GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-285626

June 15, 2000

The Honorable John Warner
Chairman
The Honorable Carl Levin
Ranking Minority Member
Committee on Armed Services
United States Senate

Subject: Defense Software: Review of Defense Report on Software Development Best Practices

On March 20, 2000, the Department of Defense provided your Committee with a report on its efforts to adopt management best practices for software development and acquisition. Defense was directed to provide this report by language in the Committee's report to accompany the National Defense Authorization Act for fiscal year 2000, Senate Report 106-50. The requirement was established because the Committee was concerned that DOD had not taken sufficient actions to address costly and long-standing software development and acquisition problems, which have been documented in many GAO, Inspector General, and department studies. Senate Report 106-50 also required GAO to review and comment on Defense's response.[1] This letter provides our comments.

Our objective in reviewing Defense's response was limited to evaluating the response to determine whether (1) it satisfied the committee's directive and (2) the information included was accurate and complete. Because we did not evaluate the effectiveness of Defense's efforts to identify and adopt best practices in software development, our comments do not constitute an assessment of whether Defense's efforts are improving software development. However, we are conducting another review of Defense's management of its software process improvement efforts, and we will provide the Committee with a copy of our report based on that review. Our review of Defense's response was conducted in April and May 2000 in accordance with generally accepted government auditing standards.

[1] The Senate required that Defense deliver a report on this issue by February 1, 2000, and that GAO provide its comments on the report within 60 days.

RESULTS IN BRIEF

In responding to the Committee's directive, Defense was required to report on its efforts to identify and adopt best practices in software development and on its efforts to address six additional issues--ranging from the employment of risk management in software development, to the management of requirements changes, to the development of metrics to help assess performance and pinpoint potential problems, to tracking software development rework expenditures.

Defense's response addressed the Committee's basic question and all six additional issues. However, the responses on some issues were incomplete and others contained inaccurate or outdated information. Specifically, of the seven total issues, Defense's response did not fully address two issues and was inaccurate or outdated on three. Table 1 summarizes of our evaluation of Defense's response.

Table 1: Evaluation of Defense's Responses to Issues in Senate Report 106-50

Issue	Response Addresses Issue?	Response Accurate/ Complete?
Defense efforts to identify and adopt best practices in software development	Yes	Yes
How risk management is used in a project or program's software development process	Yes	No
The process used to control and manage requirements changes during the software development process	Yes	Yes
The metrics required to serve as an early warning of evolving problems, measure the quality of the software product, and measure the effectiveness of the software development or acquisition process	Yes	Yes
Measures used to determine successful fielding of a software product	Partially	Yes
How Defense ensures that duplication of ongoing software development efforts are minimized; and how commercial software and previously developed software solutions are used to the maximum extent practicable	Partially	No
The portion of defense software expenditures used for rework	Yes	No

Defense's response also did not offer additional relevant information that could have improved the report. For example, Defense has begun some initiatives under its goal of building a coherent global network that focus on developing an effective Defense software management program. This information would have provided insight into current and future Defense efforts.

EVALUATION OF INDIVIDUAL SEGMENTS OF THE DEFENSE RESPONSE

The following sections provide our comments on the individual issues.

Defense efforts to identify and adopt best practices in software development

Defense's response addresses the Committee's basic question. In particular, Defense noted that it has established a policy to adopt best practices in software development by requiring software to be managed and engineered using best practices. Also, Defense is currently surveying the industry about best practices in software management, and, as a result of that survey and subsequent analysis, may implement new policy and guidance on software best practices.

In addition, Defense noted that in the future it may increase emphasis on this area by promoting the use of commercial software or other proven software and by establishing a clearinghouse to store existing and proven software components for reuse. Each of these potential initiatives would facilitate the identification and adoption of best practices.

Although defense's response addresses its policy to adopt best practices, implementation of this policy has yet to be formalized. For example, Defense has not provided guidance to software program managers on how to identify or adopt such practices. Also, even though some Defense units have information available on best practices, managers' use of data from such sources is not mandatory. In particular, although the Software Program Manager's Network has developed a 16-point plan of critical software practices, Defense has no formal program implementing the plan. Instead, Defense encourages program managers to take advantage of the network's support.

How risk management is used in a project or program's software development process

Defense's response provides information on both the reporting of risks and the risk management process. The portion of the response dealing with reporting of risks is adequate. Both the Defense Acquisition Executive Summary and the Major Automated Information System reports have the potential to provide system overseers with information on program risk, as determined by the program manager.

However, the portion of the response dealing with the risk management process is not accurate. Specifically, it reflects the use of risk management in the systems engineering and system design processes but not in software development. This is problematic because experience has shown that the software component of major acquisitions (versus hardware or firmware) is the source of most system risk, and the component most frequently associated

with late deliveries, cost increases, and performance shortfalls.[2] Private industry and government organizations have widely recognized this risk by endorsing and accepting the models and methods that define and determine an organization's software process maturity developed by Carnegie Mellon University's Software Engineering Institute (SEI).

The process used to control and manage requirements changes during the software development process

Defense's response addresses the issue. In its comments, Defense notes that individual system acquisition management offices are responsible for change control during software development and the program's software configuration control board is responsible for managing this process. Using such a board is a standard practice in software development. Defense's response did not provide any details about this process or describe the interaction that should take place between acquisition managers and the board.

The metrics required to serve as an early warning of evolving problems, measure the quality of the software product, and measure the effectiveness of the software development or acquisition process

Defense's response addresses the issue. The response discusses current Defense-sponsored software metrics support programs, such as the Practical Software Measurement program and SEI's Software Engineering Measurement and Analysis team. Defense also notes that both the Army and Navy have implemented voluntary metrics programs that identify and collect appropriate metrics to monitor key risk areas.

Defense also has other efforts underway to increase the use of metrics in software-intensive major automated information system programs. For example, Defense is sponsoring independent software assessments of selected major programs, which will provide software development baselines with recommended risk management metrics and strategies for tracking and controlling software development. Also, Defense intends to collect data from completed major programs and use it to both help develop the initial cost and schedule estimates for new programs and to mitigate risk in managing acquisition programs.

Defense officials told us these efforts will be used to develop a core set of software metrics to assist in the measurement and tracking of software process improvements. They also plan to implement automated metrics collections and the use of software analysis tools, depending on future funding and acceptance by Defense components.

[2] *Air Traffic Control: Immature Software Acquisition Processes Increase FAA System Acquisition Risks* (GAO/AIMD-97-47, March 21, 1997).

Measures used to determine
successful fielding of a software product

Defense's response partially addresses the issue but does not provide a complete answer. The response places responsibility for successful fielding of a software product on (1) the contractor developing the product and (2) the individual system maintenance process and the postdeployment software support process. However, Defense's response does not explain how the contracting unit measures the success of the contractor's effort or what, if any, Defense's requirements for maintenance or support are.

Defense's response also identifies several generic measures that could be used to evaluate success—such as maintenance costs or number of software problems reported. However, Defense does not specify whether these measures are required to be developed and/or approved. It also does not discuss what parameters or thresholds might be attached to ensure the effectiveness of the measures (e.g., what maintenance costs are appropriate for systems given functionality, changes in requirements, complexity, and sophistication; what number of software problems are appropriate given similar factors).

Finally, we found that Defense policy requires the use of a software measurement process to assess and improve the software development process and associated software products. While Defense's response does not discuss this policy, information on this policy seems to be more germane to the Committee's question as to how Defense determines successful fielding of a software product.

How Defense ensures that duplication of ongoing software development efforts are minimized; how commercial software and previously developed software solutions are used to the maximum extent practicable

Defense's response partially addresses the issue. Defense discusses two clearinghouse and analysis centers for software that are available to DOD program managers: the Data and Analysis Center for Software and the Defense Technical Information Center. However, there is no mention of any Defense policy or guidance relating to the use of these centers to reduce duplicative software development or that Defense even promotes their use.

Defense's response also identifies a set of 14 software reuse information sources, which provide guidance and a number of plans and strategies on software reuse. However, none of them provide a source of existing and proven software components that would allow managers to act on this guidance. Defense noted in its opening remarks that it may establish a clearinghouse to store existing and proven software components that are ready for reuse. Should Defense establish this clearinghouse, Defense managers would have such a source.

In addition, part of Defense's response is either inaccurate or outdated. It discusses two Defense entities that we were informed are no longer in operation--the Software Reuse Initiative Program Management Office and the Army Software Reuse Center.

The portion of defense software expenditures used for rework

Defense's response addresses the issue, but the information provided may not be fully supported by the available data. Defense states that it does not know the amount of money that it spends on software maintenance annually nor the cost segments that make up this total, such as costs for planned enhancements and costs for problem fixes. Defense also indicates that there is no practical way to separate the amount expended for planned enhancements from that expended for product fixes.

However, an approved Department of Defense journal published a July 1997 article[3] that discussed a Defense unit's effort to track costs associated with product fixes and enhancements. The article discussed why software maintenance planning and management should be formalized and quantified, and it provided a methodology for tracking costs associated with both fixes and modifications for a large Defense system, including the total staff days expended.

ADDITIONAL INFORMATION NOT INCLUDED IN DEFENSE'S RESPONSE

Defense officials separately provided us with additional information on ongoing projects related to software development. By including this information in its response to the Committee, Defense could have demonstrated that it is taking positive actions to ensure that software development is more effectively managed.

For example, Defense has two projects underway that may affect how requirements are managed, but did not provide any details about them in the report to the Committee. Under one project, Defense is developing a software product development report that will provide additional information on software requirements early in the contracting process, before development begins. Under the second project, the Defense Science Board is expected to make formal recommendations in midyear 2000 to strengthen the requirements collections process.

Defense has also begun some initiatives under its goal of building a coherent global network that include an objective of developing an effective Defense software management program. If these initiatives receive sufficient funding and support, Defense plans to issue and implement new software policies and guidance to improve software management. But several key actions under this goal were not included in Defense's response. For example, one ongoing activity focuses on developing and adopting new software concepts and best practices across Defense; another aims to renovate, revise, and/or augment existing standards; and still another seeks to develop a methodology to determine Defense-wide compliance with the SEI's Capability Maturity Model.

---

[3] "Measurements to Manage Software Maintenance," *CrossTalk: The Journal of Defense Software Engineering*, Vol. 10, No. 7, The Software Technology Support Center, Hill Air Force Base, Utah, www.stsc.hill.af.mil/CrossTalk/1997/jul/maintenance.asp.

The official who produced Defense's response told us that he was unable to include information on these ongoing projects because of a lack of time. He added that, if he now had an opportunity to do so, he would include this additional information. In addition, Defense officials noted that the program overseeing some of these initiatives was not created until after Defense's response was prepared, although briefing charts on this program show start dates for these initiatives in late 1999.

AGENCY COMMENTS

In providing oral comments on a draft of this letter, Defense generally agreed with our findings. We have incorporated Defense's specific comments where appropriate.

-- -- -- --

We are sending copies of this report to Representatives Floyd Spence, Chairman, and Ike Skelton, Ranking Minority Member, Committee on Armed Services, House of Representatives, and to Arthur Money, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. Copies will also be made available to others upon request.

Please contact me at (202) 512-6240 if you have any questions concerning this letter. Carl Higginbotham and Tonia Brown were key contributors to this letter.

Jack L. Brock, Jr.
Director, Governmentwide
and Defense Information Systems

(511973)