

September 2009

INFORMATION TECHNOLOGY

DOD Needs to Strengthen Management of Its Statutorily Mandated Software and System Process Improvement Efforts



GAO

Accountability * Integrity * Reliability



Highlights of [GAO-09-888](#), a report to congressional requesters

Why GAO Did This Study

The Department of Defense's (DOD) acquisition of weapon systems and modernization of business systems have both been on GAO's list of high-risk areas since 1995. To assist DOD in managing software-intensive systems, Section 804 of the Bob Stump National Defense Authorization Act for Fiscal Year 2003 required the Office of the Secretary of Defense (OSD) and DOD component organizations, including the military departments, to undertake certain software and systems process improvement (SSPI) actions. As requested, GAO assessed (1) the extent to which DOD has implemented the process improvement provisions of the act, and (2) the impact of DOD's process improvement efforts. To do so, GAO analyzed relevant plans, policies, guidance, performance measures, and reports against statutory requirements and relevant guidance, and interviewed DOD officials.

What GAO Recommends

GAO is making recommendations to the Secretary of Defense aimed at OSD and DOD components adopting the kind of strategic approach to process improvement embodied in section 804 and relevant guidance, and reporting to congressional defense committees on the progress and impacts of doing so. DOD partially agreed with GAO's recommendations and described actions to address each. While GAO supports DOD's actions, it does not believe they are sufficient to effectively manage a departmentwide SSPI program.

[View GAO-09-888](#) or [key components](#). For more information, contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov.

INFORMATION TECHNOLOGY

DOD Needs to Strengthen Management of Its Statutorily Mandated Software and System Process Improvement Efforts

What GAO Found

OSD and the military departments have implemented a number of statutory requirements aimed at improving their processes for acquiring software-intensive systems. However, they have not satisfied all of their respective statutory requirements, or key aspects of relevant SSPI guidance. In particular,

- OSD has issued guidance calling for military departments and defense agencies to implement process improvement programs, revised guidance to emphasize contractor past performance in source selection decisions, and established a clearinghouse for software and system acquisition and development best practices, all of which are required by the statute. However, it has not implemented a requirement in the statute related to overseeing DOD component organization process improvement programs to ensure compliance with its guidance, and it has not satisfied a key aspect of relevant guidance pertaining to monitoring organizationwide process improvement efforts. According to OSD, process improvement is a component responsibility and thus it does not view oversight of component SSPI efforts as necessary. Without strong, central leadership over DOD's improvement efforts, OSD is not fulfilling key tenets of section 804 and relevant guidance associated with well-managed software process improvement programs, and has increased the risk that component process improvement efforts and their impacts are not being maximized.
- The military departments have established process improvement programs, although two did not do so within the time frame specified in the statute. Also, each has documented processes that address the four key software process areas cited in the statute, and have taken steps to ensure that key personnel have the appropriate level of software/system-related experience or training, and to develop process improvement performance metrics, as required by the statute. However, none is using these performance metrics for continuous process improvement, as provided for in the statute and relevant guidance. Also, while each has a process governing implementation of key acquisition requirements, these processes do not fully reflect the range of verification steps advocated in relevant guidance. Reasons cited for the state of the department's respective efforts include senior leadership turnover and not viewing all the statutory requirements as necessary. By not having fully implemented the statute and relevant guidance, the military departments are not positioned to maximize the potential of their process improvement efforts.

Neither OSD nor the military departments have measured the impact of their collective or separate process improvement efforts. However, studies by GAO and others continue to identify system and software acquisition and development process weaknesses, as well as cost, schedule, and performance shortfalls, across a range of DOD software-intensive programs, thus suggesting that the potential value of these efforts has yet to be fully realized.

Contents

Letter		1
	Background	2
	DOD Has Not Fully Implemented Statutory Requirements and Guidance for Improving Software and System Processes	6
	DOD Does Not Know Impact of SSPI Efforts but Studies of Large- Scale Acquisition Programs Show that Performance Shortfalls and Process Weaknesses Continue	22
	Conclusions	28
	Recommendations for Executive Action	28
	Agency Comments and Our Evaluation	29
Appendix I	Objectives, Scope, and Methodology	32
Appendix II	Comments from the Department of Defense	34
Appendix III	GAO Contact and Staff Acknowledgments	38
Table		
	Table 1: Extent to which Military Departments Have Documented Processes for Each Key Software Area	18
Figures		
	Figure 1: View of DOD Web-based Portal	11
	Figure 2: Timeline of Establishment of SSPI Programs	14

Abbreviations

2003 NDAA	Bob Stump National Defense Authorization Act for fiscal year 2003
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
ASD(NII)/CIO	Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer
CMMI	Capability Maturity Model Integration
DOD	Department of Defense
EVM	earned value management
GCSS-MC	Global Combat Support System - Marine Corps
Navy ERP	Navy Enterprise Resource Planning
OASD(C3I)	Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
OASD(NII)/ CIO	Office of the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer
OSD	Office of the Secretary of Defense
OUSD(AT&L)	Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics
PEO	program executive officer
PSR	Program Support Review
SEI	Software Engineering Institute
SSPI	software and systems process improvement
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

September 8, 2009

The Honorable Evan Bayh
Chairman
The Honorable Richard Burr
Ranking Member
Subcommittee on Readiness and
Management Support
Committee on Armed Services
United States Senate

The Honorable Daniel K. Akaka
United States Senate

The Honorable John Ensign
United States Senate

The Department of Defense (DOD) relies heavily on software-intensive systems to support military operations and associated business functions, such as logistics, personnel, and financial management. One important determinant of the quality of these systems, and thus DOD's mission performance, is the quality of the processes used to develop and acquire them. Recognizing the importance of these processes in producing systems that perform as intended and meet cost and schedule goals, successful public and private organizations have adopted and implemented software and systems process improvement (SSPI) programs.¹

Section 804 of the Bob Stump National Defense Authorization Act for fiscal year 2003 (2003 NDAA)² requires military departments, and defense agencies that manage major acquisition programs, to establish process

¹As used in this report, SSPI refers to improvements in the processes associated with developing, acquiring, and engineering software and systems.

²Pub. L. No. 107-314, § 804, 116 Stat 2458, 2604-2605 (Dec. 2, 2002).

improvement programs.³ This report responds to your request to review the department's implementation of this requirement. As agreed, our objectives were to determine: (1) the extent to which DOD has implemented the process improvement provisions of the act, and (2) the impact of DOD's process improvement efforts. To accomplish these objectives, we reviewed SSPI policies, guidance, plans, oversight controls, and performance measures, and compared these to the statutory requirements and relevant guidance; we interviewed responsible officials of the Office of the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer (OASD(NII)/CIO), the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD(AT&L)), and the military departments; and reviewed and analyzed related studies and reports on the impact of DOD's SSPI efforts.

We conducted this performance audit at DOD and military department offices in Arlington, Virginia, from December 2008 through September 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Appendix I further discusses our scope and methodology.

Background

DOD is a massive and complex organization. To meet its missions, the department relies on a complex array of computer-dependent and mutually supportive organizational components, including the military departments and defense agencies. It also relies on a broad array of systems to support operations related to intelligence, surveillance, security, and sophisticated weaponry—as well as financial management and other business functions.

DOD's investment in major acquisition programs, including largely software-intensive weapons systems, is expected to be about \$357 billion

³DOD major defense acquisition programs are those estimated to require total research, development, test, and evaluation expenditures of more than \$365 million or procurement expenditures of more than \$2.19 billion in fiscal year 2000 constant dollars. They also include programs otherwise designated by the department as major defense acquisition programs.

over the next 5 years.⁴ We have designated DOD's business systems modernization and its acquisition of weapons systems as high-risk areas.⁵

The quality of the processes involved in developing and acquiring software and systems has a significant effect on the quality of the resulting products. Public and private organizations have reported significant returns on investment through improvements to these processes. For example, the Software Engineering Institute⁶ (SEI) reported in 2006⁷ that a major defense contractor implemented a process improvement program and improved its system development earned value management cost and schedule performance by 5 percent and 8 percent, while reducing cost and schedule variability by 34 percent and 50 percent, respectively. It also reported that the contractor reduced system defects by about 44 percent. Further, SEI reported that a defense software maintenance group decreased the cost of its services by an average of 27 percent and reduced its effort required to deliver test programs by 25 percent.

