GAO

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

160631

National Security and
International Affairs Division

B-280243

June 11, 1998

The Honorable Curt B. Weldon
Chairman, Subcommittee on Military Research and Development
Committee on National Security
House of Representatives

Subject: DOD's Information Assurance Efforts

Dear Mr. Chairman:

As requested, we are currently reviewing certain aspects of the Department of Defense's (DOD) efforts to attain information superiority. In preparation for a Subcommittee hearing this week, your office asked that we provide the results of a subset of that work--our evaluation of DOD's efforts to protect and defend its information and information systems, an activity it characterizes as information assurance. In response, this letter addresses (1) the actions DOD has taken to implement the recommendations contained in the Defense Science Board task force's November 1996 report[1] on information warfare defense, (2) DOD's development of an information assurance management process, and (3) DOD's adoption of a new information assurance certification and accreditation process. We expect to issue a report on the department's progress in implementing information superiority in the near future.

BACKGROUND

In 1996, the Chairman of the Joint Chiefs of Staff articulated a conceptual template for DOD's future warfighting, called Joint Vision 2010, that depends on information superiority over opposing forces as a key enabler. DOD defines information superiority as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." It believes the implementation of this concept, and the information systems on which it critically depends, has the potential to provide significant advantages over adversaries in conflict and add efficiencies to peacetime and wartime operations. However, increasing reliance on

[1]Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D) (Nov. 1996), Defense Science Board, Washington, D.C.

160631

information systems also exposes DOD's warfighting capabilities to significant potential vulnerabilities through attacks on those systems. The importance of protecting those systems was reflected in a recent DOD task force report that stated that information assurance is critical to attaining information superiority and commented that without it, it is increasingly likely that U.S. forces will fail to accomplish their mission.

The importance of DOD's providing protection and defense for its information and information systems is further evident when one considers the investment DOD plans in information superiority related systems. Based on its analysis of the fiscal year 1999 through 2003 Future Years Defense Plan, DOD estimates that it has budgeted an average of $43 billion a year on the Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems and activities–systems and activities on which attaining information superiority will depend.

SUMMARY

Since the Defense Science Board task force's November 1996 report on information warfare defense, DOD organizations have undertaken a variety of efforts to establish information assurance. For example, DOD has initiated a project to develop a standard methodology and management process by which opposing force (Red Team) assessments will be conducted to help identify vulnerabilities in DOD systems and networks and to determine the readiness posture and preparedness of the fighting forces. Also, the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence recently began implementing a program to bring an integrated management structure and process to information assurance activities and initiated a process for certifying and accrediting systems for information assurance. How effective these new initiatives will be, however, remains to be demonstrated.

DOD'S RESPONSE TO TASK FORCE RECOMMENDATIONS

In October 1995, the Under Secretary of Defense for Acquisition and Technology established a Defense Science Board Task Force on Information Warfare-Defense. Its purpose was to focus on the protection of information interests of national importance through the establishment and maintenance of credible information warfare defensive capabilities. In its November 1996 report, the task force concluded that there is an increased risk posed by the networked environment of DOD information systems that could seriously affect DOD's ability to carry out its missions. It also concluded that there is a need for extraordinary action to deal with the present and emerging challenges of defending against possible information warfare attacks on facilities, information

systems, and networks. It recommended over 50 actions designed to better prepare DOD against the threat of information warfare.

According to DOD officials, information assurance efforts have not been specifically organized around responding to the task force recommendations. Rather, the efforts have been driven by a combination of the task force report, other reports,[2] and events that have increased DOD's awareness about potential information security vulnerabilities. The events include DOD-simulated and actual outsider intrusions into DOD networks and an information security workshop hosted by the Defense Information Systems Agency in January 1997. The workshop focused on addressing task force recommendations and included participants from many DOD organizations.

