven methods, processes, techniques, and activities that organizations define and use to minimize program risks and maximize the chances of a program's success. Using such best practices can result in better outcomes, including cost savings, improved service and product quality, and a better return on investment. For example, two software engineering analyses of nearly 200 systems acquisitions projects indicate that teams using systems acquisition best practices produced cost savings of at least 11 percent over similar projects conducted by teams that did not employ the kind of rigor and discipline embedded in these practices.[11] In addition, our research shows that best practices are a significant factor in successful acquisition outcomes, including increasing the likelihood that programs and projects will be executed within cost and schedule estimates.[12]

We and others have identified and promoted the use of a number of best practices associated with acquiring IT systems.[13] See table 3 for a description of several of these activities.

[11]Donald E. Harter, Mayuram S. Krishnan, and Sandra A. Slaughter, "Effects of Process Maturity on Quality, Cycle Time, and Effort in Software Product Development," *Management Science*, vol. 46, no. 4, 2000; and Bradford K. Clark, "Quantifying the Effects of Process Improvement on Effort," *IEEE Software* (November/December 2000).

[12]GAO, *Information Technology: DOD's Acquisition Policies and Guidance Need to Incorporate Additional Best Practices and Controls*, GAO-04-722 (Washington, D.C.: July 2004).

[13]GAO-04-722.

Table 3: Summary of Business System Acquisition Best Practices

Business practice	Description
Architectural alignment To ensure that the acquisition is consistent with the organization's enterprise architecture.	Architectural alignment is the process for analyzing and verifying that the proposed architecture of the system being acquired is consistent with the enterprise architecture for the organization acquiring the system. Such alignment is needed to ensure that acquired systems can interoperate and are not unnecessarily duplicative of one another.
Economic justification To ensure that system investments have an adequate economic justification.	Economic justification is the process for ensuring that acquisition decisions are based on reliable analyses of the proposed investment's likely costs versus benefits over its useful life as well as an analysis of the risks associated with actually realizing the acquisition's forecasted benefits for its estimated costs. Economic justification is not a one-time event, but rather is performed throughout an acquisition's life cycle in order to permit informed investment decision making.
Requirements management To ensure that requirements are traceable, verifiable, and controlled.	Requirements management is the process for ensuring that the requirements are traceable, verifiable, and controlled. Traceability refers to the ability to follow a requirement from origin to implementation, and is critical to understanding the interconnections and dependencies among the individual requirements, and the impact when a requirement is changed. Requirements management begins when the solicitation's requirements are documented and ends when system responsibility is transferred to the support organization.
Risk management To ensure that risks are identified and systematically mitigated.	Risk management is the process for identifying potential acquisition problems and taking appropriate steps to avoid their becoming actual problems. Risk management occurs early and continuously in the acquisition life cycle.
Security management To protect the confidentiality, integrity, and availability of information and information systems.	Security management is the process for implementing controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. Security management provides for appropriate confidentiality, availability, and integrity of data and information.
System quality measurement To ensure the maturity and stability of system products.	System quality measurement is the process for understanding the maturity and stability of the system products being developed, operated, and maintained so that problems can be identified and addressed early, therefore limiting their overall impact on program cost and schedule. One indicator of system quality is the volume and significance of system defect reports and change proposals.

Source: GAO.

Prior GAO Reviews Have Identified IT Management Control Weaknesses on DOD Business System Investments

We have previously reported[14] that DOD has not effectively managed a number of business system investments. Among other things, our reviews of individual system investments have identified weaknesses in such things as architectural alignment and informed investment decision making, which are also the focus areas of the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005[15] business system provisions. Our reviews have also identified weaknesses in other system acquisition and investment management areas—such as economic justification, requirements management, and risk management.

Recently, for example, we reported that the Army's approach for investing about $5 billion over the next several years in its General Fund Enterprise Business System, Global Combat Support System-Army Field/Tactical,[16] and Logistics Modernization Program did not include alignment with Army enterprise architecture or use of a portfolio-based business system investment review process.[17] Moreover, we reported that the Army did not have reliable processes, such as an independent verification and validation function, or analyses, such as economic analyses, to support its management of these programs. We concluded that until the Army adopts a business system investment management approach that provides for reviewing groups of systems and making enterprise decisions on how these groups will collectively interoperate to provide a desired capability, it runs the risk of investing significant resources in business systems that do not provide the desired functionality and efficiency. Accordingly, we made recommendations aimed at improving the department's efforts to achieve total asset visibility and enhancing its efforts to improve its

[14]See, for example, GAO, *DOD Business Transformation: Lack of an Integrated Strategy Puts the Army's Asset Visibility System Investments at Risk*, GAO-07-860 (Washington, D.C.: July 27, 2007); GAO, *Information Technology: DOD Needs to Ensure That Navy Marine Corps Intranet Program Is Meeting Goals and Satisfying Customers*, GAO-07-51 (Washington, D.C.: Dec. 8, 2006); GAO, *Defense Travel System: Reported Savings Questionable and Implementation Challenges Remain*, GAO-06-980 (Washington, D.C.: Sept. 26, 2006); GAO, *DOD Systems Modernization: Uncertain Joint Use and Marginal Expected Value of Military Asset Deployment System Warrant Reassessment of Planned Investment*, GAO-06-171 (Washington, D.C.: Dec. 15, 2005); and GAO, *DOD Systems Modernization: Planned Investment in the Navy Tactical Command Support System Needs to Be Reassessed*, GAO-06-215 (Washington, D.C.: Dec. 5, 2005).

[15]Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, Pub. L. No. 108-375, § 332 (2004) (codified at 10 U.S.C. §§ 186 and 2222).

[16]Field/tactical refers to Army units that are deployable to locations around the world, such as Iraq or Afghanistan.

[17]GAO-07-860.

control and accountability over business system investments. The department agreed with our recommendations.

We also reported that DON had not, among other things, economically justified its ongoing and planned investment in the Naval Tactical Command Support System (NTCSS)[18] and had not invested in NTCSS within the context of a well-defined DOD or DON enterprise architecture. In addition, we reported that DON had not effectively performed key measurement, reporting, budgeting, and oversight activities, and had not adequately conducted requirements management and testing activities. We concluded that without this information, DON could not determine whether NTCSS as defined, and as being developed, is the right solution to meet its strategic business and technological needs. Accordingly, we recommended that the department develop the analytical basis to determine if continued investment in NTCSS represents prudent use of limited resources and to strengthen management of the program, conditional upon a decision to proceed with further investment in the program. The department largely agreed with these recommendations.

In addition, we reported that the Army had not defined and developed its Transportation Coordinators' Automated Information for Movements System II—a joint services system with the goal of helping to manage the movement of forces and equipment within the United States and abroad—in the context of a DOD enterprise architecture.[19] We also reported that the Army had not economically justified the program on the basis of reliable estimates of life cycle costs and benefits and had not effectively implemented risk management. As a result, we concluded that the Army did not know if its investment in this program, as planned, is warranted or represents a prudent use of limited DOD resources. Accordingly, we recommended that DOD, among other things, develop the analytical basis needed to determine if continued investment in this program, as planned, represents prudent use of limited defense resources. In response, the department largely agreed with our recommendations, and has since reduced the program's scope by canceling planned investments.

[18]GAO-06-215.

[19]GAO-06-171.

Key IT Management Controls Have Not Been Effectively Implemented on Navy Cash

DOD acquisition policies and related federal guidance provide a framework within which to manage system investments, like Navy Cash. Effective implementation of this framework can minimize program risks and better ensure that system investments are defined in a way to optimally support mission operations and performance, as well as deliver promised system capabilities and benefits on time and within budget. Thus far, key IT management controls associated with this framework have not been implemented on Navy Cash. In particular, the program's overlap with and duplication of other DOD programs has not been assessed, and the program has not been economically justified on the basis of reliable estimates of life cycle costs and benefits. As a result, the program, as defined, has not been shown to be the most cost-effective investment option.

Even if investment in the proposed Navy Cash solution is shown to be a wise and prudent course of action, the manner in which Navy Cash is being acquired and deployed is not adequate because (1) requirements have not been adequately developed and managed; (2) program risks have not been effectively managed; (3) security has not been effectively managed; and (4) system quality has not been adequately measured. As a result, the system will likely experience performance shortfalls and cost more and take longer to implement and maintain than necessary.

Program officials acknowledged these weaknesses and attributed them to, among other things, turnover of staff in key positions and their focus on deploying the system. Further, they stated that addressing these weaknesses has not been a top program priority because Navy Cash has been deployed to and is operating on about 80 percent of the ships. Nevertheless, about $60 million in development and modernization funding remains to be spent on this program. As a result, it is important that all these weaknesses be addressed to reduce the risk of delivering a system solution that falls short of expectations.

Key Controls for Justifying Planned Investment in Navy Cash Have Not Been Effectively Implemented

Investment in the proposed Navy Cash solution has not been adequately justified. Specifically, the system solution has not been assessed relative to other DOD programs that employ smart cards for electronic retail transactions. Moreover, it has not been economically justified on the basis of reliable estimates of cost and benefits over the system's expected life. As a result, planned investment in the system, as defined, may not be a cost-effective course of action.

Navy Cash Duplication with Other DOD Programs Has Not Been Assessed

DOD's acquisition policies and guidance,[20] as well as federal and best practice guidance,[21] recognize the importance of investing in business systems within the context of an enterprise architecture.[22] Moreover, the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005[23] requires that defense business systems be compliant with the federated BEA.[24] Our research and experience in reviewing federal agencies show that making investments without the context of a well-

[20]Department of Defense Directive Number 5000.1 and Department of Defense Architecture Framework, Version 1.0, Volume 1 (February 2004).

[21]Clinger-Cohen Act of 1996, 40 U.S.C. § 11315(b)(2); E-Government Act of 2002, Public Law No. 107-347 (Dec. 17, 2002); GAO, *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management (Version 1.1)*, GAO-03-584G (Washington, D.C.: April 2003); Chief Information Officer Council, *A Practical Guide to Federal Enterprise Architecture, Version 1.0* (February 2001); and Institute of Electrical and Electronics Engineers, Standard for Recommended Practice for Architectural Description of Software-Intensive Systems 1471-2000 (Sept. 21, 2000).

[22]A well-defined enterprise architecture provides a clear and comprehensive picture of an entity, whether it is an organization (e.g., a federal department) or a functional or mission area that cuts across more than one organization (e.g., personnel management). This picture consists of snapshots of both the enterprise's current or "As Is" environment and its target or "To Be" environment, as well as a capital investment road map for transitioning from the current to the target environment. These snapshots consist of integrated "views," which are one or more architecture products that describe, for example, the enterprise's business processes and rules; information needs and flows among functions, supporting systems, services, and applications; and data and technical standards and structures.

[23]Pub. L. No. 108-375, § 332 (2004) (codified at 10 U.S.C. §§ 186 and 2222).