Summary of GAO's Prior Review on DOD's SSPI Programs

In 2001, we reported that DOD lacked a corporate approach to guiding and overseeing the military department and defense agency SSPI activities, and as a result, the scope and nature of these activities varied.⁸ For example, the Air Force, Army, and certain Navy units had established programs that generally satisfied the tasks of SEI's IDEAL^{SM9} process improvement model, while the Marine Corp and other Navy units did not. Further, the military departments were using different management strategies for directing and controlling their respective SSPI activities. In light of these variations and the opportunity for DOD's component organizations to learn from and leverage each other's experiences and best practices, we concluded that the Office of the Secretary of Defense (OSD) had an

⁴GAO, *High-Risk Series: An Update* [GAO-09-271](#) (Washington, D.C.: January 2009).

⁵[GAO-09-271](#).

⁶SEI is a federally funded research and development center established at Carnegie Mellon University to address software engineering practices.

⁷SEI, Technical Report CMU/SEI-2006-TR-004, August 2006.

⁸GAO, *DOD Information Technology: Software and Systems Process Improvement Programs Vary in Use of Best Practices*, [GAO-01-116](#) (Washington, D.C.: Mar. 30, 2001).

⁹IDEALSM is a service mark of Carnegie Mellon University and stands for initiating, diagnosing, establishing, acting, and learning. IDEALSM is the SEI methodology for organizational software process improvement.

important leadership role to play in expanding SSPI across the department. Accordingly, we recommended that the Secretary of Defense:

- direct DOD component organizations to begin software process improvement efforts where our report showed none existed, and that these organizations consider following the best practices embodied in the SEI IDEALSM model and drawn from the experiences of other component organizations that have successfully implemented SSPI programs;
- direct the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)),¹⁰ in collaboration with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), to (1) issue a policy requiring DOD components that are responsible for software-intensive systems development, acquisition, or engineering to implement SSPI programs, and (2) develop and issue SSPI guidance, and, in doing so, consider basing this guidance on the SEI IDEALSM model and the positive examples within the military departments and defense agencies cited in our report; and
- direct the ASD(C3I) to (1) annually determine the components' compliance with the SSPI policy and (2) establish and promote a means for sharing SSPI lessons learned and best practices knowledge through DOD.

In response, DOD agreed that SSPI practices should be pursued and encouraged, and that information about SSPI practices should be shared among DOD components.

Summary of Section 804 of the 2003 National Defense Authorization Act

Congress included several provisions in section 804 of the 2003 NDAA related to SSPI that are consistent with the SSPI recommendations we provided to DOD in 2001.¹¹ In general, these provisions provide for a strategic and corporate approach to SSPI in the department by placing certain requirements on organizations within OSD as well as other requirements on the military departments and defense agencies. The provisions are as follows:

¹⁰This position has since been renamed as the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer (ASD(NII)/CIO).

¹¹Pub. L. No. 107-314 (Dec. 2, 2002).

Office of the Secretary of
Defense

The ASD(C3I), in collaboration with the USD(AT&L), shall:

- Prescribe uniformly applicable guidance for the administration of all the software process improvement programs established by this mandate.
- Take such actions as are necessary to ensure that the military departments and defense agencies comply with this guidance.
- Assist the secretaries of the military departments and heads of defense agencies to carry out such programs effectively by: (1) ensuring that criteria applicable to the selection of sources provide added emphasis on past performance of potential sources, as well as on the maturity¹² of the software products offered by the potential sources; and (2) identifying, and serving as a clearinghouse for, information regarding best practices in software development in both the public and private sectors.

Military Departments and
Defense Agencies

The secretary of each military department and head of each defense agency that manages a major defense acquisition program with a substantial software component shall:

- Establish a program to improve the software acquisition processes of that military department or defense agency within 120 days after the act's enactment.
- Ensure that a program to improve software acquisition processes includes, at a minimum, the following: (1) a documented process for software acquisition planning, requirements development and management, project management and oversight, and risk management; (2) efforts to develop appropriate metrics for performance measurement and continual process improvement; (3) a process to ensure that key program personnel have an appropriate level of expertise or training in software acquisition; and (4) a process to ensure implementation and adherence to established processes and requirements relating to the acquisition of software.

¹²According to DOD's May 2005 Technology Readiness Assessment Deskbook, technology should be "mature" before system development begins. Normally, for technology to be considered mature, it must have been tested in a relevant or operational environment, and found to have performed adequately for the intended application.

DOD Has Not Fully Implemented Statutory Requirements and Guidance for Improving Software and System Processes

OSD and the military departments have met some, but not all of their respective statutory requirements¹³ aimed at adopting a corporate and strategic approach to improving DOD's processes for developing and acquiring software-intensive systems, although the military departments vary in how and the extent to which they have and have not met their requirements. In addition, neither OSD nor the military departments have established programs that fully utilize SSPI guidance.

OSD officials responsible for implementing applicable provisions of the statute cited various reasons for not meeting all the requirements, including requirements being inconsistent with OSD's role. Reasons cited by military department officials included changes in senior leadership and not viewing all requirements as necessary. Regardless, this means that neither OSD nor the military departments fully complied with requirements of section 804, and as a result, have increased the risk that the billions of dollars being spent each year on DOD software-intensive system acquisitions will not benefit from an effectively and efficiently managed corporate approach to SSPI.

OSD Has Partially Satisfied Statutory SSPI Requirements

OSD has partially implemented the statutory SSPI requirements that apply to it, and relevant process improvement guidance, which are aimed at providing a corporate and strategic approach to SSPI efforts. To their credit, the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer (ASD(NII)/CIO) and USD(AT&L) jointly issued a memorandum that, among other things, established DOD's Software Acquisition Process Improvement Program and provided guidelines and expectations for OSD and component organizations relative to developing and implementing their respective SSPI programs. OUSD(AT&L) also has revised existing guidance on source selection to emphasize contractor past performance, and established a clearinghouse for information on SSPI-related best practices and lessons learned. In addition, OSD has taken other steps to assist the military departments in implementing their respective SSPI efforts.

However, OSD has not taken steps to ensure that component organizations comply with its SSPI guidance and expectations, and it has not emphasized the maturity of software products in existing source

¹³Pub. L. No. 107-314, § 804 (Dec. 2, 2002).

OSD Has Issued Guidance and Expectations for Developing and Implementing SSPI Programs

selection guidance. Without such oversight and guidance, DOD cannot adequately ensure that its organizational components are effectively and efficiently implementing SSPI activities, and thus that the risks associated with acquiring software-intensive systems are being minimized.

The statute¹⁴ states that the ASD(C3I), in collaboration with the USD(AT&L), shall prescribe uniformly applicable guidance to the military departments and defense agencies for the administration of their software process improvement programs. Relatedly, SEI's IDEAL^{SM15} model emphasizes the importance of establishing an SSPI management structure that includes setting goals and performance measures, assigning roles and responsibilities, having a plan to guide process improvement activities, and allocating and securing resources needed to execute the plan.

Consistent with the statute, the ASD(NII)/CIO and USD(AT&L) issued a joint memorandum in March 2003 that created the department's Software Acquisition Process Improvement Program, referenced section 804, and established the OSD Software-Intensive Systems Steering Group to lead and facilitate component SSPI efforts and to recommend uniformly applicable guidance for the administration of these SSPI programs. Further, the memorandum includes guidelines and expectations for component organizations' SSPI programs relative to identifying specific goals, milestones, performance measures, and resource needs, and ensuring that SSPI personnel have an appropriate level of training and experience. The guidelines also direct DOD components to identify an approach and evaluation criteria to be used in guiding and assessing their SSPI activities and goals. According to officials in the military departments that are responsible for SSPI, they have used these guidelines and expectations in developing and implementing their respective programs.

Beyond meeting the statute's requirement for prescription of guidance, the joint memorandum and relevant guidelines and expectations also satisfy key aspects of SEI's IDEALSM model. For example, the memorandum states that the components should, among other things, set goals and performance measures, assign roles and responsibilities, develop an approach and evaluation criteria to guide process improvement and to assess achievement of goals, and allocate and secure resources needed to

¹⁴Pub. L. No. 107-314, § 804(c)(1) (Dec. 2, 2002).

¹⁵Software Engineering Institute, *IDEALSM: A User's Guide for Software Process Improvement*, CMU/SEI-96-HB-001 (Pittsburgh, Pa., February 1996).

OSD Is Not Overseeing
Component SSPI Programs to
Ensure Compliance with
Guidelines and Expectations

execute the plan. Further, the memorandum stated that components' respective SSPI programs should address eight key process areas, including the four they are required to address under the act (see later section of this report for a discussion of these four process areas). By issuing these guidelines and expectations, OSD complied with the statute and took foundational steps towards DOD-wide implementation of SSPI.

According to the statute,¹⁶ the ASD(C3I), in collaboration with the USD(AT&L), is to take necessary actions to ensure that the military departments and defense agencies comply with guidance for the administration of their software process improvement programs. Relatedly, SEI's IDEALSM model recognizes the importance of overseeing and monitoring an organization's SSPI activities. For example, it states that a steering group representing senior management should be responsible for oversight of organizational SSPI efforts.

Neither OASD(NII)/CIO nor OUSD(AT&L) has overseen the military department and defense agency efforts to comply with OSD-issued SSPI guidelines and expectations, nor have they developed accountability mechanisms to ensure that the military departments and defense agencies comply. According to officials from both organizations, SSPI implementation is a component responsibility, and therefore they believe that DOD's role should be collaborative and facilitative, and should not focus on requiring compliance and accountability. Further, they stated that OSD visibility into component SSPI efforts does occur indirectly through the system acquisition Program Support Reviews¹⁷ (PSR) at major acquisition milestones, as well as through technical working groups, such as DOD's Software Working Group and Systems Engineering Forum. However, the PSRs do not address component compliance with the OSD-issued SSPI guidelines and expectations. Specifically, they do not verify that the military departments have developed appropriate metrics for continual process improvement, as required by the statute. They also do not ensure that the military departments followed key aspects of relevant SSPI guidance, such as developing and implementing strategic action plans. Further, while the technical working groups permit visibility into

¹⁶Pub. L. No. 107-314, § 804(c)(1) (Dec. 2, 2002).

¹⁷Program Support Reviews are the department's milestone reviews for each system acquisition. According to DOD's Instruction 5000.02, *Operation of the Defense Acquisition System*, OSD performs these reviews only on those acquisitions that meet certain dollar thresholds or that are otherwise designated as special interest.

component SSPI efforts, these groups do not have the authority to ensure compliance with OSD guidelines and expectations.

Without effective oversight and accountability mechanisms to ensure that components comply with the SSPI requirements, OSD has not met a key requirement of section 804 and relevant guidance, and it has increased the risk of DOD components not implementing SSPI in an effective and efficient manner and not maximizing DOD-wide process improvement outcomes.

OSD Has Partially Addressed Other Statutory Requirements and Has Taken Steps to Otherwise Assist Military Departments in Developing and Implementing SSPI Programs

The statute¹⁸ requires specific officials within OSD to assist the military departments and defense agencies in implementing SSPI programs by (1) ensuring that criteria applicable to the selection of sources provides added emphasis on potential sources' past performance and software product maturity; and (2) identifying, and serving as a clearinghouse for, information regarding best practices in software development in both the public and private sectors. OSD has partially met the first statutory requirement and fully met the second. In addition, it has provided additional assistance to the military departments, including aiding them in establishing their process improvement efforts.

OSD Guidance Emphasizes Importance of Contractor Past Performance during Source Selection, but not Maturity of Contractor Products

OUSD(AT&L) has issued source selection guidance that describes the criteria and key techniques that should be used by program offices. Among other things, this guidance provides for considering a contractor's past performance by selecting and reviewing similar efforts involving the contractor that are still ongoing or have just been completed, addressing performance expectations in the government and contractor's initial postaward meeting; and using presolicitation meetings with industry to obtain past performance information.

However, this source selection guidance does not emphasize considering the maturity of contractor products as part of source selection. According to OUSD(AT&L) officials, steps have been taken to begin to address this gap in guidance but significant work remains. For example, they cited a 2007 USD(AT&L) memorandum that encourages programs to implement a

¹⁸Pub. L. No. 107-314, § 804(c)(2) (Dec. 2, 2002).

competitive prototyping approach, which they described as one means of establishing the maturity of an acquisition program's key technologies during its early phases. They also said that OSD has recently begun working with the Navy to identify the key product maturity information needed prior to source selection. Notwithstanding these steps, source selection guidance specifically addressing product maturity has yet to be issued.

Until OSD source selection guidance also emphasizes contractor product maturity, the department will not be in full compliance with section 804, and it will increase the risk of acquisitions falling short of expectations due to the use of immature hardware and software products.

OSD Has Established a Clearinghouse for Software and System Acquisition and Development Best Practices

OSD has established a clearinghouse of best practices information relative to software and system acquisition and development processes and SSPI. Specifically, OUSD(AT&L) has partnered with the Defense Acquisition University to provide both instructor-led training and a Web-based portal to share knowledge about software process-related methodologies, such as the SEI's Capability Maturity Model Integration (CMMI®),¹⁹ SEI's IDEALSM model, and Lean Six Sigma.²⁰ For example, the portal features content areas such as software acquisition management, the SEI CMMI Acquisition model, system engineering planning, and system acquisition career fields. Further, for each content area, relevant best practices information is provided. To illustrate, the CMMI Acquisition model content area features best practices on 22 acquisition process areas, such as requirements development and management, project monitoring and control, and risk management. The primary information sources of the portal's content are conference publications, journal and trade magazines, and individuals' best practices submissions that are vetted through a content advisory group. (See fig. 1 for a top-level view of this portal.)

¹⁹The CMMI is a model used to examine an organization's software engineering process maturity. It combines earlier SEI models for software development and acquisition into one model for enterprise-wide process improvement.

²⁰Lean Six Sigma is a systematic, rigorous methodology that uses metrics and analysis to drive continuous improvement of an organization's processes.

Figure 1: View of DOD Web-based Portal

Best Practices Clearinghouse
Connecting you to Government and Industry Best Practices

Defense Acquisition University

Home | Contact | Site Map | FAQ | Help | DoD Certificate | Search

DAU Homepage
I Need Training
Continuous Learning
Knowledge Sharing
Performance Support

BPCh Menu

- Browse Content Views
- Filter Content
- Submit Content
- Feedback
- About BPCh

Welcome to the Acquisition Best Practices Clearinghouse

The DoD Acquisition Best Practices Clearinghouse (BPCh) facilitates the selection and implementation of systems engineering and software acquisition practices appropriate to the needs of individual acquisition programs. The BPCh uses an evidence-based approach, linking to existing resources that describe how to implement various best practices. These linked resources also provide descriptions of the practical results (both good and bad) of applying the practices in various contexts, from which users can learn about the results to be expected in their environment. All evidence stored is also contextualized, so that users will be guided to the lessons relevant to their program, type of problem, or specific situation.

Quick Search

Practices that have the most evidence

- Software Formal Inspections
- Pair Programming
- Trade Studies
- Architectural Reviews
- Distributed Work Allocation

Evidences that have the highest trustability scores

- Advances in Software Inspections
- An Analysis of Defect Densities Found During Software Inspections
- Measuring Inspections at Litton
- The MBASE Life-cycle Architecture Milestone Package
- Using the Win-Win Spiral model: A Case Study

BPCh Learning Guides

Guide Links

- For First-Time Users of BPCh
- Contributing Content to BPCh
- BPCh Tutorials
- Explaining Gold, Silver & Bronze Practice Maturity Levels
- Understanding the BPCh Vetting Process
- SME-Specific Training & Details

Gold Practices

- Pair Programming
- Software Formal Inspections

Practices that Reduce Schedule

- Include a Requirements Database in the RFP

Practices that Improve Quality

- Pair Programming
- Software Formal Inspections
- Software Walkthroughs

Acquisition KM Systems

AKSS ACC BPCh ACQUIRE

DAG IFC AAP DAPC

Sign In

ACQWeb

Privacy and Security | Contact | Feedback | Legal Notices

Web Help Desk
ISSC@dau.mil

Source: <https://bpch.dau.mil/Pages/default.aspx>.

By establishing a clearinghouse of information on software and system acquisition and development process best practices, OSD has provided the military departments and defense agencies with an important enabler for departmentwide process improvement.

OSD Has Taken Additional Measures to Assist Components in Implementing SSPI Programs

To OSD's credit, it established the Software-Intensive Systems Steering Group in March 2003 to assist the military departments and defense agencies in setting up their process improvement programs. More specifically, this steering group worked with the military departments and defense agencies to ensure that each had established an SSPI effort, after which the group was disestablished and its responsibilities subsumed into the Systems Engineering Forum. According to DOD officials, this forum is responsible for facilitating information sharing and discussion among DOD components about their respective SSPI efforts.

OSD has also established several software technical working groups that meet at least yearly to facilitate discussion among components on steps and actions needed to address identified software and system acquisition and development weaknesses. For example, OSD hosted a conference in 2006 to identify, among other things, SSPI issues, barriers, and recommendations. According to an OUSD(AT&L) official, this conference raised DOD-wide awareness on significant software and system engineering and management issues, such as ineffective requirements management, system engineering decisions being made without full participation of software engineers, and insufficient quantity and quality of software engineering expertise within the department.

Military Departments Have Partially Satisfied Statutory SSPI Requirements and Relevant Guidance

The military departments have largely satisfied the SSPI statutory requirements that apply to them, although in doing so they have not always followed key aspects of SEI guidance that provide for adopting a corporate and strategic approach to process improvement. Specifically, each military department has established an SSPI program or organization, although only one, the Army, did so within the statutorily specified time frame. Further, all have largely met the requirements relating to ensuring that key program personnel have an appropriate level of experience or training in software acquisition, documenting certain software and system process areas, and ensuring that acquisition programs adhere to such documented process areas. However, even though each has taken steps to provide for defining and collecting process improvement performance

Military Departments Have Established SSPI Programs, although Two Did Not Meet Statutory Deadline for Doing So

measures, none are actually using the related metrics for continuous improvement, as provided for in the law. Reasons cited by military department officials varied from changes in senior leadership impeding program continuity to some of the statutory requirements not being viewed as necessary. This means that the military departments have not fully implemented section 804, and have thus limited the potential value to be derived from their SSPI efforts.

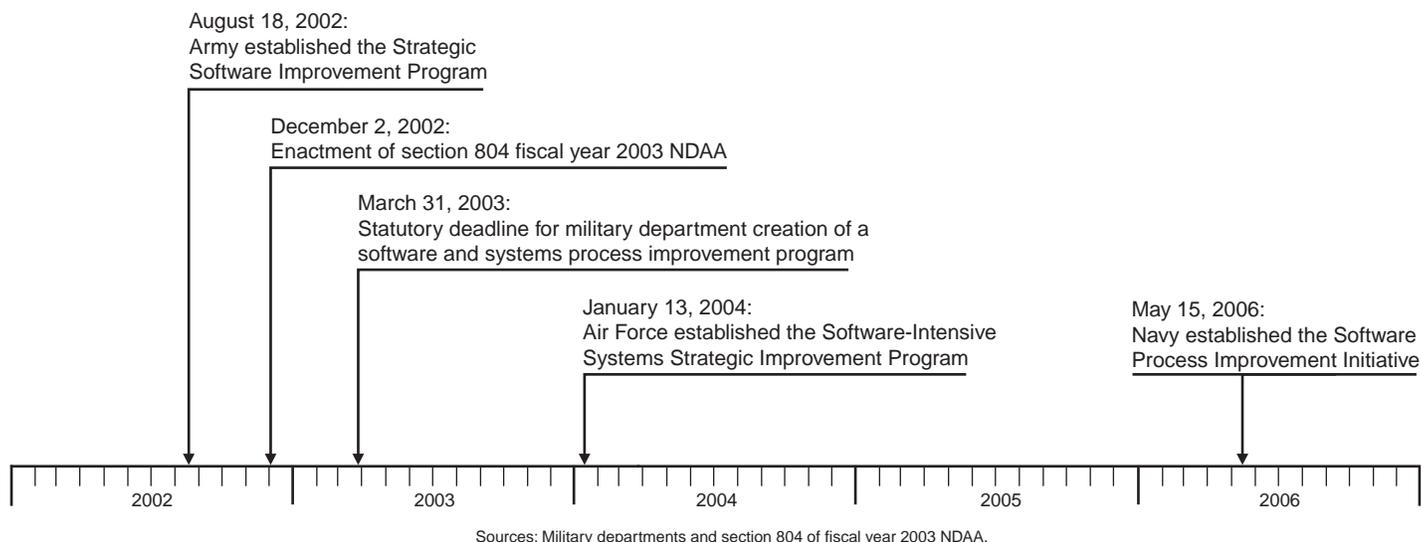
The statute required the military departments to establish process improvement programs within 120 days of the statute's enactment.²¹ When establishing an SSPI program, relevant guidance such as SEI's IDEAL^{SM22} model advocates having a program management structure that includes, among other things, defined program goals and performance measures and a strategic action plan to guide the program's implementation. According to the model, such a corporate and strategic approach is critical to implementing SSPI effectively and consistently across an organization.

Each of the military departments have established SSPI programs. However, only the Army did so within the statutorily required time frame (see fig. 2). Further, the respective program management structures being employed vary in the extent to which they reflect SEI's IDEALSM model. The military department's respective programs are described below.

²¹Pub. L. No. 107-314 was enacted on December 2, 2002. Section 804(a) required, among other things, that the military departments establish SSPI programs within 120 days, or by March 31, 2003.

²²CMU/SEI-96-HB-001.

Figure 2: Timeline of Establishment of SSPI Programs



- The Army Strategic Software Improvement Program was established in August 2002, which is prior to the statute's enactment. The goal of this program is to institutionalize improved development and business processes across the Army, and to lower costs, reduce cycle times, and enhance the performance of software-intensive systems. The program is overseen by the Army Strategic Software Improvement Program Senior Steering Group, which includes the Assistant Secretary of the Army for Acquisition, Logistics, and Technology Military Deputy and program executive officers (PEO).²³ Shortly after the Army's program was created, it assessed the state of the Army's software-intensive system acquisitions (fiscal years 2003 and 2004), and based on these assessments, it developed a Strategic Software Improvement Master Plan. Among other things, this strategic action plan provided an Army-wide roadmap for adopting and institutionalizing software-related best practices, training, continuous improvement, and research. It is updated annually to establish specific program objectives and commitments for that year. The Army has also required its PEOs to develop and implement program-specific SSPI plans that are linked to the goals of the Strategic Software Improvement Master Plan. According to Army officials, about 45 percent of the PEOs have

²³PEOs are responsible for overseeing a related group of major system acquisitions.

approved program-specific plans, and implementation of the plans is regularly tracked by PEOs and the Army senior software acquisition manager.

- The Air Force Software-Intensive Systems Strategic Improvement Program was established in January 2004, about 9 months later than the statute required. The goal of this program is to evaluate the effectiveness and progress of software management and processes for software-intensive system acquisitions and to form strategies and recommendations for improving Air Force software processes. The program is overseen by a working group that consists of Air Force software experts and engineers. Since it was established, the program issued guidance in September 2004 for improving software acquisition processes by having PEOs address 10 software process focus areas, including requirements development and management and risk management. To assist PEOs and program managers in improving software-related acquisitions, the program has also issued a guidebook on Weapons System Software Management. In contrast to the Army, the Air Force has not developed a departmentwide strategic action plan to guide process improvement implementation, as advocated by SEI.
- The Navy established its Software Process Improvement Initiative program in May 2006, which is over 3 years after the date specified in statute for doing so. According to Navy officials, changes in senior leadership impeded efforts to establish the program sooner. The purpose of the program is to evaluate existing software-related policies and procedures and to implement process improvements. The program is led by a steering group, which is headed by the Assistant Secretary of the Navy for Research, Development and Acquisition Chief Engineer and composed of senior engineers. It also consists of five focus teams, each of which is led by senior engineers. The teams' respective areas of focus are software acquisition management, software systems engineering, software development techniques, business implications, and human resources. These teams are to, among other things, draft software policy documents; develop software metrics; research and evaluate software development methodologies; examine business, acquisition, and contracting strategies and practices; and refine the required skills and capabilities needed by government software acquisition and engineering professionals. Through these Software Process Improvement Initiative steering group and team efforts, the Navy has issued a range of guidance and policies aimed at improving its software and system development and acquisition activities, including guidance and policy pertaining to software metrics, organizational staffing, and contract language. Similar to the Air Force, however, the Navy has yet to develop a departmentwide strategic action plan to guide its process improvement activities.

Military Departments Have Largely Met the Remaining Statutory Requirements

Notwithstanding that each military department now has an SSPI program, two departments were late in doing so, which in turn delayed their opportunities to exploit the benefits that the programs can produce. Moreover, the Air Force and Navy programs do not have the kind of strategic and corporate management structures that reflect recognized guidance, such as having a strategic plan to guide program implementation, thus increasing the risk that their SSPI efforts will not produce optimal results.

The statute²⁴ also required each military department to ensure that its software acquisition process improvement program include, at a minimum, (1) documented processes for software acquisition planning, requirements development and management, project management and oversight, and risk management; (2) efforts to develop appropriate metrics for performance measurement and continual process improvement; (3) a process to ensure that key program personnel have an appropriate level of expertise or training in software acquisition; and (4) a process to ensure implementation and adherence to established processes and requirements relating to the acquisition of software. The extent to which the military departments have satisfied these four requirements varies, but all have met most of them. Reasons that department officials cited for not fully meeting certain requirements vary. To the extent that a military department has not fully met a given requirement, it is not in compliance with section 804 and, as a result, has increased the risk of its acquisition programs experiencing cost overruns and schedule delays due to software-related process weaknesses.

²⁴Pub. L. No. 107-314, § 804(b) (Dec. 2, 2002).

Military Departments Have Documented Processes Addressing Four Software Process Areas

The statute²⁵ requires the military departments to document processes²⁶ addressing four key software areas—software acquisition planning, requirements development and management, project management and oversight, and risk management. These four process areas are recognized as important in relevant guidance, such as SEI's CMMI model, DOD's system acquisition policy and guidance,²⁷ and OSD's SSPI guidelines and expectations.

Each of the military departments has issued guidance that recognizes the importance of software acquisition planning, requirements development and management, project management and oversight, and risk management. Moreover, while their respective guidance documents do not define the full range of practices associated with each process area that SEI's CMMI does, they do reference and are linked to DOD acquisition policy and guidance, which we reported in 2004 do address the acquisition planning and the requirements development process areas, and partially address the project management and oversight and the risk management areas.²⁸ Further, since our 2004 report, DOD has issued supplemental guidance pertaining to risk management²⁹ that addresses the range of key risk management practices advocated by SEI. In addition, the Air Force and the Navy have also issued risk management guidance that describe these SEI CMMI key practices, such as identifying program risks, analyzing the likelihood of each risk actually occurring and its impact, and developing and implementing risk mitigation strategies. (See table 1 for a

²⁵Pub. L. No. 107-314, § 804(b)(1) (Dec. 2, 2002).

²⁶As defined by SEI, a process area represents a cluster of related practices that, when implemented correctly, satisfies a set of goals considered important for making improvement in that area. For example, the requirements development and management process area includes clusters of practices for the elicitation, refinement, documentation, and management of requirements for a system or software product.

²⁷DOD Directive 5000.1, *The Defense Acquisition System*, DOD Instruction 5000.02, *Operation of the Defense Acquisition System*.

²⁸GAO, *Information Technology: DOD's Acquisition Policies and Guidance Need to Incorporate Additional Best Practices and Controls*, [GAO-04-722](#) (Washington, D.C.: July 30, 2004).

²⁹DOD, *Risk Management Guide for DOD Acquisition, Sixth Edition* (Version 1.0), August 2006.

summary of the extent to which each military department has addressed the four software areas.)

Table 1: Extent to which Military Departments Have Documented Processes for Each Key Software Area

Military department	Software acquisition planning	Requirements development and management	Project management and oversight	Risk management
Air Force	Fully	Fully	Partially	Fully
Army	Fully	Fully	Partially	Fully
Navy	Fully	Fully	Partially	Fully

Source: GAO analysis based on DOD data.

By largely complying with section 804 and SEI guidance, the military departments are better positioned to effectively carry out these four key software process areas, thereby increasing their chances of successfully delivering promised program capabilities on time and within budget.

Military Departments Have Established Efforts to Allow Software Performance Measurement and Improvement, but Related Metrics Are Not Being Collected and Used

The statute³⁰ requires the military departments to establish efforts to develop appropriate metrics for performance measurement and continual process improvement. Relevant guidance, such as SEI's IDEALSM model and OSD SSPI guidelines and expectations, also recognizes the importance of adopting a corporate approach to such measurement. For example, the SEI model states that process improvement activities should have metrics for monitoring progress against organizational goals, and the OSD guidelines state that appropriate measures should be collected and used to determine the success or failure of SSPI efforts.

The military departments have undertaken efforts to develop SSPI-related performance metrics, as required by the statute. However, they are not currently using the metrics for continuous process improvement, as also required by the statute. Each of the military department's efforts is described below.

³⁰Pub. L. No. 107-314, § 804(b)(2) (Dec. 2, 2002).

-
- According to Army officials, the Army began a departmentwide effort to determine and implement metrics for software acquisition process improvement in 2004. However, they described the effort as not successful because the data that were collected for these metrics were not sufficiently consistent to permit meaningful departmentwide analysis. As a result, the Army ended these efforts, and instead provided its commands discretion in how each developed and collected process improvement metrics.
 - The Air Force began efforts to develop and collect software core metrics in 2004. However, similar to the Army, it left development and collection of process improvement metrics to the discretion of each PEO, rather than adopting a more corporate approach. According to Air Force guidance, devolving this to the PEOs was due to the fact that the section 804 requirement was considered subjective and not addressed in detail in OSD's guidance. As a result, the metrics that were established and used have varied across the program offices.
 - The Navy began an effort to develop and collect process improvement measures in 2008. Specifically, it issued a policy in July 2008 that directs all programs that have a software component to define and collect a set of core metrics covering, for example, software quality, and to report these metrics at program milestone reviews. According to Navy Software Process Improvement Initiative officials, programs have begun to report these metrics. They added that the data reported will be used to, among other things, assess the effectiveness of the Navy's process improvement program.

While each of the military departments has satisfied the statute's requirement to establish efforts to permit software-related measurement and improvement, none of these efforts has progressed to the point that it is actually being used to understand how well the departments' respective SSPI programs are achieving expected outcomes and having an impact. Further, the Army and Air Force efforts are diffused across its commands and PEOs, respectively, and thus do not reflect the kind of corporate approach to process improvement measurement advocated by relevant guidance.

Until each military department has established appropriate metrics and used them to understand the organizational impact of their respective SSPI programs, each will be challenged in its ability to better focus its SSPI efforts and thereby maximize their potential value.

Military Departments Have Established Processes for Ensuring Program Personnel Are Trained and Experienced

The statute³¹ requires each military department to establish a process to ensure that key program personnel have an appropriate level of expertise or training in software acquisition. Relevant guidance, such as SEI's CMMI model, DOD's acquisition policy and guidance, and OSD's SSPI memo, also address the importance of ensuring that key acquisition personnel are trained.

All three military departments require that each program manager have processes aimed at ensuring that program personnel have a certain level of experience and/or training in relevant software disciplines. For example, the Assistant Secretary of the Navy for Research, Development, and Acquisition issued a memorandum in September 2008 that requires that the Navy's acquisition workforce be trained in Defense Acquisition University-defined software-related core competencies, and that its program managers ensure that program personnel meet certification requirements. Similarly, the Army and Air Force require their PEOs to ensure that acquisition personnel are certified in the relevant acquisition career field and at the required level.

Moreover, each department has process steps aimed at verifying that these personnel have met requisite training or experience requirements. For example, each has established guidance for system acquisition program milestone reviews that requires, among other things, determining whether personnel with the needed skills, experience, and certifications are available.³² Furthermore, each captures and maintains certification information on all its personnel, which are used for workforce planning and assignment.

By having processes for ensuring that key personnel have appropriate levels of expertise or training, the military departments have not only satisfied the statute, but have also increased the chances that their acquisition programs can be successful.

³¹Pub. L. No. 107-314, § 804(b)(3) (Dec. 2, 2002).

³²This guidance employs the Probability of Program Success model, which is intended to determine the ability of a program to deliver a specified capability, within approved cost and schedule limits, that meets the performance levels mandated by the warfighter.

Military Departments Have Processes to Ensure that Acquisition Programs Implement Defined Software Processes and Requirements, but They Do Not Incorporate Key SEI Verification Steps

The statute requires³³ each military department to establish a process to ensure that its acquisition programs implement and adhere to defined software processes and requirements. Relevant guidance, such as SEI's CMMI model and OSD's SSPI guidance, also stresses the importance of evaluating both individual program and institutional adherence to defined software processes and requirements.