Although DOD has not organized its information assurance activities solely around the Defense Science Board task force's November 1996 report, we worked with staff of the DOD's Information Assurance Directorate in an attempt to draw a general assessment of DOD's position relative to the task force's recommendations. We found the following:

- Several of the task force's recommendations did not fall entirely within DOD's scope of operations and were dealt with through the President's Commission on Critical Infrastructure Protection. For example, the task force recommended establishing a center to provide Intelligence Indications and Warning, Current Intelligence, and Threat Assessments. DOD officials stated, and we verified, that this issue was addressed by the President's Commission.

- Some of the task force's recommendations were considered and then rejected. For example, the task force recommended that DOD fund, establish, and maintain a minimum essential information infrastructure that would include a fail-safe restoration capability. DOD officials told us that the Quadrennial Defense Review determined that action on this recommendation should not be taken until the information warfare threat to DOD's systems matures.

- Certain efforts that will address some of the task force's recommendations are underway. For example, the task force recommended the establishment of an opposing force (Red Team) for conducting independent assessments of

---

[2] For example, The Report of the Joint Security Commission (Feb. 1994), The Report of the Commission on Protecting and Reducing Government Secrecy (Mar. 1997), Improving Information Assurance: A General Assessment and Comprehensive Approach to an Integrated IA Program for the Department of Defense (Mar. 1997), The Quadrennial Defense Review (May 1997), DOD Inspector General draft Audit Report on DOD Management of IA Efforts (July 1997), and Information Security: Computer Attacks at the Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996).

new systems' and services' vulnerabilities and for conducting simulated information warfare attacks to verify the readiness posture and preparedness of the fighting forces. DOD has initiated a project to develop a standard methodology and management process by which opposing force (Red Team) assessments will be conducted. Additionally, DOD officials told us that the Defense Intelligence Agency will be providing concept validation of the methodology by following it step by step in an activity beginning this month.

- Some of the recommendations will be addressed through the implementation of recently adopted plans and processes. For example, a central theme of the task force's report was the need to organize and provide defensive information warfare capabilities. The recently adopted Defense-wide Information Assurance Program, as described below, is intended to provide a management process that is to bring coordination and cohesion to DOD's various information assurance activities and to provide more effective management of its information assurance resources.

DEVELOPMENT OF DOD'S INFORMATION ASSURANCE MANAGEMENT PROCESS

Despite the many efforts by the various organizations, DOD's information assurance needs are not being met in certain key areas. A recent Assistant Secretary of Defense for Command, Control, Communications and Intelligence report[3] stated that the complexity of managing DOD's information assurance efforts had increased due to the proliferation of networks across DOD and that its decentralized information assurance management could not deal with it adequately. As a result, it noted that some information assurance efforts were only minimally effective. The report further stated that DOD lacked effective processes to (1) assess the operational readiness of its information systems and networks, (2) identify its information assurance requirements, and (3) ensure that those requirements are programmed and executed in accordance with DOD's priorities.

To deal with these issues and better manage DOD's increasing dependence on globally networked information systems, the report recommended an information assurance management process for a Defense-wide Information Assurance Program. In January 1998, the Deputy Secretary directed the Assistant Secretary of Defense for Command, Control, Communications and Intelligence to develop and implement the program. How effective the new program will be however, remains to be demonstrated. According to the report,

[3]A Management Process for a Defense-wide Information Assurance Program (DIAP), Nov. 15, 1997, Assistant Secretary of Defense for Command, Control, Communications and Intelligence. This report was directed to be developed by the Fiscal Year 1999-2003 Defense Planning Guidance.

metrics will need to be developed, collected, and analyzed to demonstrate results, such as determining where and how its information assurance investments are enhancing the protection of its information systems.

Additionally, DOD's information assurance efforts are moving forward without the benefit of a completed and approved C4ISR architecture–an issue that we plan to address more fully in our upcoming report on DOD's progress in implementing information superiority. The importance of this issue is reflected in the March 1997 report of a DOD information assurance task force. In its report, that task force stated that DOD's enterprise [DOD-wide] information architectures must support its information security needs and that DOD must address security in an integrated fashion with other system attributes at the time of system design rather than as add-on products or services after design completion. It further stated that DOD must explicitly link security throughout the operational, systems, and technical architectures, noting that the operational architecture must show what, when, where, and why security should be applied; the system architecture must show where, what, and how security will be applied; and the technical architecture must provide the "building codes and standards" for what and how security will be applied.