[24]DOD has adopted a federated approach for developing its business mission area enterprise architecture, which includes the corporate BEA representing the thin layer of DOD-wide corporate architectural policies, capabilities, rules, and standards; component architectures (e.g., DON enterprise architecture); and program architectures (e.g., Navy Cash architecture).

defined enterprise architecture often results in systems that are, among other things, duplicative of other systems.[25]

Navy Cash has not been assessed and defined in a way to ensure that it is not duplicative of the Eagle Cash and EZpay programs, both of which provide for the use of smart card technology for electronic retail transactions in support of the Air Force and the Army.[26] Within DOD, the means for avoiding business system duplication and overlap is the department's process for assessing compliance with the DOD BEA and its associated investment review and decision making processes. In 2005, 2006, and 2007, Navy Cash was evaluated for compliance with the BEA. However, the BEA does not contain business activities[27] that Navy Cash supports. According to officials from DOD's Business Transformation Agency, which is responsible for DOD's BEA, these business activities are not included nor are they planned for inclusion in the BEA, because the capabilities provided by Navy Cash relate strictly to personal banking, which is outside of the current scope of the BEA. As a result, compliance could not be assessed beyond concluding that Navy Cash was compliant because it did not conflict with the BEA. Moreover, even if the BEA included the business activities that Navy Cash supports, the program's ability to assess BEA compliance would have been limited because the program office did not develop a complete set of system-level architecture products needed to perform a meaningful compliance assessment. Thus, Navy Cash's potential overlap and duplication with similar programs is not sufficiently understood.

[25]See, for example, GAO, *Information Technology: FBI Is Taking Steps to Develop an Enterprise Architecture, but Much Remains to Be Accomplished*, GAO-05-363 (Washington, D.C.: Sept. 9, 2005); GAO, *Homeland Security: Efforts Under Way to Develop Enterprise Architecture, but Much Work Remains*, GAO-04-777 (Washington, D.C.: Aug. 6, 2004); GAO, *Information Technology: Architecture Needed to Guide NASA's Financial Management Modernization*, GAO-04-43 (Washington, D.C.: Nov. 21, 2003); GAO, *DOD Business Systems Modernization: Important Progress Made to Develop Business Enterprise Architecture, but Much Work Remains*, GAO-03-1018 (Washington, D.C.: Sept. 19, 2003*);* GAO, *Information Technology: DLA Should Strengthen Business Systems Modernization Architecture and Investment Activities*, GAO-01-631 (Washington, D.C.: June 29, 2001); and GAO, *Information Technology: INS Needs to Better Manage the Development of Its Enterprise Architecture*, GAO/AIMD-00-212 (Washington, D.C.: Aug. 1, 2000).

[26]These programs are deployed and in operation, and they preceded deployment of the Navy Cash program.

[27]Business or operational activities are tasks normally conducted in the course of achieving a mission or a business goal. The BEA describes business or operational activities relevant to specific aspects of the business mission areas, such as financial visibility.

According to program officials, Navy Cash is not duplicative of Eagle Cash and EZpay because it is designed to operate on ships at sea, which do not maintain constant network connectivity with on shore networks. Therefore, they said that it requires different communications and financial transaction capabilities than the other two stored value card programs. We agree that there are important differences between the programs. However, they all perform chip-based financial transactions, and thus opportunities may exist for them to provide or reuse shared system services, as well as to merge into a DOD-wide stored value card program. According to program officials, overlap and duplication among the programs was not assessed. This means that aspects of Navy Cash could be potentially duplicative of these other programs, and thus DOD may not be pursuing the most cost-effective solution to meet its mission needs. In this regard, the program's Milestone Decision Authority told us that the differences between Navy Cash and other stored value card programs are minimal and stated that officials with the three stored value card programs have recently begun discussions with FMS on how to collaborate and possibly move towards one system solution.

Navy Cash Has Not Been Economically Justified

Investment in Navy Cash has not been economically justified on the basis of a reliable analysis of estimated system costs and expected benefits over the life of the program. Specifically, according to the latest economic analysis, the program is expected to produce estimated benefits of about $133 million for an estimated cost of about $100 million. However, the cost estimate is not reliable, because the program's 2002 economic analysis is 6 years old and is based on a cost estimate of about $100 million that was not derived in accordance with effective estimating practices, such as including all costs over the system's life cycle, and adjusting the estimate to account for program risks and material program changes. Further, this economic analysis did not comply with applicable federal guidance.[28] For example, it did not adequately consider all relevant alternatives, and it erroneously counted $40 million as cost savings rather than transfers[29] (i.e., shift of control over spending of resources from one group to another that do not result in an economic gain). Further, the economic analysis has

[28]Office of Management and Budget, *Guidelines and Discount Rates for Benefits-Cost Analysis of Federal Programs*, Circular A-94 (Washington, D.C.: Oct. 29, 1992); *Planning, Budgeting, Acquisition and Management of Capital Assets*, Circular A-11, Part 7 (Washington, D.C.: June 26, 2008).

[29]Transfers represent shifts of control over resource allocation from one group to another that do not result in economic gains. Rather, the benefits to the group that receives the transfer are offset by the costs borne by the group that provides the transfer.

yet to be validated using actual data on the accrual of benefits. Without an economic analysis that is reliable, DON's ongoing and planned investment in Navy Cash lacks justification as a cost-effective course of action.

Economic Analysis Used a Cost Estimate That Omits Relevant Costs and Was Not Derived Using Key Estimating Practices

A reliable cost estimate is an essential element for informed investment decision making, realistic budget formulation and program resourcing, meaningful progress measurement, proactive course correction, and accountability for results. According to the Office of Management and Budget (OMB),[30] programs must maintain current and well-documented estimates of program costs, and these estimates must span the full expected life of the program. Without reliable estimates, programs cannot be adequately justified on the basis of reliable costs and benefits and they are at increased risk of experiencing cost overruns, missed deadlines, and performance shortfalls.

Our research has identified a number of best practices for effective program cost estimating, and we have issued guidance that associates these practices with four characteristics of a reliable cost estimate.[31] Specifically, estimates need to be:

- *Comprehensive*: The cost estimates should include both government and financial agent costs over the program's full life cycle, from the inception of the program through design, development, deployment, and operation and maintenance to retirement. They should also provide a level of detail appropriate to ensure that cost elements are neither omitted nor double counted, and include documentation of all cost-influencing ground rules and assumptions.

- *Well-documented*: The cost estimates should have clearly-defined purposes, and be supported by documented descriptions of key program

[30]OMB, Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, (Washington, D.C.: Executive Office of the President, June 2006); Circular No. A-130 Revised, *Management of Federal Information Resources*, (Washington, D.C.: Executive Office of the President, Nov. 28, 2000); and *Capital Programming Guide: Supplement to Circular A-11, Part 7: Planning, Budgeting, and Acquisition of Capital Assets*, (Washington, D.C.: Executive Office of the President, June 2006).

[31]GAO, *Cost Assessment Guide: Best Practices for Estimating and Managing Program Costs*, Exposure Draft, GAO-07-1134SP (Washington, D.C.: July 2007).

or system characteristics (e.g., relationships with other systems, performance parameters). Additionally, they should capture in writing such things as the source data used and their significance, the calculations performed and their results, and the rationale for choosing a particular estimating method or reference. Moreover, this information should be captured in such a way that the data used to derive the estimate can be traced back to, and verified against, their sources.

- *Accurate*: The cost estimates should provide for results that are unbiased and not be overly conservative or optimistic (i.e., should represent the most likely costs). In addition, the estimates should be updated regularly to reflect material changes in the program, and steps should be taken to minimize mathematical mistakes and their significance. The estimates should also be grounded in a historical record of cost estimating and actual experiences on comparable programs.

- *Credible*: The cost estimates should discuss any limitations in the analysis performed that are due to uncertainty or biases surrounding data or assumptions. Further, the estimates' derivation should provide for varying any major assumptions and recalculating outcomes based on sensitivity analyses, and the estimates' associated risks and inherent uncertainty should be disclosed. Also, the estimates should be verified based on cross-checks using other estimating methods.

The $100 million life cycle cost estimate, as documented in the program's 6-year old economic analysis, does not reflect many of the practices associated with a reliable cost estimate, including several practices related to being comprehensive and well documented, and all related to being accurate and credible (see table 4).

Table 4: Summary of Cost-Estimating Characteristics That the Cost Estimate Satisfies

Characteristic of reliable estimates	Satisfied? [a]
Comprehensive	Partially
Well-documented	Partially
Accurate	No
Credible	No

Source: GAO analysis of DON data.

[a]"Yes" means that the program office provided documentation demonstrating satisfaction of the criterion. "Partially" means that the program office provided documentation demonstrating satisfaction of part of the criterion. "No" means that the program office has yet to provide documentation demonstrating satisfaction of the criterion.

The cost estimate of about $100 million, as documented in the program's 2002 economic analysis, does not meet all of the practices related to being comprehensive. Specifically, it only includes costs from fiscal years 2003 through 2008 (6-year period), and it does not include both the government and financial agent costs associated with development, acquisition (non-development), implementation, and operations and support over the system's life cycle. Moreover, it does not include FMS's portion of the program's cost, which is estimated to be about $100 million over a 14-year period. In addition, the cost estimate does not clearly describe how the various cost sub-elements are aggregated to produce the amounts associated with the two documented cost categories, system installation costs, and operations and maintenance costs. Therefore, it is not clear that all pertinent costs are included and no costs are double counted. Lastly, although some key assumptions have been identified, such as the ship implementation schedule, other key assumptions, such as labor rates and inflation rates, are not. As a result, the estimate cannot be considered comprehensive.

The cost estimate used in the economic analysis also addresses some, but not all, of the practices related to being well-documented. Specifically, the purpose of the cost estimate was clearly defined and a technical baseline has been documented that includes, among others things, the hardware and software specifications and planned performance parameters. However, the calculations used to derive the cost estimate, including descriptions of the methodologies used and traceability back to source data (e.g., vendor quotes, salary data), are not documented. In addition, while program officials described the estimating approach used, such as using market research and historical data to determine the costs associated with hardware, software, and installations, they did not have documentation of the methodology used to arrive at the total costs of each of these elements and how they were combined to produce the overall cost estimate. Therefore, the program's cost estimate cannot be considered well-documented.

In addition, the $100 million documented cost estimate lacks accuracy because it does not reflect an assessment of the costs most likely to be incurred. Specifically, this estimate covers only 6 years of costs (fiscal years 2003 through 2008). In contrast, the program's current cost estimate is about $320 million over a 14-year life cycle, and according to program officials, the program's life cycle is being reexamined and will likely be extended.

Lastly, the $100 million cost estimate is not credible because a complete uncertainty analysis (i.e., both a sensitivity analysis and a Monte Carlo simulation[32]) was not performed on this estimate. A sensitivity analysis reveals how the cost estimate is affected by a change in a single assumption or cost driver, such as the ship installation schedule, while holding all other parameters constant. A Monte Carlo simulation assesses the aggregate variability of the cost estimate to determine a confidence range around the estimate. Without such analyses of uncertainty, the program office cannot have confidence that the program can be completed within the cost estimate.

Program officials acknowledged the limitations in the estimate, and attributed them to turnover of staff and their current focus on deploying the system. Nevertheless, program officials stated that they intend to develop a revised cost estimate when they update the program's economic analysis, but they had yet to establish a date for accomplishing this. Given that a significant amount of development and modernization funding remains to be invested on the program, it is important that the program office economically justify such investment.

Economic Analysis Does Not Satisfy Other Relevant Guidance

According to OMB,[33] economic analyses should meet certain criteria to be considered reasonable, such as comparing alternatives on the basis of net present value and conducting an uncertainty analysis of benefits.

The program's December 2002 economic analysis meets one, does not meet four, and partially meets two of the seven OMB criteria governing how to perform such analyses. For example, while the analysis explained why the investment is needed, it did not consider the costs and benefits associated with at least three alternatives to the status quo, such as Eagle Cash, EZpay, or some derivative that provided for reuse of shared services among the programs. Moreover, at least three alternatives to the status quo were not assessed on the basis of net present value, using the proper discount rate to account for inflation. Instead, the analysis only

[32]A risk analysis can be accomplished by the use of a Monte Carlo simulation, which involves the use of random numbers and probability distributions to examine random outcomes.

[33]OMB, *Guidelines and Discount Rates for Benefits-Cost Analysis of Federal Programs*, Circular A-94 (Washington, D.C.: Oct. 29, 1992); *Planning, Budgeting, Acquisition and Management of Capital Assets*, Circular A-11, Part 7 (Washington, D.C.: June 26, 2008).

qualitatively evaluated Navy Cash against its predecessor systems. For example, the analysis included evaluation of the capabilities and limitations of the predecessor systems, but did not include evaluating the relative cost and benefits of any alternatives to Navy Cash.

In addition, the program's benefit projections erroneously counted about $40 million in cost transfers as cost savings, thus overstating projected benefits (i.e., projected benefits should only be $93 million). Transfers represent shifts of control over the spending of resources from one group to another and thus do not result in an economic gain. According to OMB guidance, transfers do not produce economic gains because the benefits to those government entities that receive such a transfer are the same as the costs borne by those government entities that provide the transfer.[34] Moreover, no uncertainty analysis was performed on the benefit estimates. (See table 5 for the results of our analyses relative to each of the seven criteria.)

Table 5: Satisfaction of OMB Economic Analysis Criteria

Criteria	Explanation	Satisfied?[a]	GAO analysis
The cost-benefit analysis should clearly explain why the investment was needed.	The analysis should clearly explain the reason why the status quo is unacceptable.	Yes	The economic analysis explained why the status quo was not viable.
At least three alternatives to the status quo should be considered.	At least three meaningful alternatives to the status quo should be examined to help ensure that the alternative chosen was not preselected.	No	Only one meaningful alternative to the status quo (i.e., Navy Cash) was considered. In addition, the predecessor systems were not examined on the basis of their cost and benefits. Rather, they were examined only in terms of their functional characteristics.
The general rationale for the cost-benefit analysis, including at least three alternatives, should be discussed.	The general rationale for the cost-benefit analysis, including at least three alternatives that are being considered, should be discussed to enable reviewers of the analysis to understand the context for the alternative selected.	Partially	The general rationale for the cost-benefit analysis was discussed, but it did not include the rationale for at least three alternatives.
The quality of the benefits to be realized from each alternative should be reasonable.	The quality of the benefit estimate for each alternative should be complete and reasonable for a net present value to be calculable and accurate.	No	The benefits estimate was not reasonable in that it included $40 million of transfers.

[34]OMB Circular No. A-94, § 6(a)(4).

Criteria	Explanation	Satisfied?[a]	GAO analysis
At least three alternatives should be compared on the basis of net present value.	The net present value should be calculated because it consistently allows for the selection of the alternative with the greatest benefit net of cost.	Partially	An estimate of the present value of cost savings or avoidances net of costs was computed for Navy Cash, but at least three alternatives were not compared on the basis of net present value.
The proper discount rate for calculating each alternative's net present value should be used.	OMB provides specific guidance on the choice of discount rate for evaluating projects whose benefits and costs will be distributed over time.	No	The proper discount rate was not used for calculating net present value. Specifically, a discount rate of 4.65 percent should have been used compared to the discount rate of 2 percent used by the program.
A complete uncertainty analysis of the benefits should be included.	Estimates of benefits are typically uncertain because of imprecision in both underlying data and modeling assumptions. Because such uncertainty is basic to virtually any cost-benefit analysis, its effects should be analyzed and reported.	No	An uncertainty analysis of the program's estimated benefits was not included.

Source: OMB guidance and GAO analysis of DON data.

[a]"Yes" means that the program office provided documentation demonstrating satisfaction of the criterion. "Partially" means that the program office provided documentation demonstrating satisfaction of part of the criterion. "No" means that the program office has yet to provide documentation demonstrating satisfaction of the criterion.

Program officials stated that they do not know why the economic analysis was not developed in accordance with OMB guidance. They also stated that they intend to update the economic analysis and, in doing so, intend to address OMB guidance. However, they did not have a date for accomplishing this because their priority is deploying the system.

Actual Accrual of Estimated Benefits Has Not Been Validated

The Clinger-Cohen Act of 1996 and OMB guidance[35] emphasize the need to develop information to ensure that IT investments are actually contributing to tangible, observable improvements in mission performance. DOD guidance[36] also states that estimated benefits should be validated to ensure that desired outcomes are being achieved. To this end, agencies should define and collect metrics to determine whether expected

[35]Clinger-Cohen Act of 1996, 40 U.S.C. sections 11101-11704, and OMB, Circular No. A-130, *Management of Federal Information Resources* (Nov. 30, 2000).

[36]DOD, *Defense Acquisition Guidebook*, Version 1.0 (Oct. 17, 2004).

benefits from a given investment are being accrued, and they should modify subsequent economic analyses to reflect the lessons learned.

Despite the fact that Navy Cash has been installed and is operating on approximately 130 ships, DON has yet to determine whether the system is actually producing expected benefits. For example, the 2002 economic analysis stated that Navy Cash would reduce cash on ships, and contribute to man-hour savings as a result of increased productivity. It also stated that it would improve quality-of-life for sailors and marines. While DON has measured the reduction in the cash onboard some ships where Navy Cash is operating, this reduction represents a transfer and is not an actual benefit. Moreover, the extent to which the system is achieving expected man-hour savings, which would constitute a true benefit, has not been measured. Lastly, customer (sailor and marine) satisfaction with the system, which is a legitimate qualitative benefit, has not been determined since a prototype of Navy Cash was installed on two ships in 2001.

Program officials stated that DON's Manpower Analysis Center[37] is responsible for measuring man-hour savings. Further, they said that customer satisfaction with the system was being measured through informal feedback from the sailors and marines, and they recently began a more formal customer satisfaction survey. They also stated that in updating the economic analysis, they plan to assess and reflect the accrual of actual benefits. However, they had not established a date for accomplishing this.

Key Controls for Ensuring That Defined Navy Cash Capabilities Are Delivered on Time and Within Budget Have Not Been Effectively Implemented

DOD policy and related guidance recognizes the importance of implementing a range of management controls associated with ensuring that IT investments are defined, developed, deployed, and operated efficiently and effectively.[38] By implementing these controls, the chances of delivering systems that perform as intended, and not costing more or taking longer than necessary, are increased. These controls include requirements development and management, risk management, security

[37]This center is responsible for, among other things, manpower analysis and work studies as directed by the Chief of Naval Operations.

[38]For example, see DOD, Department of Defense Directive Number 5000.1, *The Defense Acquisition System* (May 12, 2003); Department of Defense Instruction Number 5000.2, *Operation of the Defense Acquisition System* (May 12, 2003); *Defense Acquisition Guidebook*, Version 1.0 (Oct. 17, 2004); and Software Engineering Institute, *CMMI for Acquisition, Version 1.2*, CMU/SEI-2007-TR-017 (Pittsburgh, Pa.: November 2007).

management, and system quality measurement. For Navy Cash, none of these controls have been effectively implemented. Specifically,

- program requirements have not been adequately developed and managed;
- program risks have not been effectively managed;
- security has not been adequately managed; and
- data needed to measure two aspects of system quality—trends in unresolved change requests and evaluation of user satisfaction with the system—have not been collected and used.

As a result, Navy Cash is unlikely to perform in a manner that meets user and operational needs, and it is likely to cost more and take longer than necessary.

Navy Cash Requirements Have Not Been Adequately Developed and Managed

Well-defined and managed requirements are recognized by DOD guidance and relevant best practices as essential, and can be viewed as a cornerstone of effective system acquisition.[39] Effective requirements development and management includes (1) developing detailed system requirements; (2) establishing policies and plans for managing changes to requirements, including defining roles and responsibilities, and identifying how the integrity of a baseline set of requirements will be maintained; and (3) maintaining bi-directional requirements traceability, meaning that system-level requirements can be traced both backward to higher level business or operational requirements, and forward to system design specifications and test plans.

The program office has not satisfied these three aspects of effective requirements development and management. Specifically,

- The program office has not developed system-level requirements for Navy Cash. System-level requirements are derived from higher-level operational requirements and are specified at a level of detail needed for system developers to design and build to. Without system requirements, the ability of the program office to understand the impact of any system change requests (i.e., cost, schedule, and performance) and thus make informed

[39]DOD, *Defense Acquisition Guidebook*, Version 1.0 (Oct. 17, 2004). Software Engineering Institute, *Software Acquisition Capability Maturity Model® (SA-CMM®) version 1.03*, CMU/SEI-2002-TR-010 (Pittsburgh, Pa.: March 2002).

decisions about such changes, is limited. For example, although the program office identified a high-level requirement for the system to share information with the Retail Operations Management system used in ships' store operations, the associated system-level requirements were not defined. As a result, the deployed version of the system was not designed and developed to provide this interface. The requirement for this interface was later realized after a number of system and operational problems surfaced. Addressing these problems through a series of changes required additional time and funding. Program officials acknowledged that more effective requirements development and management practices could have avoided these problems. As another example, a system requirement for automatically deploying software patches to operational systems was not defined. Had this requirement been defined, the system design could have provided for developing a capability to minimize the level of effort required to identify, distribute, and install patches. Instead, a less efficient and labor-intensive manual process has been used.

- The program office does not have a policy or plans for managing requirements. Such policies and plans establish organizational roles and responsibilities for managing requirements, including maintaining and controlling modifications or changes to the baseline sets of requirements, establishing priorities among competing requests for changes, and assessing the impact on cost, schedule, and performance of each change. In lieu of a policy or plans, the program office has established an ad hoc change control process, whereby change proposals are approved or disapproved by a joint DON and FMS change control board based on a change management policy that was drafted in 2003. However, this policy was never finalized or approved and does not define roles and responsibilities or how requirements will be managed. Further, the board has not been chartered. Moreover, program officials told us that the board's decisions are made primarily on the basis of consensus about the need for the change and the availability of funds.

- Other than security requirements, Navy Cash requirements cannot be traced from the higher level business or operational requirements to system design specifications and test plans. Specifically, we attempted to trace a sample of Navy Cash system-level requirements backward to high-level requirements and forward to design documents and test plans and results. However, as noted above, no system-level requirements exist. Without this link in the requirements traceability chain, traceability could not be demonstrated. Having requirements traceability is essential for ensuring that developed and deployed system products satisfy operational needs and user expectations. In the case of Navy Cash, where system capabilities are reactive to change requests rather than proactively driven

by requirements, such traceability is also essential to understanding the impact to the system of each change request and thus having an informed basis for approving and prioritizing any changes.

Program officials acknowledged these weaknesses and recently stated that they intend to address them. To accomplish this, they reported that they have hired a new employee who is to be trained in requirements development and management, and who is to develop a requirements management plan.

Until the program office employs fundamental requirements development and management practices, it cannot reliably estimate the program costs and develop schedules needed to accomplish the work associated with delivering predetermined and economically justified system capabilities. The result is an inability to develop and measure performance against meaningful cost, schedule, and capability baselines, and thereby reasonably ensure that the program is meeting expectations and those responsible for it are accountable for results.

Navy Cash's Risks Have Not Been Effectively Managed

Proactively managing program risks is a key acquisition management control that, if done properly, can increase the chances of programs delivering promised capabilities and benefits on time and within budget. For Navy Cash, program risks have not been effectively managed. Rather, the program office has reacted to the realization of actual problems. In particular, plans, processes, and procedures are not in place that provide for identifying, controlling, and disclosing risks, and risk management roles and responsibilities have not been assigned to key stakeholders. As a result, the program office is not positioned to proactively avoid the occurrence of cost, schedule, and performance problems.

DOD and related guidance[40] recognize the importance of performing effective risk management on programs like Navy Cash. Among other things, effective risk management includes: (1) establishing and implementing a written plan and defined process for risk identification, analysis, and mitigation; (2) assigning responsibility for managing risks to key stakeholders; (3) encouraging program-wide participation in risk

[40]DOD, *Risk Management Guide for DOD Acquisition, 6th Edition, Version 1.0*, http://www.acq.osd.mil/sse/ed/docs/2006-RM-Guide-4Aug06-final-version.pdf (accessed Mar. 13, 2008) and Software Engineering Institute, *CMMI for Acquisition, Version 1.2*, CMU/SEI-2007-TR-017 (Pittsburgh, Pa.: November 2007).

management; and (4) examining the status of identified risks during program milestone reviews.

The program office has not fully satisfied any of the above cited risk management practices. For example:

- A written plan or defined process that provides for identifying, analyzing, and mitigating risks has not been established. In the absence of a plan and process, program officials stated that risks are informally addressed during bi-monthly program management reviews that involve key stakeholders, including the program office, FMS, and the financial agent. However, our analysis of minutes of these reviews indicates that they are more focused on reacting to the consequences of actual problems, rather than proactively attempting to avoid the occurrence of potential problems.

- While program officials stated that responsibility for managing risks rests with the program manager, roles and responsibilities for managing and identifying risks have not been documented for any key stakeholders, including individuals in the program office, and with FMS and the financial agent. Without clearly documenting their roles and responsibilities, proactive identification, disclosure, and mitigation of all key risks is unlikely to occur, and program approval and decision making authorities will not be adequately informed.

- While program officials stated that attending and participating in program management reviews is encouraged, we have yet to receive any verifiable evidence that risks are addressed in these reviews or that involvement in risk management is encouraged.

- Program officials have yet to provide any verifiable evidence that program decision making and oversight authorities have been apprised of the status of identified risks.

Program officials acknowledged the above weaknesses and attributed them to staff turnover in key positions and their focus on deploying the system rather than establishing management processes and procedures. Nevertheless, program officials stated that they intend to develop a risk plan and process, but said that this would not occur until December 2008. Given that a significant amount of development and modernization investment remains, it is important that mitigating existing risks, including those discussed in this report, as well as future risks be treated as a program priority.

Navy Cash Security Management Has Not Been Effectively Implemented

A number of Navy Cash security management weaknesses exist. Specifically, the program office has not (1) fully implemented a comprehensive patch management process; (2) followed an adequate process for planning, implementing, evaluating, and documenting remedial actions for known information security weaknesses; (3) obtained adequate assurance that FMS has effective security controls in place to protect Navy Cash applications and data; and (4) developed an adequate contingency plan and conducted effective contingency plan testing. Program officials acknowledged these weaknesses but have yet to provide us with plans for addressing them. As a result, the confidentiality, integrity, and availability of deployed and operating Navy Cash shipboard devices, applications, and financial data are at increased risk of being compromised.

Patch Management Has Not Been Fully Implemented

DOD guidance[41] states that component organizations should develop a process for patching system vulnerabilities. Further, National Institute of Standards and Technology (NIST) guidance[42] recognizes the importance of implementing comprehensive patch management that includes, among other things, (1) having a complete inventory of system hardware and software assets, (2) automatically deploying vulnerability patches, and (3) measuring patch management performance.

Although the program office performs patch management for Navy Cash, key practices have not been fully implemented. Specifically,

- A complete inventory of system assets does not exist. According to NIST, a system inventory enables organizations to monitor system hardware and software assets for the presence of all threats, vulnerabilities, and patches. While the financial agent maintains a Navy Cash asset database for the 128 ships on which the system is operating, this database is missing 3 hardware inventories and 19 software inventories. According to program officials, the financial agent's database is incomplete because it was created from purchase orders after the system was in operation. Furthermore, although the program office maintains hardware inventories for each ship in a DON configuration management database, the office does not maintain inventories of Navy Cash software. Until the program

[41]CJCSM 6510.01, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)*, CH 3 8 Mar 06.

[42]National Institute of Standards and Technology, *Creating a Patch and Vulnerability Management Program*, Special Publication 800-40 (November 2005).

office develops a complete inventory of Navy Cash system assets, it will not be able to identify and patch all system threats and vulnerabilities.

- Vulnerability patches are not deployed in an automated or timely manner. According to NIST guidance, deploying patches automatically minimizes the level of effort and time required to identify, distribute, and install patches. However, patches are currently deployed manually for Navy Cash when ships are in port for maintenance. As a result, the risk of vulnerabilities being exploited before ships return to port is increased. Although the program office plans to introduce the capability to automatically deploy patches as part of the next software release in the first quarter of fiscal year 2009, program officials said that it will take between 18 to 24 months to rollout this capability to the entire fleet. Program officials also stated that they do not know why this capability was not part of the original system requirements and design. Until the program office begins automatically deploying patches, Navy Cash assets and data will be exposed to increased risk.

- The performance of patch management is not being measured. NIST guidance recommends consistent measurement of the effectiveness of patch management through the use of metrics, such as susceptibility to attack and mitigation response time. Although program officials stated that they maintain patch management metrics, they have yet to provide us with a description of the metrics or an explanation of how they are used. Until the program office develops and uses performance metrics, it will not be able to assess and improve the effectiveness of its patch management effort.

To strengthen its patch management efforts, the program office has developed a vulnerability management guide. However, this guide has not been finalized and approved, and according to program officials, it does not follow NIST patch management guidance. Without comprehensive patch management, increased risk exists that system vulnerabilities could be exploited.

Remedial Action Plans Have Not Been Documented

The Federal Information Security Management Act (FISMA)[43] requires that agencies' information security programs must include a process for

[43]FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency. OMB has outlined steps for documenting remedial actions—referred to by OMB as a plan of action and milestones—for systems where IT security weaknesses have been identified. Additionally, NIST guidance[44] states that a plan of action and milestones should be included in a system's accreditation package and describe how the information system owner intends to address those vulnerabilities by reducing, eliminating, or accepting the identified vulnerabilities.

Since the system was accredited in November 2006, the program office has not developed any plans of action and milestones, even though medium and low information security risks were identified during security test and evaluation efforts supporting the certification and accreditation. According to program officials, the risks were accepted by the designated approving authority, rather than corrected, because they involve features that are necessary for the system to operate, such as having certain hardware interfaces and access permissions. While accepting rather than correcting such weaknesses is consistent with DON guidance[45] for developing plans of action and milestones, it is not consistent with NIST guidance. Specifically, DON guidance states that these plans are only required for accreditation decisions that are conditional upon corrective actions being taken. However, NIST guidance specifies that the development of a plan of action and milestones should include instances where risk is being accepted.

The lack of plans of action and milestones means that the program office has not adequately addressed information security risks. Moreover, the limitations in DON guidance mean that other Navy programs may not have done so as well. Until the program office fully implements a remedial action process that meets the FISMA requirements and OMB and NIST guidance, program management and oversight officials will not have

[44]NIST, *Guide for the Security Certification and Accreditation of Federal Information Systems*, Special Publication 800-37 (May 2004).

[45]This guidance for a comprehensive plan of action and milestones was distributed by the Navy Operational Designated Approving Authority, within the Naval Network Warfare Command, which is DON's central operational authority for information technology requirements, network and information operations in support of naval forces afloat and ashore. This command is responsible for granting Navy Cash its authority to operate.

sufficient assurance that all security weaknesses are being reported and tracked, and that options for addressing them are fully considered.

Information Security Requirements Have Not Been Fully Defined

FISMA requires each federal agency to develop, document, and implement an agencywide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Among other things, this includes testing system management, operational, and technical security controls. Although the program office has partnered with FMS to develop and support the operation of Navy Cash, it is ultimately responsible for ensuring the security of Navy Cash systems and data.

The program office has not taken adequate steps to ensure that security controls are tested. Specifically, the memorandum of agreement between the program office and FMS does not establish requirements for FMS and the financial agent relative to periodic information security control reviews, including reviews of applicable management, operational, and technical controls, and to provide DON with copies of information security control reviews that are performed on the Navy Cash system and its supporting infrastructure. This is important because FMS—through its financial agent[46]—provides services that support Navy Cash that must be secure, such as holding and accounting for funds distributed throughout the system and processing transactions. Although FMS has performed some management and operational control tests, such as periodic personnel and physical security assessments of selected commercial facilities that provide services and support to Navy Cash, these assessments were not designed to evaluate the technical controls of the system's computing environment because the memorandum of agreement does not include such requirements.

Until the program office and FMS establish information security requirements for overseeing the financial agent's technical information security controls, an increased risk exists that the confidentiality, integrity, and availability of information stored, transmitted, and processed by the financial agent can be compromised.

[46]Financial agent services are authorized under a number of statutes, including but not limited to, 12 U.S.C. § 265 and 12 U.S.C. § 332.

Contingency Plan Is Missing Key Elements

OMB guidance[47] requires agencies to develop contingency plans and to test those plans at least annually. NIST guidance states that contingency plans should include a sequence of recovery activities, which describe system priorities based on business impact and notification procedures, which describe the methods used to notify personnel with recovery responsibilities.[48] In addition, according to NIST, contingency plan tests should include explicit test objectives and success criteria for each planned activity and related procedure and documentation of lessons learned.

Although the program office has developed contingency plans for Navy Cash, it did not identify the sequence of recovery activities and notification procedures for recovery personnel in them. The sequence of activities should prioritize the recovery of system components by criticality and the notification procedures should describe the methods used to notify recovery personnel during business and non-business hours. Until the program office includes these areas in the contingency plans, it cannot ensure that system components will restore in a logical manner and that ship recovery personnel will be notified promptly when a system disruption is detected. In addition, while the program office has largely included explicit test objectives and success criteria in all the test procedures, they did not document the lessons learned. According to NIST, lessons learned can improve contingency plan effectiveness and this should be incorporated into the plan. According to program officials, NIST was not used for developing and conducting tests of the contingency plan. Without lessons learned, the program office will not be able to properly maintain and improve the contingency planning guide.

Until DON develops sufficient contingency plans and testing procedures, increased risk exists that Navy Cash systems, data, and operations will not be able to fully recover from a disruption or disaster.

[47]Circular No. A-130; and OMB, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, OMB Memoranda M-07-19, July 25, 2007.

[48]NIST, *Contingency Planning Guide for Information Technology Systems*, *Special Publication 800-34* (June 2002).