Each of the military departments has processes for ensuring that its programs follow defined software and system development and acquisition processes, as required by the statute. Specifically, each has issued guidance that provides for, among other things, reporting implementation progress and problems in such key process areas as acquisition planning, requirements development and management, program management and oversight, and risk management. Among other things, this reporting includes the status of a program's technology development strategy, key requirements documents, cost estimates, and risk mitigation activities.

However, the department's guidance does not include the range of verification steps that are provided for in SEI's CMMI model, which is referenced in OSD's SSPI guidance. Specifically, the CMMI model provides for conducting detailed and documented evaluations of the extent to which key software processes are being followed. Moreover, these evaluations are typically performed by an organization external to the program, and include analysis of the range of key practices that comprise a given process area. Officials with each of the military departments told us they do not conduct such evaluation activities to verify that programs conform to established software processes and requirements, and do not believe that such verification activities are appropriate. According to these officials, the combination of requiring programs to adhere to established software-related processes and requirements and the attention to this adherence at program reviews is sufficient to reasonably ensure that programs adhere.

³³Pub. L. No. 107-314, § 804(b)(4) (Dec. 2, 2002).

Without the range of process adherence verification advocated by SEI, the military departments lack a level of assurance that SEI's research has shown is needed. As discussed in the next section, our reviews of software-intensive DOD acquisition programs show that many fail to fully implement and thus adhere to key software-related processes. This means that the level of process adherence assurance that occurs under the military departments' current program review guidance is not always sufficient, and therefore may allow for process weaknesses that in turn increase the chances of program cost, schedule, and performance shortfalls.

DOD Does Not Know Impact of SSPI Efforts but Studies of Large-Scale Acquisition Programs Show that Performance Shortfalls and Process Weaknesses Continue

As previously noted, neither OSD nor the military departments are using performance measures to understand how well the department's collective SSPI efforts are meeting goals and producing expected outcomes, and thus DOD officials told us they do not know the corporate impact of these efforts. This void in SSPI-related measurement is not consistent with either the statute, which requires that each military department develop SSPI performance measures, or SEI's IDEALSM and CMMI models, which state that measurements are key to effectively monitoring and evaluating the impact of process improvement. OSD and military department officials cited various reasons for not measuring the impact of their SSPI efforts, including difficulties in obtaining accurate information from their respective programs and the subjective nature of performance measurements that have been defined. By not knowing the impacts accruing from these efforts, the department is not positioned to maximize the potential of its SSPI efforts.

In the absence of DOD knowledge of the impact of its SSPI efforts, studies by us and others of the department's major system acquisition programs suggest that these programs have yet to fully realize the benefits from the kind of SSPI required by section 804 and advocated by SEI. In particular, we recently reported that as of March 2009, DOD's large-scale, software-intensive system acquisitions continue to fall short of cost, schedule, and performance expectations. Specifically, in 2008, DOD's portfolio of major defense acquisition programs experienced average delays in delivering initial operational capabilities of 22 months, which is a 4-month increase in delays compared to 5 years ago. Moreover, these programs collectively overran their cost estimates by about \$296 billion,³⁴ which is greater than

³⁴GAO, *Defense Acquisitions: Assessments of Selected Weapon Programs*, [GAO-09-326SP](#) (Washington, D.C.: Mar. 30, 2009).

comparable overruns experienced 5 years ago. Relatedly, we continue to report on weaknesses in the extent to which a range of programs has implemented system and software acquisition and development processes, including weaknesses in the four key process areas that the act specifically referenced as SSPI focus areas—acquisition planning, requirements development and management, program management and oversight practices, and risk management. These process implementation weaknesses are described below.

Software Acquisition Planning

One of the purposes of acquisition planning is to establish and maintain the plans that govern the execution of acquisition programs. Among other things, it includes defining work products and tasks as well as estimating needed resources and schedules, negotiating contractor and stakeholder commitments, and identifying and analyzing risks associated with delivering work products and executing tasks. Acquisition planning is important because it results in plans and estimates that provide the basis for executing programs and measuring performance. For example, estimates of program cost and effort, which are generally based on results of analysis using models or historical data applied to size, activities, and other planning parameters, are used to develop budgets and control costs and schedules during program execution.

Our work continues to show that the department is challenged in its efforts to effectively perform the key practices associated with the acquisition planning key process area. For example, we recently reported that the Navy Enterprise Resource Planning (Navy ERP) program did not develop a life cycle cost estimate in accordance with relevant guidance.³⁵ More specifically, we reported that Navy ERP's cost estimate was not grounded in a historical record of comparable data from similar programs and was not based on a reliable schedule baseline, both of which are necessary to having a cost estimate that can be considered credible and accurate. We concluded that these acquisition planning limitations could result in actual program costs continuing to exceed the estimates, and made recommendations to address each limitation. DOD largely agreed with our recommendations.

³⁵GAO, *DOD Business Systems Modernization: Important Management Controls Being Implemented on Major Navy Program, but Improvements Needed in Key Areas*, [GAO-08-896](#) (Washington, D.C.: Sept. 8, 2008).

Similarly, we recently reported that the Global Combat Support System-Marine Corps (GCSS-MC) also had not developed a life cycle cost estimate that was grounded in a historical record of comparable data from similar programs, and it did not account for significant risks associated with the program's aggressive schedule, both of which limited the estimate's credibility and accuracy.³⁶ As a result, we concluded that the Marine Corps did not have an adequate basis for informed investment decision making, and that actual program costs would likely not be consistent with estimates. Accordingly, we made recommendations aimed at addressing each of these weaknesses. DOD agreed with our recommendations.

Requirements Development and Management

Well-defined and managed requirements are recognized by DOD directives and guidance and other relevant guidance as essential.³⁷ Effective requirements development and management includes, among other things, (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 bidirectional 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. Effective requirements development and management is important because requirements provide the cornerstone of any new system development or acquisition program.

Our work continues to show that the department is challenged in its efforts to effectively perform key practices associated with the requirements development and management key process area. For example, we recently reported that the Navy's program for creating cashless environment on ships, known as Navy Cash, had not defined and implemented key practices for developing and managing requirements, and thus was without basic requirements documentation needed to inform program cost and schedule estimates and accomplish work associated

³⁶GAO, *DOD Business Systems Modernization: Key Marine Corps System Acquisition Needs to Be Better Justified, Defined, and Managed*, [GAO-08-822](#) (Washington, D.C.: July 28, 2008).

³⁷DOD, *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).

with delivery of needed system capabilities.³⁸ In particular, the program had not defined how system requirements were to be managed and who would be responsible for managing them. Instead, the program had adopted a reactive approach to developing and managing requirements that consisted of considering requests for requirements changes proposed as part of the program's change control process. As a result, we concluded that Navy Cash could not develop and measure performance against meaningful cost, schedule, and capability baselines, and could not reliably ensure that the system would meet expectations or that those responsible for it could be held accountable for results. Accordingly, we made recommendations to address these limitations, which DOD agreed to implement.

Similarly, we recently reported that the Army Future Combat System program had not adequately developed and managed requirements.³⁹ Specifically, during the system's initial stages of development, the program did not establish firm requirements and preliminary designs to meet requirements. Consequently, after more than 5 years, the Army was still seeking to stabilize system designs at a time when the program was already past the midpoint of the development phase, which is the point when a program would normally be demonstrating a stable design capable of meeting performance requirements. We concluded that the program would likely need to relax system design requirements in order to stay within schedule commitments. Accordingly, we made recommendations to address each limitation. DOD agreed with the recommendations.

Recent DOD studies have also identified deficiencies in requirements development and management practices that have resulted in cost overruns and schedule delays. For example, a September 2008 DOD briefing stated the cost of these system acquisitions has grown by 33 percent over the past 10 years due to, among other things, insufficient requirements analysis.

³⁸GAO, *DOD Business Systems Modernization: Planned Investment in Navy Program to Create Cashless Shipboard Environment Needs to Be Justified and Better Managed*, [GAO-08-922](#) (Washington, D.C.: Sept. 8, 2008).

³⁹GAO, *Defense Acquisitions: Decisions Needed to Shape Army's Combat Systems for the Future*, [GAO-09-288](#) (Washington, D.C.: Mar. 12, 2009).

Program Management and Oversight

The purpose of program management and oversight is to understand a program's progress against commitments so that any needed corrective actions can be taken. Among other things, program management and oversight consists of comparing the actual cost, schedule, and quality of work products and tasks to plans and estimates; determining whether significant deviations exist; and developing corrective actions, if necessary, to address the deviations. One accepted technique for managing and overseeing program performance is earned value management (EVM), which is a means for determining and disclosing actual work completed in comparison with cost and schedule estimates.

Our work continues to show that the department is challenged in performing key practices related to the program management and oversight key process area. For example, we recently reported that the Navy ERP program had not performed basic EVM activities, such as conducting integrated baseline reviews of its cost and schedule estimates,⁴⁰ resulting in actual program costs and schedules that did not track to estimates. Similarly, we recently reported that GCSS-MC's was not effectively performing EVM because its schedule baseline was not reflective of important practices, such as conducting a schedule risk assessment or allocating schedule reserve.⁴¹ As a result, we concluded that actual program cost and schedule figures will not be consistent with estimates, and will not provide an adequate basis for informed investment decision making. Accordingly, we made recommendations to address each limitation, which DOD agreed to implement.

DOD has also found that program management and oversight process deficiencies were impacting major acquisitions. For example, a September 2008 DOD briefing⁴² on system acquisition software problems states that over the past 11 years, the department incurred system estimation changes totaling approximately \$201 billion, systems engineering changes totaling approximately \$147 billion, and systems schedule changes totaling approximately \$70 billion. To understand the cause of these shortfalls, DOD performed related analysis that identified problems with management and oversight of programs' integrated master plans, integrated master schedules, EVM data, and risk management.

⁴⁰[GAO-08-896](#).

⁴¹[GAO-08-822](#).

⁴²DOD, *Software Problems Found on DOD Acquisition Programs*, September 2008.

Risk Management

DOD and relevant guidance⁴³ recognize the importance of performing effective program risk management. 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 management; and (4) examining the status of identified risks during program milestone reviews. Risk management is important because it focuses on avoiding problems and their associated cost and schedule impacts before they occur.

Our work continues to show that the department is challenged in its efforts to effectively manage risk. For example, we recently reported that the Navy Cash program had not developed plans, processes, or procedures to identify, mitigate, and disclose risks, nor had it assigned risk management roles and responsibilities to key stakeholders.⁴⁴ As a result, the program was not proactively attempting to avoid the occurrence of cost, schedule, and performance problems, but rather was reacting to the consequences of actual problems. To address these limitations, we made a number of recommendations, which DOD agreed to implement.

Similarly, we recently reported that while the Navy ERP program had defined and established a process for proactively avoiding problems, it had not effectively implemented risk mitigation strategies for some significant risks, such as those associated with data conversion and organizational change management.⁴⁵ As a result, operational testing of the system at the first user organization revealed significant problems that required additional resources and time to correct. In addition, we reported that not all known risks had been included in the risk inventory, such as not having adequately implemented program-level EVM. We concluded that not having effectively addressed such risks had not only contributed to existing schedule delays but would also likely contribute to future cost and schedule shortfalls. To address these limitations, we made a number of recommendations, which DOD agreed to implement.

⁴³DOD, *Risk Management Guide for DOD Acquisition, 6th Edition, Version 1.0*, and Software Engineering Institute, *CMMI for Acquisition, Version 1.2* CMU/SEI-2007-TR-017 (Pittsburgh, Pa., November 2007).

⁴⁴[GAO-08-922](#).

⁴⁵[GAO-08-896](#).

Conclusions

An SSPI program, if properly defined and implemented, can have a positive impact on the quality and cost of software-intensive system acquisition and development programs. In the case of DOD, such impacts could be significant given the enormous size and mission significance of its many programs. Congress has recognized this tremendous potential by directing OSD and the military departments and defense agencies to take a range of statutorily defined SSPI-related steps. To their credit, OSD and the military departments have satisfied a number of these statutory requirements, but they have not satisfied them all. Moreover, they also have not fully satisfied key aspects of relevant guidance associated with well-managed SSPI programs to include measuring the impact of their collective efforts. As a result, DOD does not know whether it is meeting organizational SSPI goals and achieving desired institutional outcomes, and thus whether program changes are warranted. Given that studies by us and others continue to identify weaknesses in DOD's implementation of key software and systems development and acquisition process areas, the department has yet to realize the full potential of an effectively and efficiently managed corporate approach to SSPI.

While the reasons cited by OSD organizations and the military departments for not fully satisfying SSPI statutory requirements and relevant guidance vary, they can be traced to a lack of a DOD-wide strategic approach to SSPI that includes strong central leadership and strategic planning. Such an approach is reflected in the statute and relevant guidance, and includes departmentally assigned and endorsed responsibilities and authorities, clearly defined strategic plans and performance measures, and rigorously enforced accountability mechanisms. Until DOD adopts such an approach, it will continue to fall short of statutory requirements and relevant guidance, and will thus not be positioned to reap the potential benefits promised by properly defined and implemented SSPI efforts.

Recommendations for Executive Action

To strengthen DOD's management of its SSPI efforts, we recommend that the Secretary of Defense direct the ASD(NII)/CIO and the USD(AT&L), in concert with the military departments and defense agencies, to

- jointly develop a DOD-wide strategic plan, and supporting organizational component plans, for ensuring that all of the requirements in section 804 of the 2003 NDAA, as well as relevant SEI guidance, are fully implemented; and

-
- jointly and periodically report to the congressional defense committees on their progress in implementing the plan and the impacts of doing so.

Agency Comments and Our Evaluation

In written comments on a draft of this report, signed by the Acting Director of Systems Engineering and reprinted in appendix II, the department described our report as important and insightful, adding that it provides useful feedback on DOD's software acquisition practices that may require improvement. In addition, it committed to promoting and applying process improvement across the department in support of the fiscal year 2003 NDAA section 804 process improvement provisions and DOD's system engineering efforts. To this end, it stated that it will consider our findings and that it partially agreed with our two recommendations.

In partially agreeing with our first recommendation, DOD stated that it agrees that it needs to formalize the DOD-wide process improvement activities that its Software Working Group has under way, and to do so, it will do an analysis comparing these activities to the section 804 requirements, and it will develop objectives and a plan to respond to our recommendations. However, DOD commented that it does not believe that a DOD-wide strategic plan is needed to meet the section 804 requirements. Further, it said that the SEI guidance that our report references should not be seen as a panacea, noting that other techniques exist and are used within the department and that section 804 does not require any specific techniques or methodologies. In response, we support DOD's planned actions and agree with most of its comments, as they are consistent with the intent of our recommendation. Specifically, we agree that section 804 does not require a specific technique or methodology. Further, we agree that the SEI guidance that our recommendation references is neither a panacea nor the only available technique or methodology. Accordingly, our recommendation specifically provides for using *relevant* SEI guidance, and it does not preclude using other available guidance. Further, while we agree that section 804 does not require a strategic plan, we would note that our report identifies the root cause of DOD's currently decentralized and inconsistently pursued range of SSPI efforts as being a lack of a corporate and strategically driven approach to process improvement, that includes clearly assigned responsibility and accountability for achieving strategic outcomes and results across the heterogeneous, component-based process improvement activities. As a result, the full intent of our recommendation is aimed at having the department adopt a more strategic and coordinated approach to SSPI, which is consistent with section 804. While the department's planned actions to address our recommendation would be

part of such an approach, they alone are not sufficient. Therefore, we would encourage DOD to fully implement our recommendation.

In partially agreeing with our second recommendation, DOD stated that it would periodically report to its congressional committees on its progress in implementing the section 804 requirements, as we recommended, and would do so through a new report that DOD is to provide under a recently enacted public law. However, it stated that this reporting will be limited to its plans for addressing our first recommendation. Moreover, it added that its efforts to respond to both of our recommendations will not extend beyond software acquisition process improvement, and thus will not include system-related process improvement, which it stated our report includes. In this regard, the department stated that section 804 only calls for software acquisition process improvement. We support DOD's use of this existing reporting mechanism, but again encourage the department to implement the full scope of our first recommendation for the reasons discussed above, and to also report in line with the full scope of our recommendation. Further, we encourage the department to not limit its process improvement activities to software acquisition. As our report states, section 804 is consistent with the SSPI recommendations that we made to DOD in 2001,⁴⁶ and these recommendations extend to software and system development and acquisition. Further, section 804 specifically uses the terms software acquisition and development, and it specifically refers to defense programs with a substantial software component, which are in fact defense systems that are intensively dependent on software.

DOD also provided technical comments on a draft of this report that we have incorporated throughout the report, as appropriate.

⁴⁶[GAO-01-116](#).

We are sending copies of this report to interested congressional committees. We will also send copies to the Secretary of Defense and the Director of the Office of Management and Budget. Copies of this report will be available at no charge on the GAO Web site at www.gao.gov.

Should you or your offices have any questions on matters discussed in this report, please contact me at (202) 512-3439 or at hiter@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix III.



Randolph C. Hite
Director, Information Technology Architecture
and Systems Issues

Appendix I: Objectives, Scope, and Methodology

Section 804 of the Bob Stump National Defense Authorization Act for fiscal year 2003¹ required the Department of Defense (DOD) to establish process improvement programs for its military departments and defense agencies that manage major acquisition programs. Our objectives were to assess: (1) the extent to which DOD has implemented the process improvement provisions of the act, and (2) the impact of DOD's process improvement efforts. The scope of work focused on the efforts and activities of the Office of the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer (OASD(NII)/CIO) and the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD(AT&L)), because both have responsibility for, among other things, software and system process improvement, oversight of major acquisition programs, and establishment of policies and procedures related to software and system acquisition.² Our scope also focused on the Departments of the Army, Air Force, and Navy, and did not include any defense agencies, because as of October 2008 about 99 percent of DOD's major programs were being managed by either the military departments or DOD (only one major acquisition program was being managed by a defense agency).

To address the first objective, we reviewed relevant ASD(NII)/CIO and USD(AT&L) and military department process improvement and system acquisition policies, guidance, plans, oversight controls, and performance measures. We also interviewed responsible officials within each of these organizations concerning their respective efforts to address relevant aspects of the act. We then compared their respective efforts to the provisions in the act as well as other relevant guidance, such as the Software Engineering Institute's IDEALSM and Capability Maturity Model Integration models. Where we found deviations, we interviewed responsible officials to determine reasons for the deviations.

To address the second objective, we reviewed available documentation and interviewed officials from OASD(NII)/CIO, OUSD(AT&L), and the military departments concerning efforts to determine the impact of their respective and collective process improvement efforts. In addition, we reviewed recently issued GAO reports and DOD assessments addressing

¹Pub. L. No. 107-314, § 804 (Dec. 2, 2002).

²The ASD(NII)/CIO was formerly known as the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)). The act specifically cites ASD(C3I).

software-related process and practice weaknesses and program cost and schedule outcome changes.

We conducted this performance audit at DOD and military department offices in Arlington, Virginia, from December 2008 through September 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Defense



OFFICE OF THE DIRECTOR OF
DEFENSE RESEARCH AND ENGINEERING
3040 DEFENSE PENTAGON
WASHINGTON, DC 20301-3040

AUG 26 2009

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

Dear Mr. Hite:

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-09-888, "INFORMATION TECHNOLOGY: DoD Needs to Strengthen Management of its Statutorily Mandated Software and System Process Improvement Efforts," dated July 22, 2009 (GAO Code 310664). Detailed comments on the report recommendations are enclosed.

The Department thanks the GAO for this insightful draft report and the recommendations, which we can continue to fold into our systems engineering revitalization efforts. We believe it is an important report, as it gives Congress more visibility into our continuing efforts to improve systems engineering across the defense acquisition community. The draft report provides useful feedback about software acquisition areas that may still require improvement, and we will take the findings from this report in consideration as we continue to monitor our software acquisition practices.

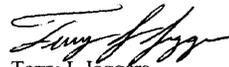
It is important to note that while the Software Engineering Institute's specific process improvement techniques highlighted may improve insight and impose better controls over software development; they should not be seen as a panacea. Significant challenges associated with acquisition and sustainment of complex defense systems are not always well served by generalizing software development and process improvement across programs; it is important to take into account a program's acquisition characteristics (size, complexity, stage of development, technology precedent, team makeup, length of service). The Department has conducted a number of root-cause analyses to show that many problems attributed to software were not caused by software processes, but to other factors outside the realm of Section 804. We will continue to address software issues in our program support reviews, and as part of our acquisition oversight activities.

1

In addition, DoD's organization-wide Continuous Process Improvement program, codified in DoDI 5010.43, *Implementation and Management of the DoD-Wide Continuous Process Improvement/Lean Six Sigma (CPI/LSS) Program*, cites process improvement techniques such as lean six sigma, theory of constraints, and business process reengineering. Although many such improvement initiatives have been implemented across DoD, we have learned that imposing a specific process improvement methodology across the board does not well serve the needs of the wide diversity of complex acquisition programs. Further, the Section 804 legislation did not require any specific software acquisition process improvement techniques or methodologies, as the report implies.

We will continue to promote and apply process improvement across our DoD acquisition programs as warranted and to improve software acquisition in support of the 2003 NDAA Section 804 and our systems engineering efforts.

Sincerely,



Terry J. Jagers
Acting Director
Systems Engineering

Enclosure:
As stated

GAO DRAFT REPORT DATED JULY 22, 2009
GAO-09-888 (GAO CODE 310664)

“INFORMATION TECHNOLOGY: DoD Needs to Strengthen Management of its
Statutorily Mandated Software and System Process Improvement Efforts”

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense direct the Assistant Secretary Defense for Networks and Information Integration/Chief Information Officer (ASD(NII)/CIO) and the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), in concert with the military departments and defense agencies, to jointly develop a DoD-wide strategic plan, and supporting organizational component plans, for ensuring that all of the requirements in Section 804 of the Bob Stump National Defense Authorization Act for FY 2003, as well as relevant Software Engineering Institute guidance, are fully implemented.

DOD RESPONSE: Partial Concur. The DoD agrees with continuing to track the progress of the implementation of all the requirements of Section 804 and plans to do so by formalizing many of the activities ongoing in the DoD-wide Software Working Group (SWWG). The DoD will do a gap analysis on our implementation of Section 804 to develop objectives and a plan of action to respond to the recommendations. The Department does not believe that a DOD-wide strategic plan is warranted to meet the Section 804 requirements.

Software Engineering Institute (SEI) guidance was not a requirement of the Section 804 legislation. While the DoD has been a sponsor of many of the SEI products, such as the CMMI Product Suite, and continues to support its prudent use, the results of its implementation have not always been as we had hoped when we began its development. In 2007 the Defense Contract Management Agency (DCMA) conducted a study relating Earned Value Management (EVM) data on program performance and the reported CMMI maturity level of the respective programs that reported less than positive results. SEI guidance will simply continue to provide guidance for our efforts, not govern them.

DoD Proposed Revision of Recommendation 1: The GAO recommends that the Secretary of Defense direct the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), and the Assistant Secretary Defense for Networks and Information Integration/Chief Information Officer (ASD(NII)/CIO), in concert with the military departments and defense agencies, to jointly conduct a gap analysis to prepare objectives and a plan of action focused on implementation of the specific requirements of Section 804 of the FY 2003 National Defense Authorization Act.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense direct the ASD(NII)/CIO and the USD(AT&L), in concert with the military departments and defense agencies, to jointly and periodically report to the congressional defense committees on its progress in implementing the plan and the impacts of doing so.

DOD RESPONSE: Partial Concur. DoD will address this reporting in accordance with our recommended revision of Recommendation 1 and the Section 804 requirements. Such reporting will be through the new Joint Developmental Test/Systems Engineering (DT/SE) Capabilities Report that DoD is to provide to Congress on a periodic basis per the Weapon Systems Acquisition Reform Act of 2009 (Public Law 111-23).

Section 804 calls for software acquisition process improvement, which is what we will be judging in our reporting. The GAO report frequently addresses software and systems process improvement (SSPI). No inference should be made that DoD will perform oversight of SE capability the same way we oversee improvement of the software acquisition processes for these reporting requirements.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Randolph C. Hite, (202) 512-3439, or hiter@gao.gov

Staff Acknowledgments

In addition to the individual named above, Tonia Johnson (Assistant Director), Sher'rie Bacon, Mathew Bader, Elena Epps, Rebecca Eycler, Franklin Jackson, Freda Paintsil, and Madhav Panwar made key contributions to this report.

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 afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

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

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

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

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

