GAO

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

Accounting and Information
Management Division

B-258185

September 23, 1994

The Honorable William J. Perry
The Secretary of Defense

Attention: DOD Office of the Inspector General
            Director for GAO Surveys and Reviews

Dear Mr. Secretary:

As part of our continuing work on the development and
acquisition of embedded computers for major weapons systems,
we have been reviewing the Air Force's F-22 aircraft program
for the Chairman, Subcommittee on Research and Technology,
House Committee on Armed Services. Our specific objectives
were to (1) describe and assess the Air Force's strategy for
developing embedded computers and software for the F-22 and
(2) identify risks that could adversely affect the program.

In August 1993, we briefed representatives from the Air
Force and your office on the results of our review. We have
done follow-up work since then on the actions being taken to
address our concerns. The purpose of this letter is to
highlight these concerns, as well as key issues that warrant
your continued attention.

Our review disclosed that the Air Force's planned strategy
for F-22 software development, which was in its early
stages, was generally sound in concept. Capitalizing on
lessons learned, the strategy was intended to avoid mistakes
that had hampered previous highly software-dependent
programs and to give software more attention than had
traditionally been the case. Noteworthy features of the
strategy include (1) early assessment of contractors'
software capabilities, (2) a commitment to be event, rather
than schedule, driven, (3) use of integrated product teams
to facilitate early identification and correction of
problems, (4) use of a common software language (5) use of
common automated software development tools, and
(6) preparation of comprehensive software development plans
that call for rigorous quality assurance and risk management

programs and the collection of software costs and other software metrics[1] to measure progress.

We found that while many of the features of the F-22 software strategy were being followed, some significant ones were not. For example, the quality assurance program, in general, and the independent verification and validation of software products, in particular, were less rigorous than planned. Further, contractors were not being required to provide the software metrics called for in the plan to help monitor progress and control costs. The Air Force has taken action to strengthen these areas over the past fiscal year.

In addition to these problems, we identified two critical technical risk areas that could adversely affect the F-22 program. First, the F-22's software strategy called for each of the more than 25 geographically dispersed contractors to use the same automated tools to facilitate software design, development, test, integration, and support. However, some of these tools, known collectively as the system/software engineering environment (S/SEE), were not available or were not working as planned. As a result, the software contractors fashioned their own solutions, using a variety of manual and automated tools that were not standard across the F-22 program. The Air Force and Lockheed, the prime contractor, are attempting to correct the S/SEE problems. However, the likelihood of continued development delays, cost increases, and complications with software integration and support is magnified as more software is developed without a standard and effective S/SEE.

The second technical risk is that the Air Force does not know if the two common integrated processors (CIPs) will be able to meet the high-speed processing requirements called for in the F-22's design. The CIP design is based on microprocessor technology that is still in development. Failure of the CIP to perform as projected could lead to replacement of the processors or the addition of a third processor, either of which could necessitate costly, time-consuming software design and coding changes.

When we discussed these two technical risk areas with the Air Force last year, both issues were being addressed, but

---

[1]Software metrics are tools for monitoring and managing software projects. These tools use mathematical models to measure elements of the development process, such as time, cost, and resources.
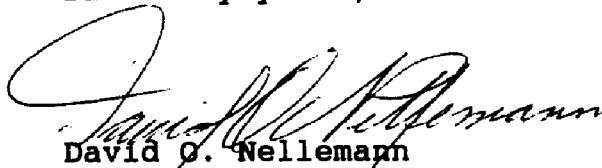
neither was being formally reported to top Defense management. Because these risk areas are so significant, and because a key tenet of the F-22 software plan is to elevate such problems to top management for expeditious resolution, we recommended that the Air Force formally report these risk areas in its quarterly Defense Acquisition Executive Summary. The Air Force is formally reporting the CIP problem, but continues to address S/SEE problems without such formal reporting, much as software problems have been treated in past programs.

In summary, we found that although the Air Force designed its software strategy to attempt to preclude problems that plagued past software development efforts, it was not rigorously implementing the strategy. The Air Force has initiated actions intended to address these shortcomings, but it is imperative that, as it moves forward, it faithfully adheres to the software development plan. Continued management attention to computer and software risks will be critical to avoiding technical problems that could surface during subsequent stages of the program and have hampered previous such efforts.

We are sending copies of this letter to the Chairman and Ranking Minority Member, Subcommittee on Research and Technology, House Committee on Armed Services. We will also send copies to the Chairmen and Ranking Minority Members of the House and Senate Committees on Appropriations and the Senate Committee on Armed Services, to the Secretary of the Air Force, and to other interested parties upon request.

We plan to stay abreast of F-22 embedded computer and software issues as part of our continuing work for the Subcommittee. As such, we would appreciate being kept apprised of the actions being taken to address our concerns. If you have any questions or would like to discuss these issues further, please contact me at (202) 512-2666 or John Stephenson, Assistant Director, at (202) 512-6225.

Sincerely yours,

David G. Nellemann
Director, Information Resource
  Management/National Security and
  International Affairs

(511307)