Navy Cash Quality Measures Are Not Being Collected

Effective management of programs like Navy Cash depends in part on the ability to measure the quality of the system being acquired and operated.[49] One measure of system quality is the trend in the number of unaddressed, high-priority system change requests.

Sufficient data to measure trends in open (i.e., unresolved) system change requests, which is a recognized indicator of a system's stability and quality are not being collected. To the program's credit, it has formed a group consisting of program office, FMS, and financial agent representatives to review and decide whether to approve requests for changes to the system. However, this group is not consistently collecting data as to when a change request is opened or closed and what the priority level of each change request is. Thus, it does not know at any given time, for example, how many change requests are pending, the significance of pending change requests, and the age of these change requests. Program officials acknowledged these weaknesses but stated that their focus has been on deploying the system. This means that the program office cannot know and disclose to DOD decision makers whether the system's stability and maturity are moving in the right direction.

In addition, the program office has not consistently collected data on user and operator satisfaction with the system. Specifically, the program office conducted two surveys in the last 6 years—a user satisfaction survey and a shipboard merchant satisfaction survey—but neither of these surveys is meaningful. More specifically, the user satisfaction survey was done in 2002 and thus is dated; and it covered only two ships and a prototype version of Navy Cash and thus its scope is limited. In addition, neither survey produced a response rate that can be generalized and projected (about 50 percent and 20 percent for the two ships in the user survey, and about 30 percent for the merchant survey).

Program officials stated that they have relied on informal user feedback from disbursing officers, who have indicated overall satisfaction with the system. Nevertheless, they said that a survey of users and operators is being planned and expected to be completed by the fall of 2008. Without meaningful data about Navy Cash's stability and the satisfaction of those who use it, it is not clear Navy Cash is a quality system.

[49]IEEE Std 12207-2008, *Systems and software engineering – Software life cycle processes*, (Piscataway, N.J.: 2008).

Conclusions

Navy Cash's potential duplication of other DOD programs that perform similar functions, combined with its lack of meaningful economic justification, together mean that the department does not have an adequate basis for knowing whether Navy Cash, as defined, is the most cost-effective solution to meeting its strategic business and technological needs. Because such a basis is absolutely fundamental to informed investment decision making, a compelling case exists for the department to reevaluate current plans for investing almost $60 million of additional modernization funding to further develop the system.

Even if reevaluation supports current or modified investment plans, the manner in which the program is being executed remains a source of considerable cost, schedule, and performance risk. In particular, without employing fundamental requirements development and management practices, the department cannot reliably estimate program costs and develop schedules needed to accomplish the work associated with delivering predetermined and economically justified system capabilities. In addition, without effective risk management, the department is not positioned to proactively avoid the occurrence of cost, schedule, and performance problems. Furthermore, the lack of adequate security management puts the confidentiality, integrity, and availability of deployed and operating Navy Cash shipboard devices, applications, and financial data at increased risk of being compromised. Moreover, without meaningful data about the Navy Cash's stability and the satisfaction of those who use it, it is not clear that Navy Cash is a quality system.

To overcome each of these weaknesses, it is important to not only acknowledge them, which the program office has done, but to also treat them as program priorities, including developing and implementing plans for addressing them, which the program office has largely not done.

Recommendations

Because of the uncertainty surrounding whether Navy Cash, as defined, represents a cost-effective solution, we recommend that the Secretary of Defense direct the Secretary of the Navy to limit further investment of modernization funding in the program to only (1) deployment to remaining ships of already developed and tested capabilities; (2) correction of information security vulnerabilities and weaknesses on ships where it is deployed and operating; and (3) development of the basis for an informed decision as to whether further development and modernization is economically justified and in the department's collective best interests.

To develop the basis for an informed decision about further Navy Cash development, we further recommend that the Secretary of Defense, direct the appropriate DOD organizations to (1) examine the relationships among DOD's programs for delivering military personnel with smart card technology for electronic retail and banking transactions; (2) identify, in coordination with the respective program offices, alternatives for optimizing the relationships of these programs in a way that minimizes areas of duplication, maximizes reuse of shared services across the programs, and considers opportunities for a consolidated stored value card program across the military services; and (3) share the results with the appropriate organizations for use in making an informed decision about planned investment in Navy Cash.

To further develop this basis for an informed decision about Navy Cash development, we also recommend that the Secretary of Defense direct the Secretary of the Navy to ensure that the appropriate Navy organizational entities prepare a reliable economic analysis that encompasses the program's total life cycle costs, including those of FMS, and that (1) addresses cost-estimating best practices and complies with relevant OMB cost-benefit guidance and (2) incorporates data on whether deployed Navy Cash capabilities are actually producing benefits.

To address Navy Cash information security management weaknesses and improve the operational security of the system, we recommend that the Secretary of Defense direct the Secretary of the Navy to ensure that the Navy Cash program manager, in collaboration with the appropriate organizations, take the following five actions:

- Develop and implement a patch management approach based on NIST guidance, which includes a complete Navy Cash systems inventory; an automated patch deployment capability; and a patch management performance vulnerability measurement capability, including metrics for susceptibility to attack and mitigation response time.

- Institute a process to plan, implement, evaluate, and document remedial actions for deficiencies in Navy Cash information security policies, procedures, and practices, and ensure that this process meets FISMA requirements, as well as applicable OMB and NIST guidance.

- Update the NAVSUP/FMS memorandum of agreement, in collaboration with FMS, to establish specific security requirements for FMS and the financial agent to periodically perform information security control reviews, including applicable management, operational, and technical

controls, of the Navy Cash system, and to provide NAVSUP with copies of the results of these reviews that pertain to the Navy Cash system and its supporting infrastructure.

- Develop a complete contingency plan to include a (1) sequence of recovery activities and (2) procedures for notifying ship personnel with contingency plan responsibilities to begin recovery activities; and to test the contingency plan in accordance with NIST guidance, including documenting lessons learned from testing.

To address DON information security guidance limitations, we also recommend that the Secretary of Defense direct the Secretary of the Navy to ensure that the Navy Operational Designated Approving Authority, as part of the Naval Network Warfare Command, updates its certification and accreditation guidance to require the development of plans of action and milestones for all above identified security weaknesses.

If further investment in development of Navy Cash can be justified, we then recommend that the Secretary of Defense direct the Secretary of the Navy, through the appropriate chain of command, to ensure that the Navy Cash program manager takes the following actions.

- With respect to requirements development and management, (1) develop detailed system requirements; (2) establish policies and plans for managing changes to requirements, including defining roles and responsibilities, and identifying how the integrity of a baseline set of requirements will be maintained; and (3) maintain bi-directional requirements traceability.

- With respect to risk management, (1) establish and implement a written plan and defined process for risk identification, analysis, and mitigation; (2) assign responsibility for managing risk to key stakeholders; (3) encourage program-wide participation in risk management; (4) include and track the risks discussed in this report as part of a risk inventory; and (5) apprise decision making and oversight authorities of the status of risks identified during program reviews.

- With respect to system quality measurement, collect and use sufficient data for (1) determining trends in unresolved change requests and (2) understanding users' satisfaction with the system.

Agency Comments and Our Evaluation

Both DOD and FMS provided written comments on a draft of this report. In DOD's comments, signed by the Deputy Under Secretary of Defense (Business Transformation) and reprinted in appendix II, the department stated that it concurred with 9 of our 11 recommendations, partially concurred with 1, and non-concurred with the remaining 1. In non-concurring with our recommendation for limiting further investment in the program, the department actually concurred with two out of three aspects of the recommendation. Nevertheless, for the aspect of our recommendation aimed at limiting further investment in the program to certain types of spending, it stated that it did not concur with limiting investment to the exclusion of needed maintenance (e.g., technology refresh) of operational systems. We agree with this comment, as it is consistent with statements in our report, including the recommendation summary on the report's highlights page and the report's conclusions, both of which focus on limiting investment of modernization funding only, and not operations and maintenance funding. To avoid any misunderstanding as to our intent, we clarified our report.

With respect to our recommendation for optimizing the relationships among DOD's programs that provide smart card technology for electronic retail and banking transactions, the department stated that, while it concurs with the overall intent of the recommendation, it believes that the Office of the Under Secretary of Defense (Comptroller) is the appropriate organization to implement it. Since our intent was not to prescribe the only DOD organization that should be responsible for implementing the recommendation, we have slightly modified the recommendation to provide the department flexibility in this regard.

Notwithstanding DOD's considerable agreement with our recommendations, the department provided additional comments on the findings that underlie several of the recommendations, which it described as needed to clarify and avoid confusion about the program. For various reasons discussed below, we either do not agree with most of these additional comments or do not find them germane to our findings and recommendations.

- First, the department stated that the report's overall findings understate the program's discipline and conformance with applicable guidance and best practices. We do not agree. Our review extended to six key acquisition control areas, all of which are reflected in DOD's own acquisition policies as well as other federal guidance. Effective implementation of these controls can minimize program risks and better ensure that system investments are defined in a way to optimally support

mission operations and performance, as well as deliver promised system capabilities and benefits on time and within budget. However, we found that none of these key IT management controls were being effectively implemented on Navy Cash, and the department agreed with our recommendations aimed at correcting this.

- Second, the department stated that the report's findings do not accurately capture the program's maturity since the system has been deployed to over 80 percent of its user base. While we do not question the extent to which the system has been deployed to date, and in fact state in our report that the system has been deployed to about 80 percent of the fleet, we do not agree that the program is mature, as evidence by the numerous IT management control weaknesses that we found and the fact that about $60 million in modernization funding remains to be spent on the system.

- Third, the department stated that it recognizes that some security management limitations exist, but added that these limitations do not pose a serious risk to the confidentiality, integrity, or availability of the deployed system, and that our report may cause cardholders to become unnecessarily concerned. We do not agree that these limitations do not pose a serious risk. Our report details a number of serious security management weaknesses relative to both DOD and NIST guidance, such as not following an adequate process for planning, implementing, evaluating and documenting remedial actions for known information security vulnerabilities, as well as not obtaining adequate assurance that FMS has effective security controls in place to protect Navy Cash applications and data. As a result, we appropriately conclude in our report that such failures to effectively manage Navy Cash security places the confidentiality, integrity, and availability of deployed and operating shipboard devices, applications, and financial data at increased risk of being compromised. Swift implementation of our recommendations is the best solution to alleviating any cardholder concerns that may arise from these weaknesses.

  In FMS's comments, signed by the Commissioner of FMS and reprinted in appendix III, the service stated that our recommendations will help strengthen Navy Cash and that it has begun addressing our findings and recommendations. In addition, it stated that it will support DOD in implementing the recommendations, and consistent with DOD, commented that it did not agree with one part of one of our recommendations, adding that limiting investment in Navy Cash beyond fielding and maintaining already tested system capabilities would place future operations at risk. As stated above, this recommendation is focused on limiting further investment in modernization funding, not operations

and maintenance funding. To avoid any confusion about this, we have added language to other parts of the report to emphasize this focus.

In addition to the above, and notwithstanding its overall agreement with our recommendations, FMS provided other comments relative to several of the findings that underlie our recommendations.[50] As discussed below, we either do not agree with these additional comments or do not find them to be germane to our findings and recommendations.

- First, FMS stated that our report does not identify a security breach, loss of cardholder or government funds, unauthorized release of personal or other sensitive information, or any other compromise of system integrity. We agree that our report does not identify these things, as the scope of work was not intended to identify them. Rather, our scope focused on the program's implementation of key security management controls outlined in DOD and NIST guidance. In this regard, we found serious information security management control weaknesses and concluded that these weaknesses increased the risk to the confidentiality, integrity, and availability of information stored, transmitted, and processed by the financial agent.

- Second, FMS stated that the issue of whether Navy Cash is duplicative of other similar DOD smart card programs was addressed before Navy Cash was initiated in 2001, when DON and FMS determined that for technical and cost reasons it could not alter the other DOD programs to meet Navy Cash requirements. We do not find this comment relevant to our recommendation because our point is not that one of the other DOD programs should be altered and used in place of Navy Cash. Rather, our point is that these smart card programs need to be looked at collectively to decide whether it is in the department's best interest to continue investing in separate smart card programs or to invest in a single department-wide solution. This point is consistent with FMS's stated goal of having a single smart card for DOD.

- Third, FMS stated that it disagreed with our finding that the Navy Cash benefits projection erroneously counted $40 million as cost savings rather than cost transfers, adding that this value represents not merely a transfer between agencies but actual savings to the United States. While we do not

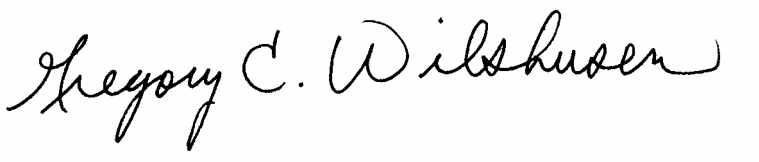
[50]We did not assess the assertion by FMS that Navy Cash funds constitute public money and thus must be held in the Treasury or in an account held by a Treasury designated financial agent.

disagree that this interest savings represents a benefit to the United States government, it also represents a cost—interest foregone—to holders of Treasury debt. Therefore, the interest savings represents a transfer rather than savings from one member or sector to another.

We are sending copies of this report to interested congressional committees; the Director, Office of Management and Budget; the Congressional Budget Office; the Secretary of Defense; the Secretary of the Treasury; and the Department of Defense Office of the Inspector General. We also will make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site http://www.gao.gov.

If you or your staffs have any questions on matters discussed in this report, please contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov, or Gregory C. Wilshusen at (202) 512-3789 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.

Randolph C. Hite
Director
Information Technology Architecture and Systems Issues



Gregory C. Wilshusen
Director
Information Security Issues

Appendix I: Objective, Scope, and Methodology

Our objective was to determine whether the Department of the Navy (DON) is effectively implementing information technology management controls on Navy Cash. We selected Navy Cash primarily because the Department of Defense's (DOD) inventory of DON systems identified the program as one of DON's five largest development and modernization investments. To address the objective, we focused on the following management areas (1) architectural alignment; (2) economic justification; (3) requirements development and management; (4) risk management; (5) security management; and (6) system quality measurement. In doing so, we analyzed a range of program documentation, such as the acquisition strategy, business case, economic analysis, agreements between the partnering organizations, and interviewed cognizant officials, such as the Milestone Decision Authority, program manager, and Financial Management Service (FMS) and financial agent officials responsible for Navy Cash.

To address architectural alignment, we reviewed the program's business enterprise architecture (BEA) compliance assessments and system architecture products as well as versions 4.0, 4.1, and 5.0 of the BEA and compared them to the BEA compliance requirements described in the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005[1] and DOD's BEA compliance guidance and evaluated the extent to which the compliance assessments addressed all relevant BEA products. We also reviewed DOD guidance for program architecture development, such as DOD's Business Transformation Guidance, and compared Navy Cash's program architecture development activities to this guidance. In addition, we interviewed Navy Cash and FMS officials, as well as Navy Cash's Milestone Decision Authority, and requested related documentation on the potential duplication between Navy Cash and other DOD programs that involve the use of smart card functionality, such as the Air Force's and Army's Eagle Cash and EZpay programs.

To address the program's economic justification, we reviewed the latest economic analysis to determine the basis for the cost and benefit estimates. This included evaluating the analysis against Office of

[1]Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, Pub. L. No. 108-375, § 332 (2004) (codified at 10 U.S.C. §§ 186 and 2222).

Management and Budget guidance and GAO's Cost Assessment Guide.[2] In addition, we interviewed cognizant program officials, including the Navy Cash program manager and FMS, regarding their respective roles, responsibilities, and actual efforts in developing and/or reviewing the economic analysis and the extent to which measures and metrics showed that projected benefits in the economic analysis were actually being realized. We also interviewed cognizant officials such as the Milestone Decision Authority about the purpose and use of the program's economic analysis for managing the investment in the Navy Cash program.

To address requirements development and management, we reviewed relevant program documentation, such as the concept of operations document, and interviewed relevant program officials and evaluated this information against relevant best practices.[3] We also reviewed interface requirements documents, minutes of program management meetings, and traceability of security requirements. In addition, we interviewed program officials involved in the requirements management process to discuss the change control process they use and their roles and responsibilities for managing requirements.

To address risk management, we reviewed relevant risk management documentation, such as program management review meeting minutes and compared the program office's activities with DOD's risk management guidance[4] and related best practices.[5] We analyzed the effectiveness of the program's management reviews in terms of managing risks. In doing so, we interviewed cognizant program officials responsible, such as the program manager, Milestone Decision Authority, and FMS officials to discuss their roles and responsibilities and obtain clarification on the

[2]Office of Management and Budget, *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs*, Circular No. A-94 (Oct. 29, 1992); *Planning, Budgeting, Acquisition and Management of Capital Assets*, Circular A-11, Part 7 (Washington, D.C.: June 26, 2008); GAO, *Cost Assessment Guide:* "*Best Practices for Estimating and Managing Program Costs*," 2007 exposure draft.

[3]Software Engineering Institute, *Software Acquisition Capability Maturity Model® (SA-CMM®)*, version 1.03, CMU/SEI-2002-TR-010 (Pittsburgh, Pa.: March 2002).

[4]DOD, *Risk Management Guide for DOD Acquisition, 6th Edition, Version 1.0*, http://www.acq.osd.mil/sse/ed/docs/2006-RM-Guide-4Aug06-final-version.pdf (accessed Mar. 13, 2008).

[5]Software Engineering Institute, *CMMI for Acquisition, Version 1.2*, CMU/SEI-2007-TR-017 (Pittsburgh, Pa.: November 2007).

program's approach to managing risks associated with acquiring and implementing Navy Cash.

To address security management, we reviewed relevant security documentation, such as DOD and National Institute of Standards and Technology information security guidance, and the Navy Cash afloat and ashore system security authorization agreements. In addition, we observed the system in operation aboard the USS Theodore Roosevelt and discussed security issues with ship personnel, program office, FMS, and financial agent officials. We also reviewed USS Harry S. Truman contingency plan test results. Additionally, we reviewed a database used to maintain the inventory of Navy Cash hardware and software assets as a part of our analysis on the Navy Cash vulnerability management program. Furthermore, we interviewed cognizant DON, FMS, and financial agent officials to discuss their roles and responsibilities and obtain clarification on the program's approach to protecting the confidentiality, integrity, and availability of Navy Cash systems and information.

To address system quality measurement, we reviewed program documentation, such as change request logs, and a plan of action and milestones for change requests. We also compared the program's data collection and analysis practices relative to these areas to program guidance and best practices.[6] We reviewed the plans for and results of surveys that were performed on user and shipboard merchant satisfaction with Navy Cash, and we interviewed program management and technical officials.

We conducted our work at DOD offices and program office and ship facilities in the Washington, D.C. metropolitan area, Norfolk, Virginia, and Mechanicsburg, Pennsylvania, between June 2007 and September 2008, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient,

[6]GAO, *Year 2000 Computing Crisis: A Testing Guide*, GAO/AIMD-10.1.21 (Washington, D.C.: November 1998); and IEEE Std 12207-2008, *Systems and software engineering – Software life cycle processes* (Piscataway, N.J.: 2008).

appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Comments from the Department of Defense

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION
TECHNOLOGY
AND LOGISTICS

AUG 2 7 2008

Mr. Randolph C. Hite
Director, Information Technology Architecture and Systems Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Hite:

This is the Department of Defense (DoD) response to the GAO draft report GAO-08-922, "DOD BUSINESS SYSTEMS MODERNIZATION: Planned Investment in Navy Program to Create Cashless Shipboard Environment Needs to Be Justified and Better Managed," dated July 18, 2008 (GAO Code 310660). Detailed comments on the recommendations are enclosed.

The Department concurs with nine of the recommendations and partially concurs with one recommendation and non-concurs with one recommendation. The Department also believes that the overall findings of the report understate the level of discipline and conformance with applicable guidance and best business practices. Additionally, the report's findings do not accurately capture the maturity of the program since the system has been deployed to over 80 percent of the planned user base. Finally, the Department would like to note that development of the system has been a simple, low cost adaptation of a system made up of primarily commercial-off-the-shelf products.

With regard to GAO's first recommendation, although the Department concurs that an updated economic analysis is needed to decide "as to whether further development and modernization is economically justified and in the department's collective best interests," the Department intends to avoid any significant disruption of afloat disbursing operations to ensure that the warfighters continue to have access to their pay. Navy Cash must remain operational while corrective actions to address GAO's recommendations are underway. The earliest installed systems are nearing the end of their expected operational life due to aging hardware and technology obsolescence. These must be replaced through a planned technical refresh, in order to maintain already developed and tested capabilities.

Information technology management controls continue to be a top priority throughout the entire DoD as we modernize our business systems. As the Department continues to move forward, we appreciate the GAO's input in our on-going business systems modernization efforts.

Sincerely,

Paul A. Brinkley
Deputy Under Secretary of Defense
(Business Transformation)

Enclosure:
As stated

GAO DRAFT REPORT DATED JULY 18, 2008
GAO-08-922 (GAO CODE 310660)

"DOD BUSINESS SYSTEMS MODERNIZATION: PLANNED INVESTMENT IN NAVY PROGRAM TO CREATE CASHLESS SHIPBOARD ENVIRONMENT NEEDS TO BE JUSTIFIED AND BETTER MANAGED

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy to limit further investment in the program to only: (1) deployment to remaining ships of already developed and tested capabilities; (2) correction of information security vulnerabilities and weaknesses on ships where it is deployed and operating; and (3) development of the basis for an informed decision as to whether further development and modernization is economically justified and in the department's collective best interests.

DOD RESPONSE: Non-Concur. The Department concurs with the recommendation to reduce system vulnerabilities and to update the economic justification. However, the Department non-concurs that the Navy limit its investment in the program to solely those activities listed in the recommendation. Some investment beyond the parameters suggested by GAO is needed to maintain the current system to ensure that afloat disbursing operations continue and that the warfighter continues to have access to their pay. Instead, the Navy will limit its investment in the program to fielding and maintaining already tested capabilities and selection and testing of technology refresh hardware, which is required to maintain the already developed and tested capabilities.

The Navy Cash Program Office will complete the economic justification and address the report's other recommendations prior to making the investment in the technology refresh hardware that is currently planned to be delivered to the Fleet in Fiscal Year (FY) 2010.

Today, most Navy Cash system updates (including Information Assurance Vulnerability Management (IAVM) updates) are fielded through ship maintenance actions. A new software release which will automate Information Assurance Vulnerability (IAV) updates to Navy Cash servers and report compliance to the Navy Cash program is in the accreditation process. Currently, IAV patches are supported during ships grooms or by having shipboard Information Technology (IT) personnel support the Navy Cash servers with updates.

Target completion date for these corrective actions is September 30, 2009.

Attachment
Page 1 of 7

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense, through the appropriate chain of command, direct the Director of the DoD Business Transformation Agency, to: (1) examine the relationships among DoD's programs for delivering military personnel with smart card technology for electronic retail and banking transactions; (2) identify, in coordination with the respective program offices, alternatives for optimizing the relationships of these programs in a way that minimizes areas of duplication, maximizes reuse of shared services across the programs, and considers opportunities for a consolidated stored value card program across the military services; and (3) share the results with the appropriate organizations for use in making an informed decision about planned investment in Navy Cash.

DOD RESPONSE: Partially Concur. The Department concurs with the overall intent of the recommendation, but believes that the appropriate organization within DoD is the Office of the Under Secretary of Defense (Comptroller) (OUSD(C)). OUSD(C) is responsible for cash disbursement to Sailors and Marines across the globe as well as reconciling the Department's fund balance with the Treasury. As such, OUSD(C), utilizing the Investment Review Board (IRB) structure, will task a functional team to work with the Navy Cash Program Office and other program offices within DoD as appropriate to examine the relationships among DoD's programs for delivering military personnel smart card technology for electronic retail and banking transactions. OUSD(C) will identify alternatives, if any, for optimizing those relationships and will present those alternatives to the DoD Financial Management IRB and Defense Business Systems Management Committee (DBSMC) upon completion of the analysis.

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy to ensure that the appropriate Navy organizational entities prepare a reliable economic analysis that encompasses the program's total life cycle costs, including those of Department of the Treasury, Financial Management Service (FMS) and that: (1) addresses cost-estimating best practices and complies with relevant OMB cost benefit guidance; and (2) incorporates data on whether deployed Navy Cash capabilities are actually producing benefits.

DOD RESPONSE: Concur. In 2006, the Navy Cash Program Office did a high level review of Navy Cash to determine if system capabilities were producing anticipated benefits. The Program Office learned that ships overwhelmingly exceeded the expected goal of carrying less cash, which was a major goal of the system and central to the economic analysis.

The Navy Cash Program Office will develop a comprehensive and reliable economic analysis in compliance with relevant Office of Management and Budget (OMB) cost benefit guidance prior to technology refresh hardware procurement for installation on ships.

Target completion date for developing this economic analysis is September 30, 2009.

Attachment
Page 2 of 7

RECOMMENDATION 4: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy to ensure that the Navy Cash program manager, in collaboration with the appropriate organizations develop and implement a patch management approach based on National Institute of Standards and Technology (NIST) guidance, which includes a complete Navy Cash systems inventory; an automated patch deployment capability; and a patch management performance vulnerability measurement capability, including metrics for susceptibility to attack and mitigation response time.

DOD RESPONSE: Concur. The Navy Cash program is in the process of resubmitting an updated certification package to the Naval Network Warfare Command (NNWC), which is the program's Designated Approving Authority, to ensure that the Navy Cash revised patch management procedures comply with all current security directives.

The next planned release, which is already going through the accreditation process, includes an automated patch deployment capability. As part of configuration management, the program office will work with stakeholders to consolidate our existing tracking tools into a single systems inventory to track the deployment of automated patches, and measure the patch management performance vulnerability, in accordance with NIST Standards. Completion for system accreditation and tracking tool development will be in FY 2009.

Target completion date for completing our corrective actions is March 31, 2009.

RECOMMENDATION 5: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy to ensure that the Navy Cash program manager, in collaboration with the appropriate organizations institute a process to plan, implement, evaluate, and document remedial actions for deficiencies in Navy Cash information security policies, procedures and practices, and ensure that this process meets Financial Information Security Management Act (FISMA) requirements, as well as applicable OMB and NIST guidance.

DOD RESPONSE: Concur. To address GAO's recommendation, the program office in conjunction with its stakeholders will finalize the draft Information Assurance Vulnerability Management Guide and accompanying IAVM Coordinator Standard Operating Procedure to include documenting remedial actions for deficiencies in the Navy Cash system in the System Level IT Security Plan of Action and Milestones (POA&M), in accordance with FISMA requirements and Department of Navy, OMB, and National Institute of Standards and Technology (NIST) Guidance.

As stated in the response to Recommendation 4, the Navy Cash program is in the process of resubmitting an updated Certification package to NNWC to ensure that the Navy Cash revised patch management procedures comply with all current security directives.

Target completion date for completing our corrective actions is March 31, 2009.

Attachment
Page 3 of 7

RECOMMENDATION 6: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy to ensure that the Navy Cash program manager, in collaboration with the appropriate organizations update the Naval Supply Systems Command (NAVSUP)/Treasury Financial Management Services (FMS) memorandum of agreement, in collaboration with FMS, to establish specific security requirements for FMS and the financial agent to periodically perform information security control reviews, including applicable management, operational, and technical controls, of the Navy Cash system, and to provide NAVSUP with copies of the results of these reviews that pertain to the Navy Cash system and its supporting infrastructure.

DOD RESPONSE: Concur. The Treasury FMS Security office has conducted several security reviews of the Treasury Financial Agent's security posture in accordance with Treasury's Electronic Systems Processing Security Guidelines. They are also developing electronic systems processing security guidelines for applications like Navy Cash.

The Navy Cash Program Office will work with Treasury to update the Memorandum of Agreement (MOA) to reflect the security guidelines that FMS places on its financial agents.

Target completion date for completing our corrective actions is May 31, 2009.

RECOMMENDATION 7: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy to ensure that the Navy Cash program manager, in collaboration with the appropriate organizations develop a complete contingency plan to include a: (1) sequence of recovery activities; and (2) procedures for notifying ship personnel with contingency plan responsibilities to begin recovery activities; and to test the contingency plan in accordance with NIST guidance, including documenting lessons learned from testing.

DOD RESPONSE: Concur. The recovery strategies in the Navy Cash Contingency Planning Guide will be updated to include a more detailed sequence of recovery activities and procedures for notifying ship personnel with contingency plan responsibilities to begin recovery activities. The Navy Cash Contingency Plan test procedures will be updated to include the documentation of lessons learned, in accordance with NIST guidance.

Target completion date for completing our corrective actions is May 31, 2009.

RECOMMENDATION 8: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy to ensure that the Navy Operational Designated Approving Authority, as part of the Naval Network Warfare Command, updates it certification and accreditation guidance to require the development of plans of action and milestones for all above identified security weaknesses.

Attachment
Page 4 of 7

DOD RESPONSE: Concur. The requirement for a System Level IT Security Plan of Action and Milestone (POA&M) is included in the new Department of Defense Information Assurance Certification and Accreditation Process (DIACAP). The Navy Cash Program Office has developed a System Level IT Security POA&M in the pending Certification and Accreditation package for the next software update for Navy Cash.

Target completion date for completing our corrective actions is December 31, 2008.

For the following three recommendations, if further investment in development of Navy Cash can be justified then:

RECOMMENDATION 9: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy, through the appropriate chain of command, to ensure that the Navy Cash program manager: (1) develop detailed system requirements; (2) establish policies and plans for managing changes to requirements, including defining roles and responsibilities, and identifying how the integrity of the baseline set of requirements will be maintained; and (3) maintain bi-directional requirements traceability.

DOD RESPONSE: Concur. The Navy Cash Program Office will define system requirements and establish related policies and plans adequate to manage changes to requirements and to maintain bi-directional requirements traceability in accordance with best business practices for all future efforts.

Target completion date for completing our corrective actions is May 31, 2009.

RECOMMENDATION 10: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy, through the appropriate chain of command, to ensure that the Navy Cash program manager: (1) establish and implement a written plan and defined process for risk identification, analysis, and mitigation; (2) assign responsibility for managing risk to key stakeholders; (3) encourage program-wide participation in risk management; (4) include and track the risks discussed in this report as part of a risk inventory; and (5) apprise decision making and oversight authorities of the status of identified risks during program reviews.

DOD RESPONSE: Concur. While the Navy Cash Program Office addressed program risks regularly and successfully through our Program Management Review process, the Program Office has since instituted a more formal risk management approach as recommended here and in accordance with the Naval Systems Commands Risk Management Policy (NAVSUP INSTRUCTION 5000.20). The effort was kicked-off at the program review held June 10-11, 2008, with formal documentation currently under development.

Target completion date for completing our corrective actions is December 31, 2008.

RECOMMENDATION 11: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy, through the appropriate chain of command, ensure that the

Attachment
Page 5 of 7

Navy Cash program manager: (1) determines trends in unresolved change requests and (2) understands users' satisfaction with the system.

DOD RESPONSE: Concur. In the past, the Navy Cash Program Office has only dealt with a minimum number of proposed changes, and all proposed changes were well-documented. The Program Office will add the detail to the existing process as recommended here.

It is important to highlight that the user base has been and continues to be an important participant in essentially every program discussion. As indicated in the report, the Program Office is currently conducting another survey and will revise/repeat the survey process as required to ensure understanding of user satisfaction.

Target completion date for completing our corrective actions is September 30, 2009.

COMMENTS TO THE DRAFT AUDIT REPORT:

The Department believes the following details and clarifications will help readers of this report to better understand statements made in the report that were not directly addressed in the recommendations or responses.

Navy Cash is designated as an Acquisition Category (ACAT) III program and is not a Major Automated Information Systems (MAIS) program. To manage the acquisition and deployment of Navy Cash, the Navy established a program management office within the Naval Supply Systems Command (NAVSUP). The program office grew over time from 4 Full Time Equivalents (FTE) in September 2000, to 8.5 FTEs in June 2008. NAVSUP has partnered with the Treasury's FMS not only because of statutory regulations on holding public funds (31 C.F.R. Part 202, 31 U.S.C. § 3302), but also to take advantage of the Treasury's extensive experience in fielding stored value card programs with the Army, Air Force and Marine Corps.

Navy Cash is a fully developed system, currently installed on 128 ships and is over 80 percent deployed. The system has achieved the major program goals for cost, schedule, and performance. Half of the ships remaining in our deployment schedule are new construction ships that have not yet been delivered to the Navy. In addition, Navy's partnership with the Treasury and the Treasury Financial Agent provided access to what are, in effect, proven Commercial Off-the-Shelf (COTS) products that required little modification to provide the financial services necessary to support Navy Cash.

The Department recognizes some limited areas for improvement in security management as described in our responses, but these limitations do not represent a serious risk to the confidentiality, integrity, or availability of the deployed Navy Cash systems, as indicated on Page 8 of the report. The Department is concerned that cardholders would become unnecessarily concerned.

Attachment
Page 6 of 7

Although this report primarily focuses on cashless retail functions, it needs to be noted that the core capability of Navy Cash is to enable Sailors and Marines embarked on Navy ships access to their pay in accordance with 31 U.S.C. § 3342 and The Debt Collection Improvement Act of 1996.

Attachment
Page 7 of 7

Appendix III: Comments from the Department of the Treasury, Financial Management Service

COMMISSIONER

DEPARTMENT OF THE TREASURY
FINANCIAL MANAGEMENT SERVICE
WASHINGTON, D.C. 20227

August 18, 2008

Mr. Randolph C. Hite
Director, Information Technology Architecture and Systems Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Hite:

Thank you for the opportunity to comment on the Government Accountability Office's (GAO) draft report entitled "DoD Business Systems Modernization, Planned Investment in Navy Program to Create Cashless Shipboard Environment Needs to Be Justified and Better Managed" (GAO-08-922). We appreciate GAO's efforts to identify improvements in the Navy Cash program which is managed jointly by the U.S. Department of the Navy (Navy) and the Financial Management Service (FMS).

The Navy Cash program has successfully met the Navy's goal of transforming cash management by removing the vast majority of cash from the Fleet's operations. Since its introduction in 2001, the program has displaced more than $300 million in coin and currency on 128 Navy ships, through the issuance of more than 200,000 financial smart cards to Sailors and Marines who have initiated more than 100 million transactions. Information security is critically important to both the Navy and FMS. We note that the draft report identifies no security breach, loss of cardholder or government funds, unauthorized release of personal or other sensitive information, or any other compromise of system integrity in connection with these operations.

The GAO recommendations identified in the draft report will help strengthen the Navy Cash program, and we are already addressing several of the findings and recommendations. Please note our comments below and in an attachment to this letter.

First, we note that the draft report requires Navy to ensure that FMS strengthen its Information Technology security program in accordance with the Federal Information Security Management Act (FISMA) requirements. FMS will continue to support the Navy in its efforts to comply with the report's recommendations so long as implementation is consistent with FMS' policies and the statutory authorities and regulations which govern the provision of financial services by FMS' financial agents. FMS has unique authority to designate financial and fiscal agents to assist in the performance of many functions related to the nation's finances. *See, e.g.*, 12 U.S.C. §§ 90, 391. This authority permits FMS to effectively administer centralized public funds deposit, management, and accounting functions, without the expense of developing and maintaining its own banking system. Navy Cash funds constitute public money under 31 C.F.R. Part 202 and thus, in accordance with 31 U.S.C. § 3302, must be held in the Treasury or in an account held by a Treasury designated financial agent.

The commercial banking institutions selected by FMS to act as financial agents are highly regulated and must act in compliance with rules issued by the Office of the Comptroller of the Currency (OCC), Federal Reserve Board, Federal Deposit Insurance Corporation (FDIC) and private organizations (i.e. MasterCard and NACHA). FMS is in the process of strengthening its Information Technology security program to improve FMS' oversight of the internal controls employed by its financial agents. FMS recognizes the importance of improved oversight of the manner in which its financial agents implement security controls in order to ensure that stringent security procedures are in place.

Second, the draft report questions whether Navy Cash is duplicative of similar smart card programs operated by the Air Force and Army. This issue was addressed before the Navy Cash program was implemented in 2001. Given the unique requirements of ships at sea, FMS and Navy determined that the functionality of the other Department of Defense (DoD) smart card programs could not support Navy Cash. Among other things, Navy Cash requires a dual-factor smart card that functions on ship (integrated circuit chip) and ashore (magnetic stripe), an automated end-of-day settlement process, and a "split pay" program that allows the Sailor/Marine to allocate a portion of his or her pay to the Navy Cash card. For both technical and cost reasons, none of the other FMS/DoD smart card platforms could be altered to provide this functionality.

In 2004, DoD and FMS agreed on a goal of a "single smart card." Efforts to advance this concept include two proofs of technology pilots (conducted in 2005 and 2006) with DoD using the Common Access Card. Also, an Inter-Agency Stored Value Card team, which was chartered in 2007, is assisting FMS as it develops a stored value card strategy to support a single DoD smart card for the future.

Finally, we want to clarify the statement in the draft report that "the [Navy Cash] benefits projection erroneously counted $40 million as cost savings rather than cost transfers...." We disagree with this statement. The initial Business Case Analysis ("BCA") estimated that when implemented fleetwide, Navy Cash would displace $459 million in cash that would otherwise be held outside of the Treasury. The BCA calculated the time value of the funds retained in the Treasury to be in excess of $40 million for the first six years of the program. This value is not merely a transfer between agencies, but represents actual savings to the United States.

Again, thank you for the opportunity to comment on this draft GAO report. If you have any questions or wish to discuss these comments in more detail, I can be reached at (202) 874-7000, or you may contact Sheryl Morrow on (202) 874-6720.

Sincerely,

Judith R. Tillman

Enclosure

ENCLOSURE

Financial Management Service's (FMS) Response to Recommendations in Government Accountability Office's Draft Report DoD Business Systems Modernization, Planned Investment in Navy Program to Create Cashless Shipboard Environment Needs to Be Justified and Better Managed (GAO-08-922).

Recommendation 1: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy to limit further investment in the program to only: (1) deployment to remaining ships of already developed and tested capabilities; (2) correction of information security vulnerabilities and weaknesses on ships where it is deployed and operating; and (3) development of the basis for an informed decision as to whether further development and modernization is economically justified and in the department's collective best interests.

> Response: FMS agrees with the recommendation to correct system vulnerabilities and update economic justification for the Navy Cash program. However, FMS disagrees with the recommendation to limit investment beyond fielding and maintaining already tested capabilities because the recommendation would place future operations at risk. Important components of the Navy Cash system architecture are at end-of-life. Therefore, the process to identify, test, and certify replacement equipment must continue or the program's operations will be jeopardized. FMS will support Navy in its update of the economic analysis of the program's costs and benefits.

Recommendation 2: The GAO recommends that the Secretary of the Defense through the appropriate chain of command, direct the Director of the DoD Business Transformation Agency, to: (1) examine the relationships among DoD's programs for delivering military personnel with smart card technology for electronic retail and banking transactions; (2) identify, in coordination with the respective program offices, alternatives for optimizing the relationships of these programs in a way that minimizes areas of duplication, maximizes reuse of shared services across the programs, and considers opportunities for a consolidated stored value card program across the military services; and (3) share the results with the appropriate organizations for use in making an informed decision about planned investment in Navy Cash.

> Response: FMS welcomes DoD's continued support and input in connection with its efforts to review, develop, and implement a strategy that will ultimately result in a single, multi-functional smart card to meet DoD's cash management needs.

Recommendation 3: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy to ensure that the appropriate Navy organizational entities prepare a reliable economic analysis that encompasses the program's total life cycle costs, including those of Department of the Treasury, Financial Management Service

(FMS) and that: (1) addresses cost-estimating best practices and complies with relevant OMB cost benefit guidance; and (2) incorporates data on whether deployed Navy Cash capabilities are actually producing benefits.

Response: FMS will support Navy in its analysis of the program's costs and benefits.

Recommendation 4: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy to ensure that the Navy Cash program manager, in collaboration with the appropriate organizations develop and implement a patch management approach based on National Institute of Standards and Technology (NIST) guidance, which includes a complete Navy Cash systems inventory; an automated patch deployment capability; and a patch management performance vulnerability measurement capability, including metrics for susceptibility to attack and mitigation response time.

Response: FMS will support Navy in its implementation of this recommendation and is currently working with Navy to implement an automated patch deployment capability.

Recommendation 5: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy to ensure that the Navy Cash program manager, in collaboration with the appropriate organizations institute a process to plan, implement, evaluate, and document remedial actions for deficiencies in Navy Cash information security policies, procedures and practices, and ensure that this process meets Financial Information Security Management Act (FISMA) requirements, as well as applicable OMB and NIST guidance.

Response: FMS will support Navy in its implementation of this recommendation, and will ensure that implementation is consistent with FMS' and other authorities related to the banking services provided by FMS' financial agent.

Recommendation 6: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy to ensure that the Navy Cash program manager, in collaboration with the appropriate organizations update the Naval Supply Systems Command (NAVSUP)/FMS memorandum of agreement, in collaboration with FMS, to establish specific security requirements for FMS and the financial agent to periodically perform information security control reviews, including applicable management, operational, and technical controls, of the Navy Cash system, and to provide NAVSUP with copies of the results of these reviews that pertain to the Navy Cash system and its supporting infrastructure.

Response: FMS will work with NAVSUP to update the Memorandum of Agreement (MoA) to reflect the security guidelines that FMS places on its financial agents. FMS is in the process of enhancing its existing security requirements and oversight of its financial agents and will ensure that Navy is

provided access to the results of the reviews that pertain to the Navy Cash program.

Recommendation 7: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy to ensure that the Navy Cash program manager, in collaboration with the appropriate organizations develop a complete contingency plan to include a: (1) sequence of recovery activities; and (2) procedures for notifying ship personnel with contingency plan responsibilities to begin recovery activities; and to test the contingency plan in accordance with NIST guidance, including documenting lessons learned from testing.

Response: FMS will support Navy in its implementation of this recommendation, and will ensure that implementation is consistent with FMS' and other authorities related to the banking services provided by FMS' financial agent.

Recommendation 8: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy to ensure that the Navy Operational Designated Approving Authority, as part of the Naval Network Warfare Command, updates it certification and accreditation guidance to require the development of plans of action and milestones for all above identified security weaknesses.

Response: FMS will support Navy in its implementation of this recommendation, and will ensure that implementation is consistent with FMS' and other authorities related to the banking services provided by FMS' financial agent.

Recommendation 9: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy, through the appropriate chain of command, to ensure that the Navy Cash program manager: (1) develop detailed system requirements; (2) establish policies and plans for managing changes to requirements, including defining roles and responsibilities, and identifying how the integrity of the baseline set of requirements will be maintained; and (3) maintain bi-directional requirements traceability.

Response: FMS will support Navy in its implementation of this recommendation, and will ensure that implementation is consistent with FMS' and other authorities related to the banking services provided by FMS' financial agent.

Recommendation 10: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy, through the appropriate chain of command, to ensure that the Navy Cash program manager: (1) establish and implement a written plan and defined process for risk identification, analysis, and mitigation; (2) assign responsibility for managing risk to key stakeholders; (3) encourage program-wide participation in risk management; (4) include and track the risks discussed in this report as part of a risk inventory; and (5) apprise decision making and oversight authorities are of the status of identified risks during program reviews.

Response: FMS will support Navy in its implementation of this recommendation, and will ensure that implementation is consistent with FMS' and other authorities related to the banking services provided by FMS' financial agent.

Recommendation 11: The GAO recommends that the Secretary of Defense direct the Secretary of the Navy, through the appropriate chain of command, ensure that the Navy Cash program manager: (1) determines trends in unresolved change requests and (2) understands users' satisfaction with the system.

Response: FMS will support Navy in its implementation of this recommendation, and will ensure that implementation is consistent with FMS' and other authorities related to the banking services provided by FMS' financial agent.

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Randolph C. Hite (202) 512-3439 or hiter@gao.gov
Gregory C. Wilshusen (202) 512-3789 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contact persons named above, key contributors to this report were Neelaxi Lakhmani (Assistant Director), Jenniffer Wilson (Assistant Director), Ed Glagola (Assistant Director), Monica Anatalio, Carolyn Boyce, Harold Brumm, West Coile, Neil Doherty, Cheryl Dottermusch, Joshua Hammerstein, Mustafa Hassan, Michael Holland, James Houtz, Ethan Iczkovitz, Rebecca LaPaze, Anh Le, Josh Leiling, Mary Marshall, Karen Richey, Melissa Schermerhorn, Karl Seifert, Jonathan Ticehurst, and Adam Vodraska.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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