ADOPTION OF A NEW CERTIFICATION AND ACCREDITATION PROCESS

In addition to the new information assurance management process, DOD has recently adopted a new Information Technology Security Certification and Accreditation Process. In December 1997, the Assistant Secretary of Defense for Command, Control, Communications and Intelligence issued DOD Instruction 5200.40 that established this process as a standard DOD-wide approach to protecting and securing the entities comprising the Defense Information Infrastructure, including automated information systems, networks, and sites. The process requires comprehensive information assurance evaluations of all information technology systems in accordance with specified analytical procedures, including vulnerability risk assessments and acceptance determinations. In addition, it specifies that certification and accreditation will be done at "applicable systems level" and involve systems program or operation management and senior staff, users, and working level security managers.

As with the new management process, successful operation of the new certification and accreditation process remains to be seen, pending its full implementation. Because of the possibility of inconsistent application of the procedures, aspects of the process may warrant attention. Specifically, because the process disperses certification and accreditation responsibilities among organizations and systems, standards could be interpreted and applied inconsistently among various organizations. If such inconsistencies occur, the process may not meet its objective.

Similarly, the process permits dispersed decision-making for accepting risk levels posed by individual systems. However, when systems approved on an individual level become interconnected through a network, the most vulnerable system would set the risk level for the other systems in the network. As a result, security of some systems that need higher levels of protection by virtue of their use and the kind of information maintained on them may unknowingly take on additional and unacceptable risks.

AGENCY COMMENTS

In oral comments on a draft copy of this letter, DOD provided one technical correction, but otherwise agreed with its contents. This letter reflects the technical change DOD suggested.

SCOPE AND METHODOLOGY

To evaluate what actions DOD and the services had undertaken to implement the recommendations of the Defense Science Board task force on information warfare defense, we reviewed the task force report and discussed specific actions taken regarding the report's recommendations and current and planned information assurance activities with appropriate level senior and other DOD officials. These officials were responsible for information assurance and information operations oversight within the offices of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence; Defense Information Systems Agency; Joint Staff; military services; and the National Security Agency. From these officials, we obtained and reviewed key documents relevant to information assurance actions and plans, including a November 15, 1997, Secretary of Defense report to Congress on Information Security Activities of the Department of Defense; a November 15, 1997, Assistant Secretary of Defense for Command, Control, Communications and Intelligence report to the Deputy Secretary of Defense on a Management Process for a Defense-wide Information Assurance Program (DIAP); and DOD Instruction 5200.40 on DOD's Information Technology Security Certification and Accreditation Process.

We also met with the Chairman of the Defense Science Board task force and a former Defense Information Systems Agency director to obtain their views on DOD's responses to the task force's recommendations and the problems facing DOD with respect to information assurance. Finally, we received briefings from appropriate officials at the U.S. Atlantic Command, Army Training and Doctrine Command, U.S. Central Command, and the National Security Agency on the results of wargame simulation exercises and network security events that demonstrated significant information network security problems, and we received a briefing on and tour of Defense Information Systems Agency's Global Operations and Security Center.

We conducted this review from November 1997 to June 1998 in accordance with generally accepted government auditing standards.

- - - - -

We are sending copies of this letter to the Ranking Minority Member of the subcommittee, the Chairman and Ranking Minority Member of the full committee, other interested congressional committees, and the Secretary of Defense. We will also make copies available to others upon request.

Please contact me at (202) 512-4841 if you or your staff have any questions concerning this letter. The major contributors to the letter were Charles F. Rey, Charles R. Climpson, Robert R. Hadley, Gregory K. Harmon, and Bruce H. Thomas.

Sincerely yours,

Allen Li
Associate Director
Defense Acquisitions Issues

(707354)

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

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

or visit:

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

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

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

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

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

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

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested