United States General Accounting Office

GAO

Report to the Chairman, Committee on Armed Services, House of Representatives

March 2001

INFORMATION SECURITY

Progress and Challenges to an Effective Defense-wide Information Assurance Program

GAO

Accountability * Integrity * Reliability

GAO-01-307

Contents

Letter 3

Appendixes

Appendix I: DIAP Interorganizational Relationships 32

Appendix II: DIAP Staff Responsibilities According to the DIAP Implementation Plan 35

Tables

Table 1: Entities Interacting With DIAP and Their Responsibilities 32

Figures

Figure 1: Key Entities Interacting With DIAP and Their Relationships 34

Abbreviations

ASD	Assistant Secretary of Defense
C^3I	Command, Control, Communications, and Intelligence
CIO	chief information officer
CIP	critical infrastructure protection
DIAP	Defense-wide Information Assurance Program
DISA	Defense Information Systems Agency
DOD	Department of Defense
FEIT	Functional Evaluation and Integration Team
IA	information assurance
IC	intelligence community
I&IA	Infrastructure and Information Assurance
INFOSEC	information security
IT	information technology
MCEB	Military Communications-Electronics Board
NSA	National Security Agency
OASD	Office of the Assistant Secretary of Defense
PDIT	Program Development and Integration Team
PKI	public key infrastructure
PPBS	Planning, Programming, and Budgeting System
RC	reserve component

GAO
Accountability * Integrity * Reliability

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

March 30, 2001

The Honorable Bob Stump
Chairman, Committee on Armed Services
House of Representatives

Dear Mr. Chairman:

The components, military services, and agencies of the Department of Defense (DOD) share many risks in their use of globally networked computer systems to perform operational missions, such as identifying and tracking enemy targets, and daily management functions, such as paying soldiers and managing supplies. Weaknesses in these systems can give hackers and other unauthorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive military data. Weaknesses in DOD systems and associated risks have been highlighted by numerous reports of vulnerabilities, organized intrusions, and theft related to department systems and networks, and by our 1996 report on penetrations and on pervasive vulnerabilities in DOD computer systems, which recommended implementation of a departmentwide information security program.[1]

In January 1998, DOD responded to these risks by announcing its plans for a Defense-wide Information Assurance Program (DIAP), intended to promote integrated, comprehensive, and consistent information assurance (IA) practices across the department. IA refers to the range of information security activities and functions needed to protect and defend DOD's information and systems. DOD estimates a department IA budget of at least $6 billion for the 5-year period from fiscal years 2001 through 2005. In February 1999, the department issued an approved DIAP Implementation Plan, which described, at a high level, the program's goals, objectives, and organizational structure, and confirmed its responsibility for the planning, coordination, integration, and oversight of Defense-wide computer security initiatives.

Given its importance as DOD's central focal point for IA, we were asked to examine the progress and accomplishments of DIAP since its inception. We were also asked to identify obstacles to further progress. This report

[1] *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* (GAO/AIMD-96-84, May 22, 1996).

provides a summary of DIAP's accomplishments to date in addressing the department's IA goals and challenges to further progress. Our accompanying recommendations identify DOD actions critical to improving DIAP's effectiveness.

Results in Brief

Since its inception, DIAP has made progress in addressing IA issues, which are one of the department's highest information technology (IT) priorities. DIAP has undertaken several activities to begin addressing DOD's four critical goals in this area: integrating IA with mission readiness criteria, enhancing the IA capabilities and awareness of department personnel, improving monitoring and management of IA operations, and establishing a security management infrastructure. In each of these areas, department-level actions have also been undertaken by organizations other than DIAP. Work is also underway to establish a program baseline of current department IA efforts and resources, a comprehensive set of IA policies, and improvements in other functional areas such as architectural standards.

Although the department has made progress, it has not yet met its goals. Draft readiness assessment metrics have yet to be tested; proposed actions to enhance the department's IA human resources are not yet ready for implementation; the organizations, policies, and procedures for monitoring and managing IA are not fully defined across the department; and planning and coordination for implementation of security management technologies and operations is not yet consistent throughout the department. Further, the process of cataloging DOD's IA activities and resources to develop a program baseline has been limited to only one major program, the Information Systems Security Program, while other IA activities remain to be identified and validated. Also, department policies do not yet provide a comprehensive framework for ensuring adequate coverage and integration of DOD's IA approach. In addition, DIAP has not fully addressed its responsibilities in areas such as architectural standards, acquisition support, and research.

DIAP's progress has been limited by weaknesses in its management framework and unmet staffing expectations. DOD has not established a performance-based management framework for IA improvement at the department level. As a result, DOD remains unable to accurately determine the status of IA across the department, the progress of its improvement efforts, or the effectiveness of its IA initiatives. Also, a lack of planned personnel has kept the DIAP staff from fulfilling its central role in planning,

monitoring, coordinating, and integrating Defense-wide IA activities, and changes in the composition and authority of other key organizations interacting with DIAP have left it without a consistent and fully supportive environment for its operations. Achieving its vision for information superiority will require the commitment of DOD to proven IA management practices.

To improve progress toward the department's IA goals, we are making several recommendations to the Secretary of Defense in the areas of component commitments to DIAP and executive-level monitoring of DIAP progress. We are also recommending that the DOD Chief Information Officer (CIO) institute performance-based management of DIAP through a defined budget and performance objectives, and that the DIAP program manager take steps to address the program's unmet IA goals. In commenting on a draft of this report, DOD generally concurred with our recommendations.

Background

DOD relies increasingly on globally networked computer systems to manage the information it uses to perform operational missions and daily management functions. These systems provide military offensive and defensive capabilities as well as intelligence support. According to DOD, the department operates 2 million to 3 million computers, 100,000 local area networks, and 100 long-distance networks—including service-based, joint defense, and intelligence computers and networks such as the Global Command and Control System, which supports distributed collaborative, worldwide planning for crisis and contingency operations, and the Joint Worldwide Intelligence Communication System, with more than 100 sites worldwide.

DOD views information as a strategic resource vital to national security and information superiority as the foundation of its vision of modern warfare. It has concluded that IA is essential to DOD's information superiority. DOD defines IA as "Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation . . . [which] includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities."[2] In this context, *availability* is assured access by authorized users, *integrity* is protection from unauthorized change, *authentication* is verification of the originator, *confidentiality* is protection from unauthorized disclosure, and *nonrepudiation* is undeniable proof of participation. A 1997 DOD task force report acknowledged that the department requires substantial IA capabilities for its highly interconnected computing and communications environment, noting that "without information assurance, it is increasingly likely that our forces will fail to accomplish their mission."[3]

Other policy and guidance documents also emphasize the critical role of IA in DOD's mission. In October 1998, the *Joint Doctrine for Information Operations* identified IA as an essential component of the military's defensive information operations. In February 2000, the DOD CIO's annual report on IA identified it as the department's second highest priority IT issue, following Year 2000 remediation. In March 2000, the Deputy Secretary of Defense issued a guidance and policy memorandum recognizing the pivotal role of global networking in departmental activities and requiring the use of IA safeguards and operational procedures for all of DOD.

Several Factors Affect DOD's Ability to Protect Its Systems

Defense operations rely increasingly on interconnected information systems, which results in sharing of security risks among all interconnected organizations. In this environment, an adversary need only find and penetrate a single poorly protected system and then use access to that system to penetrate other interconnected systems. Consequently, coordination of IA efforts across DOD is important to maintain adequate security throughout its systems and networks.

[2] *Joint Doctrine for Information Operations*, Joint Publication 3-13, October 9, 1998.

[3] *Improving Information Assurance: A General Assessment and Comprehensive Approach to an Integrated IA Program for the Department of Defense*, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, March 28, 1997.

Historically, the department's information systems have also been beset by vulnerabilities. Reports by us and DOD document serious and pervasive deficiencies that can impair the military's ability to (1) control physical and electronic access to its systems and data, (2) ensure that software is properly authorized, tested, and functioning, (3) limit employees' ability to perform incompatible functions, and (4) resume operations in the event of a disaster.[4] Numerous Defense functions, including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll have been adversely affected by system attacks and fraud. DOD, in turn, has acknowledged the need for improvements.[5]

The department's IA challenges are heightened by the growing threat of Internet-based attacks. Intrusions into government information systems—including DOD's—continue to escalate, in number and complexity, requiring better detection, faster damage containment, and more efficient reporting mechanisms.[6] Furthermore, DOD recognizes that increasing availability of its systems to authorized users has also increased opportunities for unauthorized access, presenting the most serious threat to DOD information.[7] In this environment, security incidents remain an ongoing problem for DOD.[8]

[4]*DOD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk* (GAO/AIMD-99-107, August 26,1999) and *DOD Management of Information Assurance Efforts to Protect Automated Information Systems*, DOD Office of the Inspector General, September 25, 1997.

[5]DEPSECDEF Policy Memorandum, "Management of the Department of Defense (DOD) Information Assurance (IA) Program," January 30, 1998.

[6]*Information Security: The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data* (GAO/T-AIMD-99-146, April 15, 1999).

[7]*DOD Insider Threat Mitigation: Final Report*, [DOD] Insider Threat Integrated Process Team, undated.

[8]GAO/AIMD-99-107, August 26, 1999.

DOD has identified an even more fundamental challenge underlying these organizational and technological challenges—a shortage of qualified personnel to fill positions that manage and protect its information systems. Although poor planning of system procurements, downsizing of military and civilian personnel, and an increased emphasis on outsourcing have contributed to DOD's IT personnel shortage, this shortage also reflects a broader problem in recruiting and retaining IT security professionals in both the public and private sectors, according to a DOD human resources study.[9]

DIAP Is DOD's Focal Point for IA

In January 1998, the Deputy Secretary of Defense responded to these challenges by forming DIAP and assigning responsibility for its oversight to DOD's CIO, who is also the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C^3I)). DIAP was established to meet DOD's need for "integrated, comprehensive, and consistent Defense-wide IA practice," and to develop DOD into "a model practitioner of IA" for the nation.

In February 1999, DOD's CIO established four critical departmentwide strategic IA goals:

- Make IA an integral part of DOD mission readiness criteria.
- Enhance DOD personnel IA awareness and capabilities.
- Enhance DOD IA operational capabilities.
- Establish an integrated DOD Security Management Infrastructure.

DIAP was intended to help meet these goals by planning, coordinating, integrating, and overseeing IA activities, and by supporting review and assessment of IA resource investments on a departmentwide basis. In this regard, DIAP became DOD's official program for ensuring the continual integration and coherent execution of all IA functions, activities, and program resources. DIAP was to continually monitor and act as a facilitator for the execution of IA resources, which remained the responsibility of the commanders-in-chief, military services, and Defense agencies where the activities and programs reside.

[9] *Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense*, Office of the Secretary of Defense, Information Assurance and Information Technology Human Resources Integrated Process Team, August 27, 1999.

Responsibility for the creation and management of DIAP was assigned to the Director of Information Assurance, a position reporting to the CIO. The Director was designated DIAP's program manager and was authorized a staff of representatives from DOD component organizations to support Defense-wide IA planning, programming, budgeting, and execution review. In addition to the DIAP staff, the Director of IA also maintains a staff dedicated to the Office of Infrastructure and Information Assurance (I&IA).

As depicted in its management plan, the DIAP program structure also included the following individuals and organizations that contribute to achieving the department's IA goals:

- DOD CIO Council – monitors and coordinates IT investments, including IA; [10]
- National Information Security (INFOSEC) manager – assesses cyber threats and security posture for national security systems;
- Defense Information Infrastructure adviser – plans, develops, and supports C^3I systems and engineers the information infrastructure;
- Senior DIAP Steering Group – provides strategic direction and guidance on IA issues to the DOD CIO and the CIO Council; and
- IA Group – develops and recommends coordinated positions on department IA issues.

The policy memorandum that established DIAP specified that a detailed implementation plan be submitted by March 1998; an initial operational capability achieved by May 1998; and a full operational capability established by August 1998. However, the implementation plan was not approved until February 1999, and the approved plan did not include dates for DIAP's initial or full operational capability.

The implementation plan created a staff director, reporting to DIAP's program manager, with responsibility for (1) coordinating DIAP, (2) developing a process to assess return on IA investments, and (3) overseeing the execution of DOD IA policies, functions, and programs.[11]

[10]The Deputy Secretary of Defense officially disbanded the DOD CIO Council in March 2000. A new CIO Executive Board, which assumed the council's responsibilities, was created at that time.

[11]*Implementation Plan for the Defense-wide Information Assurance Program (DIAP)*, Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, February 12, 1999.

DIAP would also work with an Intelligence Community (IC) coordinator to ensure integration and compatibility of IA efforts. Appendix I provides a description of certain IA-related Defense organizations and their relationships with DIAP, based on the implementation plan.

The implementation plan also established the general structure of the DIAP staff and assigned it a variety of responsibilities. The plan described expected DIAP staffing levels, with specific numbers of personnel to be provided by the Office of the Secretary of Defense, the Joint Staff, each of the military services, and several Defense agencies.

As described in the implementation plan, DIAP staff was divided into two teams, the Functional Evaluation and Integration Team (FEIT) and the Program Development and Integration Team (PDIT). FEIT was assigned responsibility for development of Defense-wide IA performance goals, standards, metrics, and oversight of functional areas. The organization of FEIT reflects, in part, each of the four DOD IA goals corresponding to readiness assessments, human resources, the operational environment, and security management. The remaining FEIT functional areas address policy integration, architecture, acquisitions, and research and development. PDIT was assigned responsibility for oversight, coordination, and integration of the department's IA resource programs through participation in DOD's IA planning and budgeting processes, and was specifically charged with tasks such as categorizing program activities, developing departmentwide budgets, and preparing the CIO's annual IA assessment. Liaison positions were established to coordinate DIAP activities with special communities whose interests span multiple functional areas. Appendix II lists DIAP staff responsibilities for each program area as outlined in the implementation plan.

Objectives, Scope, and Methodology

The objectives of our review were to (1) examine the progress and accomplishments of DIAP since its inception and (2) identify obstacles to further progress. To determine the progress and accomplishments of DIAP, we ascertained its mission, responsibilities, and organization through analysis of documents provided by DOD. We gathered and analyzed information on DIAP plans, activities, products, and accomplishments from the DIAP staff, the Office of the ASD(C^3I) (OASD(C^3I)), and DOD organizations that interact with the staff, including the departments of the Army, Navy, and Air Force; Reserve Affairs; the Joint Staff; and the following defense agencies:

- Ballistic Missile Defense Organization,
- Defense Advanced Research Projects Agency,
- Defense Information Systems Agency (DISA),
- Defense Intelligence Agency,
- Defense Logistics Agency,
- Defense Security Service,
- National Imagery and Mapping Agency,
- National Reconnaissance Office, and
- National Security Agency (NSA).

We selected these organizations primarily based on their roles in defense-related IA as documented in the 1999 *DOD CIO Annual Information Assurance Report*. We also reviewed DOD self-assessments, plans for departmentwide IA activities, and inspector general reports on DIAP and other departmentwide IA activities.

We focused on the DIAP's accomplishments and plans most clearly tied to DOD's IA goals, and thus did not compile a comprehensive inventory of all DIAP accomplishments, particularly those led by other Defense components. We identified interactions of the DIAP staff with each Defense organization and the impact of DIAP staff efforts as perceived by those organizations.

We also reviewed IA plans, products, and accomplishments of groups outside of the DIAP staff and assessed the mechanisms used to integrate the activities of these groups with those of the DIAP staff. These outside groups included

- the Joint Staff,
- the IA Panel,
- the INFOSEC Research Council, and
- the Office of Infrastructure and Information Assurance in OASD(C^3I).

We did not attempt to determine the proportion of IA accomplishments attributable to the DIAP staff or to other organizations. We verified activities and events related to accomplishments where feasible but did not verify all claims of accomplishments.

To identify challenges to DIAP, we obtained information from DOD officials, staff members, contractors, and other federal government representatives that showed evidence of factors that hindered DIAP activities and the achievement of DIAP objectives. Finally, we compared DIAP's management approach with characteristics of high-performing organizations.[12]

We performed our work at OASD(C^3I), DIAP, and DOD component offices in the Washington, D.C., area. Our work was conducted from March 2000 through January 2001, in accordance with generally accepted government auditing standards. We obtained oral comments on a draft of the report from the Deputy Assistant Secretary of Defense for Security and Information Operations.

DIAP Has Made Progress but Has Not Yet Met Goals

DIAP has made progress, but a significant effort remains before it will achieve its IA goals. DIAP has developed draft department-level IA readiness metrics, identified actions to address current IA human resource limitations, enhanced IA monitoring and management by characterizing operations and defining departmentwide policies, and applied a strategy to track security management implementation. In addition, it has improved the department's understanding of its IA resources and needs through identification of the resources that make up a departmentwide program baseline and development of several policies to address the department's goals. Other department efforts that support DIAP's goals include definition of an architecture framework for addressing IA in interconnected systems and identification of IA research topics.

However, DIAP has not yet achieved the goals originally envisioned in its management and implementation plans. Department-level IA readiness reports are not yet available, component IA training and certification plans are not yet being monitored across the department, and not all IA-related operations issues have yet been uniformly addressed. Further, a lack of complete and consistent data from across the department has prevented DOD from accurately assessing its current IA status, and departmentwide IA policies have not been integrated or enforced.

[12] *Management Reform: Using the Results Act and Quality Management to Improve Federal Performance* (GAO/T-GGD-99-151, July 29, 1999).

IA Readiness Metrics Have Been Drafted but Are Not Yet Operational

DOD's IA readiness assessment goal states that "All DOD organizational elements shall operate and maintain their computer-based information functions, information systems and their supporting networks and resources at levels of IA consistent with the enterprise and network mission functions they perform."[13] Recognizing the importance of IA to department readiness, DIAP has drafted metrics for IA readiness assessment at a strategic, departmentwide level in the areas of people, operations, training, equipment and infrastructure, and processes. An example of an IA metric is the number of system outages caused by infrastructure failures during a fixed period. Joint force-level IA metrics were separately developed, approved, and issued by the Joint Staff for its own use and for use by the commanders-in-chief, military services, and combat support agencies.[14] The DIAP staff plans further development of department readiness metrics, coordination between department and joint force metrics, and integration of the metrics into management processes.

Although these metrics have been developed, systems and processes are not yet in place to provide department decisionmakers with data to assess the department's IA readiness status. DOD plans indicate that department-level readiness reports will not be available before late 2002. DIAP personnel stated several factors that contribute to this shortfall. First, they said that DOD's automated readiness reporting systems are limited in their current capability to capture IA-related inputs, and they said that these systems could not be easily modified to provide that capability. Second, they noted that processes for developing strategic department-level and joint force IA metrics have been largely independent of each other, presenting risks for unnecessarily burdensome reporting requirements and interpretation conflicts. Further, neither DIAP nor the Joint Staff have taken steps, such as testing the metrics on a specific program, to ensure that the metrics are appropriate. Therefore, data reported by components, services, and agencies may not provide a true picture of DOD's readiness status. Without reliable reporting on IA, the Congress and the department lack important information with which to determine whether DOD is maintaining adequate levels of operational readiness.

[13] *Implementation Plan or the Defense-wide Information Assurance Program (DIAP)*, Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, February 12, 1999.

[14] The combat support agencies include the Defense Intelligence Agency, DISA, Defense Logistics Agency, National Imagery and Mapping Agency, and NSA.

Human Resources Policy Recommendations Have Been Formulated but Not Yet Implemented

DIAP contributed to a 1999 joint study by the Undersecretary of Defense for Personnel and Readiness and ASD(C^3I), which concluded that the weakest link in its IA is the people who use, administer, and manage its information systems and technologies.[15] The study also identified a lack of information about the composition and activities of the department's IT personnel as the key human resources issue affecting DOD IA and recommended department actions aimed at establishing a sustaining pool of skilled IA/IT professionals to meet the current and future technological needs of the department. The DIAP staff supported the development and coordination of a policy directive, issued in July 2000, which assigned DOD organizations to lead implementation of each recommendation. The DIAP staff plans to coordinate an action plan with responsible DOD organizations to address the new policy.

According to DIAP officials, a key factor limiting progress in improving DOD's human resources practices is that certain DOD components have not yet submitted training and certification plans to the OASD(C^3I) Director of IA, although they were required to do so by August 1998. The plans, if available, would represent a baseline of current activity that could be used to assess further actions needed to comply with the July 2000 directive. However, DIAP officials told us that no steps have been taken to enforce this requirement. DOD's progress in improving human resources management is further hampered by the time required to fill gaps in data about the status of DOD's IT and IA personnel—from 3 to 5 years after completion of the departmentwide execution plan, according to the 1999 joint study.

IA Monitoring and Management Have Been Enhanced but Are Not Yet Consistent Across the Department

Monitoring and management of DOD's information systems and computer networks provide visibility into and control of IA levels throughout the department. Primary responsibility for this area rests with DOD's Joint Task Force-Computer Network Defense. Although it is not directly responsible for the area, DIAP has enhanced IA operational monitoring and management through its efforts to characterize operations and define policies to improve the department's IA posture. DIAP participated in an OASD(C^3I) study to identify needed policies and requirements for defense of DOD's computer networks, then supported the development of DOD

[15] *Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense, Final Report*, Office of the Secretary of Defense, August 27, 1999.

instructions intended to implement those policies. DIAP also assisted in developing a Defense-wide policy that requires vulnerability notices issued by components to be coordinated with the Joint Task Force-Computer Network Defense to ensure consistent communications about vulnerabilities across the department.

The DIAP staff plans to use information it has gathered about IA operations to develop a policy for certifying IA support facilities, policy and instructions for continuity of operations at IA support facilities, and a program structure for coordinating IA support groups across the department.[16] The Joint Staff is developing guidance for operating such facilities. The DIAP staff expects to contribute enhancements to a Defense-wide IT database for IA-related system components.

However, the department still lacks comprehensive operational policies and procedures that would provide consistency in IA monitoring and management across the department. For example, no departmentwide policy on the use of intrusion-detection systems has been established. The absence of such operational policies impairs DOD's ability to realistically manage risks to its information and systems. Also, the DIAP staff has not addressed identification and implementation of the best IA tactics, techniques, and procedures in the operations of DOD components as described in the DIAP strategic plan. DIAP officials said that unmet staffing expectations had prevented them from taking action on this objective.

Planning for Security Management Technologies Has Addressed Public Key Infrastructure but Not Other Technologies

Public key infrastructure (PKI) technology is the foundation of DOD's security management services, which provide confidence in secure operation of the Defense information infrastructure.[17] Program management for DOD's PKI initiatives rests with NSA, and DISA and NSA have established a partnership for developing and applying PKI throughout the Defense information infrastructure. In support of this goal, DIAP has established processes to consistently budget and track component

[16]Such groups include Network Operations Control Centers, Network Operations Security Centers, and Computer Emergency Response Teams, which are charged with preventing, detecting, and responding to security breaches in the department's information systems.

[17]A PKI is a system of hardware, software, policies, and people that, when fully and properly implemented, can provide a suite of information security assurances—including confidentiality, data integrity, authentication, and nonrepudiation—that are important in protecting sensitive communications and transactions.

activities in implementing PKI technology associated with computer applications. DIAP helped to draft and coordinate the department's guidance on adapting applications to use public key technology, which was issued in November 1999 and augmented more general PKI guidance that was issued in May 1999.

Current DIAP activity focuses on working with components to ensure that adequate steps are being taken to plan and budget for applications capable of supporting DOD PKI policy and to establish a Defense-wide PKI budget. The DIAP staff has begun to maintain a list of successfully tested PKI applications and plans to issue an annual report of "enabled" systems, a mechanism that would support identification of duplicate testing across DOD organizations. In addition, some coordination of coalition-related PKI issues has been performed within the Office of I&IA. Future plans include overseeing and coordinating development of a Defense-wide key management infrastructure.

While progress has been made on PKI, other security management technologies have not yet been planned or coordinated on a departmentwide basis. For example, DIAP staff have not addressed topics such as workstation security, virtual private networks, and security management tools. According to DIAP officials, resources have not been available to address these additional topics.

IA Program Baseline Development Has Begun but Is Not Complete

Establishing a program baseline is useful as a way to define the activities, human resources, and funding required to meet performance-based goals, and can be used to facilitate effective program management and oversight. The DIAP staff has begun to build a program baseline that catalogs the full range of department efforts and resources in IA. The staff reviewed the largest element of the baseline—the Information Systems Security Program, managed by NSA—to understand its components, and established an IA Resources Team to address other component IA activities and programs that are not a part of that program. The staff also developed instructions, categorization methods, and an automated tool for tracking component IA funding requests for fiscal years 2002 through 2007. In addition, the staff compiled the annual report for the CIO on departmentwide IA efforts and participated in various departmental planning and budgeting activities. The DIAP staff has earmarked $1.2 million of the OASD($C^3I$) fiscal year 2001 budget for contractor support to carry out further IA baseline development activities, including improving department coverage, continued participation in department planning and

budgeting, definition of the IA domain and mission, and development of an investment strategy and cost model for components' IA-related resources.

Although DIAP has developed mechanisms to define an IA program baseline, its work to date is incomplete. Specifically, DIAP's efforts relied on program data provided by the Defense components that are neither complete nor consistent. For example, information on IA resources associated with embedded systems—such as computers that control the functions of airplanes or tanks—has not been gathered. Further, differing internal policies and procedures for structuring budgets among components have produced inconsistent information. For example, a portion of the budgets reported by components did not fit any of the 10 classifications used by DIAP.

Three additional factors have contributed to the incomplete and inconsistent view of DOD's IA resources. First, no budget or funding was specifically identified for DIAP at the time of its creation, and DIAP therefore remains dependent on discretionary funding from OASD(C^3I) to support staff activities. Second, DIAP staff have not initiated the development of a detailed system of IA budget codes for identifying and comparing IA efforts and resources across DOD, as called for in the DIAP management plan. While DIAP officials said they lacked the staff needed for this assignment, we also noted that other DOD officials disagreed on the need for these detailed IA budget codes. Third, DIAP has not yet integrated planning, programming, and budgeting data with the department's acquisition management or requirements-generation systems to provide a comprehensive view of IA resources and funding priorities. A DIAP official stated that program staff have no plans to address this issue until DIAP achieves greater influence on DOD's program management processes. Without the information that an IA baseline would provide, DOD remains limited in its ability to determine its IA expenditures and unmet resource needs, and therefore it is not positioned to effectively manage and oversee its attempts at improvement.

IA Policies Continue to Be Developed but Are Not Fully Integrated or Enforced

Since its inception, DIAP has been involved in the development and integration of departmentwide IA policies. For example, the DIAP staff provided support by developing a pilot library of IA policy. The I&IA staff partially addressed the need for policy integration and evolution planning by performing a high-level analysis of existing policy to develop an IA policy framework and to identify gaps and issues. The Joint Staff's Office of IA also partially addressed this area by developing a matrix summarizing IA

documents applying only to the military services. The Joint Staff plans to continue updating military guidance with IA considerations. The DIAP staff plans to continue its support for policy development through participation in department IA working groups, and expects to expand the content and search capabilities of its policy tool, provide demonstrations and briefings, and distribute copies of the tool if adequate funding is provided for fiscal year 2001.

The primary means for considering changes to IA policy within the department is now the IA Panel, which was formed to provide advice on IA policy to the Director of IA and the Military Communications-Electronics Board (MCEB)—a group of department-level executives responsible for providing guidance, direction, and coordination on communications and electronics matters for DOD components. The panel has addressed several areas of policy development, such as the use of mobile code[18] and foreign national access to DOD's unclassified network. Other groups such as the DIAP staff and I&IA staff contributed to IA policy development in areas such as computer network defense and the Global Information Grid[19] by collaborating with a wide range of working groups and Defense organizations. In addition, staff in I&IA led the coordination efforts of the department's IA Policy Working Group.

Although progress has been made in selected areas of IA policy, representatives of the IA Panel, DIAP staff and I&IA staff stated that they had not developed a strategy to ensure that the full scope of IA issues associated with DOD policies, directives, and guidance are being addressed. In addition, DIAP officials stated that they were not assessing the departmentwide implementation of IA policy, as assigned in the implementation plan, and had no plans to determine compliance with IA policies across DOD.

[18]Mobile code is software that is brought into a user's computer system from a remote location and executed without the user's explicit consent.

[19]DOD defines the Global Information Grid as the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policymakers, and support personnel.

Other Functional Areas Have Not Been Fully Addressed

DIAP has not fully addressed its assigned responsibilities in three other areas—architectural standards and system transformation, acquisition support and product development, and research and technology. A variety of other entities within the department were also involved in these areas. However, their work was not coordinated or integrated with other related DIAP activities.

In the area of architectural standards and system transformation, DIAP was to ensure integration of IA technologies, products and procedures through approaches such as enterprisewide standards and incremental improvement. DIAP's activities in IA architecture focused on participating in the IA Architecture Working Group formed in August 1999. The initial task of this group was to produce an IA architecture prototype based on the systems and operations of the United States Pacific Command. With DIAP staff participation, the group identified information exchange requirements for the command and developed an IA architectural framework to describe existing and future IA capabilities. The group expects to apply its architectural framework to additional Defense environments, however, no detailed plan has been developed.

Although it was initially involved in the working group's activities, continued DIAP participation is uncertain. The DIAP staff position for IA architecture has been vacant since November 1999, and the DIAP staff has not integrated this work into its other activities.

Regarding acquisition support and product development, DIAP was to focus on development and implementation of guidance for department IA requirements, products, and technology trends. However, no milestones were established, and DIAP management told us that no significant progress had been made. For example, an effort to revise DOD directives to address IA-related acquisition was suspended because it could not be completed in time to be integrated with other upgrades to DOD policies. Plans for fiscal year 2001 focus on different issues, such as placing an IA advocate in each department group involved in IT acquisitions, increasing Defense program managers' awareness of IA-related issues, and proposing improvements to DOD directives to address IA in acquisitions.

In the area of research and technology, the DIAP was tasked with leveraging existing research and development activities inside and outside DOD to ensure that they are consistent with the department's mission needs and changes in IT. While some actions were initially taken by DIAP staff to participate in IA research coordination activities, DIAP has stopped doing this and is no longer working towards this objective. Specifically, DIAP staff in the past participated in the INFOSEC Research Council, an affiliation of Defense research organizations[20] that coordinates DOD efforts relating to IA research and development. The council identified a list of "hard problems" in IA research to aid in planning research and also developed a database of IA-related research programs. Since the departure of the DIAP staff member for IA research in February 2000, however, there has been little coordination between DIAP staff and the council, and no efforts have been undertaken to link existing IA research work to other areas of DIAP responsibility such as policy development or acquisition, as called for in the DIAP implementation plan. Furthermore, the staff has no plans to coordinate or integrate IA research with other DOD technology management activities, such as forecasting and technology transfer, which are important in an environment of rapid technology change.

DIAP Faces Management Challenges That Have Hindered Progress

DIAP's progress has been hampered by several challenges in establishing an infrastructure for Defense-wide IA to support the department's goals. Specifically, DOD has not yet applied an effective management framework for structuring, operating, and overseeing Defense-wide IA efforts consistent with the characteristics of high-performing organizations. Little evidence exists that the management practices associated with model organizations have been applied to DIAP, and DOD executives acknowledged that such practices were not in place. Moreover, DIAP has not been staffed as intended, and guidance and oversight activities have been weakened by a lack of continuity in key organizations responsible for those areas. Consequently, some functions assigned to DIAP have not been fulfilled. Taken together, these challenges have limited DIAP accomplishments and impeded DOD's ability to determine the effectiveness of its IA improvement efforts.

[20]Consistent participants on the INFOSEC Research Council have included: the Army, the Navy, the Air Force, the Central Intelligence Agency, the Defense Advanced Research Projects Agency, NSA, the Department of Energy, and the National Institute of Standards and Technology.

DOD Has Not Applied Characteristics of Leading Organizations to IA Management

Over the past decade, the Congress has established a framework designed to create and sustain high-performing organizations across the government.[21] Our work in assessing federal agencies under this legislation and guidance has consistently shown the need to build and strengthen their management through a disciplined implementation of management practices, such as those used by high-performing organizations: [22]

- A clear mission and vision that is communicated by top leadership.
- A strategic planning process that yields results-oriented goals and measures.
- Organizational alignment to achieve goals.
- The use of sound financial and performance information to make decisions.
- The strategic use of technology to achieve goals.
- Effective management of human capital.

We identified concerns about DIAP in each of these six areas.

DOD Leadership Lacks a Unified Mission and Vision for DIAP

A clear and consistent mission and vision of an organization's path through change is essential to obtaining strong, visible, and sustained commitment of top leadership. Communication of the common mission and vision throughout an organization ensures that program roles are understood and fulfilled. Differences in understanding of and commitment to an organization's mission and vision can hamper the effectiveness of decision-making processes, management approaches, personnel development, and program integration.

We found disagreement among DOD officials regarding DIAP's mission and vision and, in some cases, a lack of support for the role of DIAP as outlined in its implementation plan. Officials representing several DOD components expressed a need for products and activities planned for DIAP such as IA policy and training. They also stated that the current level of coordination and planning would not have occurred without DIAP and the visibility provided by that program. However, other officials cited a lack of DOD

[21]Elements of this framework include the 1993 Government Performance and Results Act; the 1990 Chief Financial Officers Act and related financial management legislation; and information technology reform legislation, including the 1996 Clinger-Cohen Act.

[22]*Management Reform: Using the Results Act and Quality Management to Improve Federal Performance* (GAO/T-GGD-99-151, July 29, 1999).

leadership and support for DIAP and stated that individual components should continue to manage their own IA activities without DIAP involvement. Taken together, these views indicate that support for DIAP is not consistent across the department and that communication about DIAP's mission and vision from DOD leaders has not been adequate.

DIAP Has Not Developed Performance Goals or Measures

Results-oriented goals and quantifiable measures provide essential mechanisms for promoting a common view of what is to be accomplished and for assessing the progress of programs. DIAP was specifically charged with the development of Defense-wide IA performance goals, standards, and metrics in its eight functional areas, a central responsibility for performance-based management.

DOD executives acknowledged the need for comprehensive performance goals and measures to manage DIAP and its staff, but also acknowledged that this approach is not yet being used. Departmental IA readiness metrics are under development, and performance goals and metrics have been drafted for the DIAP staff; however, both products require further development and are not yet suitable for assessing performance. Further, none of DOD's IA annual reports, which are prepared by the DIAP staff, have presented data that show how DIAP's activities have helped achieve the department's IA goals.[23]

DOD officials have concluded that work on performance goals and measures cannot start before a baseline of IA resources is established. Yet progress in establishing a program baseline has been slow, as previously noted. As a result, it is unknown when departmental performance goals and measures will be completed or when DOD will be able to use them to conduct performance-based IA management.

Contributions From DOD Organizations Are Not Integrated to Achieve DIAP Goals

High-performing organizations find ways to integrate contributions from various efforts to support organizational processes and achieve expected results. Effective integration requires that contributors understand and are committed to their assigned responsibilities. Mechanisms for ensuring the accountability of contributors are also important for supporting organizational goals.

[23] *DOD CIO Annual Information Assurance Report*, May 1999, and 1999 DOD CIO Annual Information Assurance Report, February 2000.

As described in appendix I, responsibilities for achieving DIAP goals are dispersed among various organizations. In addition to its executive positions, advisory bodies, and coordination groups, DIAP has sponsored or participated in at least 39 IA-related working groups involving three distinct reporting chains (civilian defense, military, and intelligence). Yet Defense policy does not assign DOD components and their managers specific responsibilities with regard to DIAP and its groups nor are mechanisms to enforce such responsibilities in place. Without specific definition of their responsibilities and accountability for their involvement with DIAP activities, Defense components have provided inconsistent support in areas such as assigning staff, responding to information requests, attending coordination meetings, and reporting plans and progress on DOD IA initiatives. A DIAP Program Execution Plan, as envisioned in the 1999 *DOD CIO Annual Information Assurance Report*, would clarify organizational responsibilities with regard to DIAP, but such a plan has not yet been developed.

The DIAP staff itself cannot require DOD components to contribute to its activities or respond to its requests for information. Further, DIAP managers have no mechanism for ensuring that DOD organizations meet their commitments to provide staff to the program. In addition, DIAP funding, which is provided by OASD(C^3I), is not clearly distinguished from funding for other department IA activities and is subject to competition from the other projects funded by OASD(C^3I).

Changes in the purpose and constituents of organizations such as the IA Group, the Senior IA Steering Committee, and DOD's CIO Council have also impeded the alignment of defense organizations with DIAP goals. According to DOD officials, these organizations did not begin to address their responsibilities for guidance and oversight until their reconstitution as the IA Panel and the CIO Executive Board in late 1999 and early 2000. Clear and comprehensive definition of and accountability for the assignments for these groups and their interaction with other areas of DIAP are essential to ensuring alignment of DIAP groups and goals.

Financial and Performance Information Needed for IA Program Decisions Is Unavailable, Incomplete, or Unverified

Accurate, reliable, and timely data form the foundation for sound management decision-making. Obtaining quality data is dependent on the procedures used to verify and validate the data collected for performance assessment. Well-established data definitions and collection procedures are essential to building confidence in performance information.

DOD officials were unable to provide information on the department's total budget, expenditures, and departmental status for IA and could not estimate when that information would be available. This is due, in part, to limitations in capturing the IA-related data by the automated systems DOD uses for planning, programming, and budgeting; readiness reporting; and personnel classification, as described in the sections on accomplishments earlier in this report. According to DOD officials, problems have also surfaced with collection and verification of component programmatic, financial, and technical data for DIAP due to differences in interpreting terminology and instructions across the Defense community. According to DIAP officials, neither DOD leadership nor DIAP management have assessed the existing systems or procedural limitations for collecting IA data or developed a plan for systematically remedying them. Without timely, reliable, and useful financial and performance reporting, performance-based management for the department's IA activities will be difficult.

DIAP Has Not Yet Planned to Leverage Technology to Achieve Its IA Management Goals

Performance-based management has been shown to work best when it is integrated into the culture and day-to-day activities of organizations. Since IT figures prominently in DOD's view of IA implementation—as shown by initiatives on PKI, intrusion detection, and vulnerability management—such technology presents DOD with opportunities to establish an electronic foundation for IA performance management.

Although DIAP has supported the definition and planning of such technology initiatives, DIAP officials told us that they have not yet evaluated the corresponding opportunities for enhancing IA management processes and controls. Elements of a technology vision that would support performance-based management have surfaced in efforts such as the IA architecture framework, but DOD officials agreed that these elements have not yet been integrated at the department level. Planning for integration of IA technologies with IA performance management processes would help to ensure that IA decisions remain relevant to the evolving IA environment.

DOD Has Exhibited Weaknesses in Its Management of DIAP's Human Resources

Organizational success is greatly enhanced by making the right employees available and providing them with the training, tools, structures, incentives, and accountability to work effectively. DOD itself has recognized that the success of it IA initiatives depends on qualified personnel.[24] This success also hinges on the availability and skills of personnel charged with DIAP management.

Although DOD has attempted to improve its utilization of department-level IA staff by consolidating the IA Group and IA Panel, it has not yet taken steps to ensure that DIAP staffing levels consistently meet the department's overall commitment. It also has not addressed several outstanding personnel issues that DIAP officials believe are important to the program's effective operation. Specifically, formal position descriptions that would identify the knowledge, skills, and experience needed by DIAP staff have not yet been developed. In addition, incentives have not been developed for staffing DIAP positions that are hard to fill because of perceived drawbacks in career advancement, nor have clear expectations for personnel performance been set using individual performance objectives and plans. Addressing such issues could provide better overall staffing of DIAP and improve the program's performance.

DIAP Staffing Commitments Have Not Been Met

Although IA is a top DOD IT priority and DIAP is responsible for promoting consistent IA across the department, DOD has never fully staffed the program. Specifically, various DOD organizations have not fully and promptly met their commitments to provide DIAP with staff. It took 8 months for DIAP to acquire its initial staff, and it has not achieved the total of 30 to 34 personnel specified in its approved implementation plan. Instead, the greatest number of these positions filled at any one time has been 16. During our review, the DIAP staff consisted of 12 personnel primarily detailed from NSA and DISA. The Joint Staff, military services, and other Defense agencies were also directed through DIAP's implementation plan to provide personnel to the DIAP staff office; however, they have not filled the positions identified in that plan, frequently citing their own personnel shortages as a constraint on assigning staff to departmental IA efforts. These staffing shortfalls have limited the ability of the DIAP staff to achieve its objectives and reach its planned full operational capability, and have impeded development of performance

[24] *Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense*, Final Report, August 27, 1999.

goals, measures, and plans that would further define the responsibilities and future efforts for DIAP.

In addition to staffing shortfalls, continuing changes to department-level groups during the life of DIAP—specifically, the IA Group, the Senior DIAP Steering Group, and DOD's CIO Council—have limited the guidance and oversight of DIAP's initial work. In the fall of 1999, the IA Group formed by DOD's IA Management Plan was merged with a previously existing working group, the IA Panel. The groups were examining related issues and held substantially the same membership, which created creating scheduling conflicts that affected meeting attendance. The reconstituted IA Panel has incorporated the responsibilities of the IA Group into its mission and reports to both the MCEB and the Director of I&IA. The official charters of the IA Panel and MCEB reflecting these role changes had not been approved at the close of this review. Nevertheless, the IA Panel has provided a forum for information exchange among components on IA issues and was acknowledged during several of our interviews as an effective mechanism for department IA coordination.

The disbanding of the Senior DIAP Steering Group has also contributed to DOD's limited guidance and oversight of DIAP. The steering group had been intended to provide strategic direction and guidance on IA issues to DIAP and later to the DOD CIO and CIO Council. At the close of our review, strategic direction and guidance for department IA were being developed by staff in the Office of I&IA. However, the draft IA Panel charter indicates that MCEB would share this role with the Director of IA. Accordingly, a revision to the MCEB charter was being coordinated to reflect its added IA responsibilities.

Neither the DOD CIO Council nor its successor, the CIO Executive Board, have provided direction or guidance to DIAP to date, although both have discussed departmental IA issues. The DOD CIO Council, chartered 8 months before the formation of DIAP, was officially disbanded in March 2000 by the Deputy Secretary of Defense and replaced by the larger CIO Executive Board to provide a more decision-oriented approach toward department acquisition, management, use, and oversight of technology. DIAP management and implementation plans had called for increasing Defense agency representation on the CIO Council to improve its ability to address IT and IA across the department. However, the new CIO Executive Board has not adopted this approach. Instead, its membership does not include many DOD agencies, and thus these agencies do not participate in board decisions.

Conclusions

While DIAP has addressed issues related to DOD's departmental IA goals, established new IA policy, improved communication across the department, and initiated mechanisms for monitoring IA efforts throughout DOD, many IA issues remain on which it has not taken action or only begun to work. Given the high priority that DOD puts on IA, we believe the DIAP should have made progress on more of its implementation plan objectives by this time and gone further with the ones it has begun to address. Top-level DOD management has not carried out oversight commensurate with the program's high-priority role nor has DIAP received the resources that were judged necessary by DOD when the program was initiated. DOD continues to face significant personnel, technical, and operational challenges in implementing an effective departmentwide IA program—something it cannot afford to ignore. A stronger management framework for DIAP consisting of adequate funding and oversight would establish the foundation needed to make greater progress in addressing such challenges.

Recommendations for Executive Action

To significantly improve departmentwide management of IA, we recommend that the Secretary of Defense take the following actions:

- Commit senior department personnel to developing a DIAP Program Execution Plan that further defines and integrates DIAP-related roles and responsibilities, organizational relationships and accountability, ongoing efforts, and plans; establishes commitments to DIAP at the component, service, and agency levels; specifies measurable outcomes related to department operations for determining the success of DIAP and time frames for achieving them; and builds on existing DIAP accomplishments.
- Establish written objectives and agreements for departmentwide support of DIAP that provide for clear and realistic responsibilities, adequate personnel, expected outcomes, and mechanisms for monitoring and enforcing agreements. The agreements should specify the organizational positions and entities responsible for integrating DOD's IA actions, managing IA-related aspects of DOD's mission performance, and providing independent oversight and assessment of IA improvement.
- Establish a structured process led by the DOD CIO and CIO Executive Board for regularly monitoring the progress of DIAP toward achieving department goals and using these results to adjust IA program objectives and resources.

- Reinforce the department's commitment to the high priority of IA by providing regular reporting to the Secretary of Defense on the progress, issues, and results of actions to establish IA readiness assessment across the department.

We also recommend that the DOD CIO take the following actions:

- Define a program budget element or subelement that encompasses IA-related personnel and activities of OASD(C^3I) and provides an annual approved budget, adequate and appropriate personnel, and performance goals and measures.
- Establish, document, and implement a performance-based management plan and process for the DIAP staff consistent with those of high-performing organizations.

To enhance progress in achieving the DIAP's IA goals, we recommend that the OASD(C^3I) Director of Information Assurance take the following actions:

- Develop and implement a plan for instituting IA readiness metrics that addresses key obstacles that have hindered efforts to date through (1) enhancements to existing automated reporting systems to capture IA-related data, (2) improved coordination between proposed department-level and joint force IA metrics, and (3) validation of the proposed metrics to ensure that they produce useful information.
- Develop and implement an action plan for achieving the department's July 2000 IA human resources policy directive.
- Develop comprehensive operational polices and procedures to provide consistency in IA monitoring and management across the department,
- Expand security management technology planning to include issues beyond PKI, including workstation security, virtual private networks, and security management tools.
- Complete development of an IA program baseline, including establishing a detailed system of budget codes for identifying IA resources across the department and integrating planning, programming, and budgeting data with the department's acquisition management and requirements-generation systems.
- Develop and implement a strategy for establishing an integrated set of DOD IA policies, directives, and guidance, and establish a mechanism for determining whether DOD components are in compliance.

- Take steps to fully address assigned DIAP responsibilities in three other areas—architectural standards and system transformation, acquisition support and product development, and research and technology.

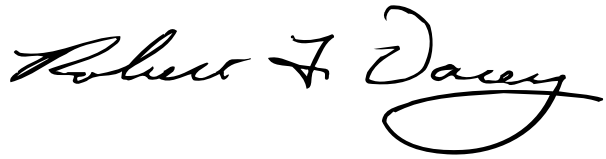
Agency Comments and Our Evaluation

In oral comments on a draft of this report, the Deputy Assistant Secretary of Defense for Security and Information Operations concurred with all of our recommendations except one. Regarding our draft recommendation that the DIAP Director develop a strategy for establishing an integrated set of IA policies, directives, and guidance, DOD stated that IA policy development was the responsibility of the IA Directorate within OASD(C^3I) rather than the DIAP Staff Director. We agree that IA policy development should be managed within the IA Directorate, and in the final report we have revised our recommendation so that it is addressed to the OASD(C^3I) IA Director. For consistency, we also directed several other recommendations to the OASD(C^3I) IA Director. DOD provided additional information on its planned and ongoing efforts to address our recommendations, and we incorporated that information into our report where appropriate.

As agreed with your office, unless you publicly announce the contents of this report earlier, we will not distribute it until 30 days from the date of this letter. At that time, we will send copies of this report to Representative Ike Skelton, Ranking Minority Member of the Committee on Armed Services, House of Representatives; Representative Curt Weldon, Chairman, and Representative Solomon P. Ortiz, Ranking Minority Member, of the Subcommittee on Military Readiness, House Committee on Armed Services; and other interested congressional committees. We are also sending copies to the Honorable Donald H. Rumsfeld, Secretary of Defense; the Honorable Rudy de Leon, Deputy Secretary of Defense; and the Honorable Arthur L. Money, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence and Chief Information Officer. This report will also be available on GAO's home page at *http://www.gao.gov*.

If you or your office have any questions on this report, please call me at (202) 512-3317. Major contributors to this report included John de Ferrari, Peggy Hegg, and Paula Moore.

Sincerely yours,



Robert F. Dacey
Director, Information Security Issues

DIAP Interorganizational Relationships

The table below identifies the key entities and officials that interact with DIAP and their associated responsibilities. The composition of each group is described. Figure 1 provides a conceptual view of DIAP interorganizational relationships.

Table 1: Entities Interacting With DIAP and Their Responsibilities

Entity/official	Responsibilities	Composition	Date named to support DIAP
DOD Chief Information Officer (CIO)	Oversees development and implementation of DIAP Establishes processes to ensure appropriate review of IA program goals and investments	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C^3I))	January 30, 1998
DOD CIO Council	Monitors and coordinates the department's investment review, budget formulation, and financial execution for IT	DOD CIO Deputy DOD CIO CIOs of armed services Undersecretaries of Defense for Policy, Acquisition and Technology, and Comptroller Directors of Program Analysis and Evaluation Joint Staff DISA (technical adviser)	January 30, 1998 (disbanded March 31, 2000)
CIO Executive Board	Advises the DOD CIO in information management, interoperability, and security Coordinates with the Intelligence Community (IC) CIO Executive Council	All CIO Council positions[a] Undersecretary of Defense for Personnel and Readiness CIOs for Joint Staff, IC, and Joint Forces Command ASD(C^3I) Directors from the Navy and Air Force Director of NSA (security adviser) DOD General Counsel (legal adviser)	March 31, 2000

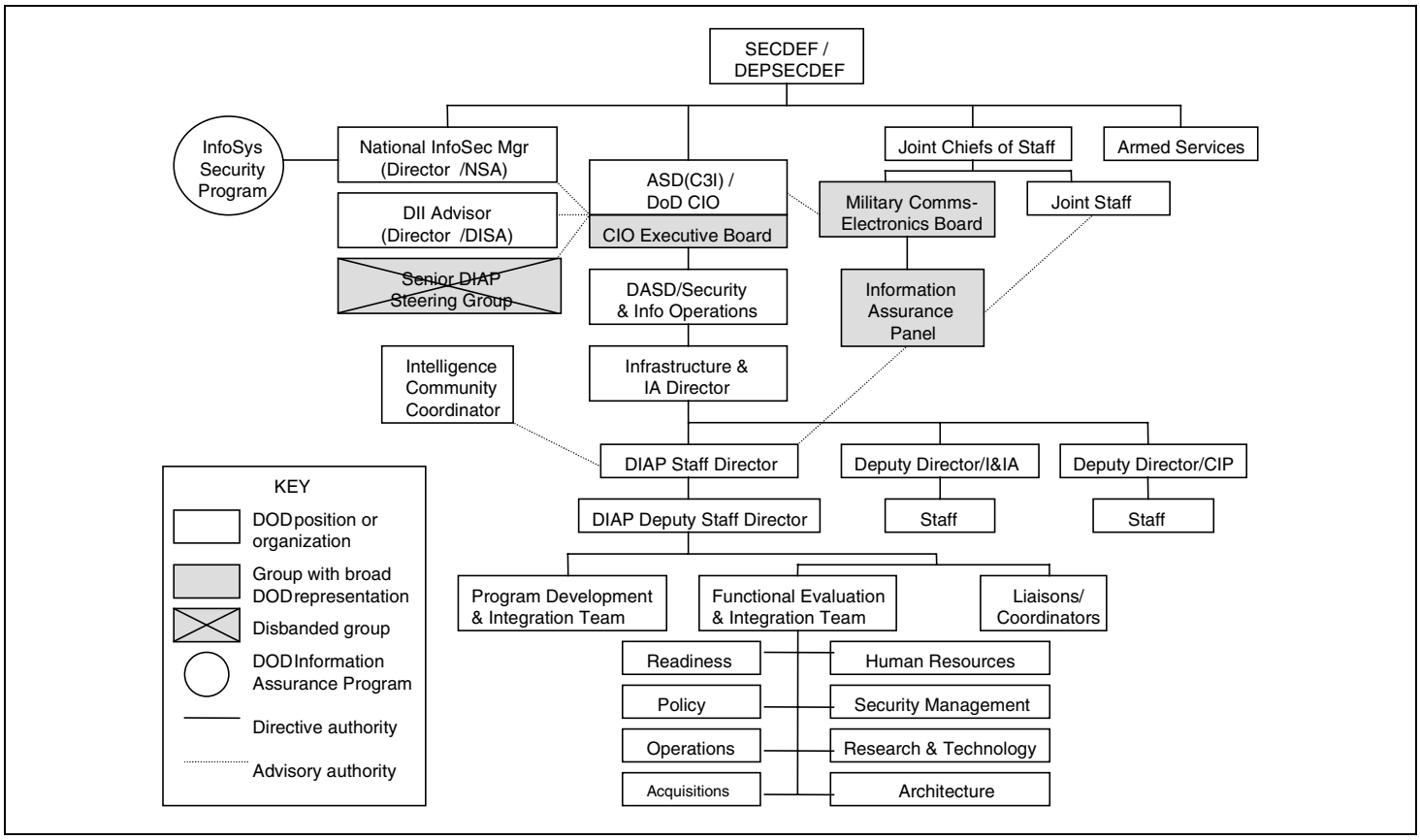
(Continued From Previous Page)

Entity/official	Responsibilities	Composition	Date named to support DIAP
National INFOSEC	Disseminates threat information Assesses overall security posture and vulnerability of national security systems	Director of NSA	January 30, 1998
Defense Information Infrastructure Adviser	Plans, develops, and supports C^3I systems Engineers system, network, and security of Defense Information Infrastructure	Director of DISA	January 30, 1998
IA Group	Develops and recommends coordinated positions on department IA issues	Representatives from Defense components DIAP Staff Director (chair)	January 30, 1998 (effectively merged with the IA Panel October 1999)
IA Panel	Assesses and recommends DOD positions on IA Identifies and raises issues to the MCEB and the Director of I&IA Reviews IA programs to optimize resources Recommends implementation authority for IA policies and procedures Determines effectiveness of and adherence to existing DOD IA directives	Representatives from Defense components and the U.S. Coast Guard DIAP Staff Director and J6K (cochairs)	Implemented as of October 15, 1999 (awaiting formal approval of MCEB charter containing list of subordinate positions)
Senior DIAP Steering Group	Provides strategic direction and guidance on IA issues to DOD CIO and CIO Council	Executives drawn from military services and IA Defense agencies	January 30, 1998 (effectively disbanded prior to this review)
DIAP Staff Director	Coordinates DIAP development within DOD PPBS Develops process to assess returns on IA investments Oversees execution of DOD IA policies, functions, and program	Position in OASD(C^3I)	February 12, 1999
IC Coordinator	Ensures integration and compatibility of IC and DOD IA efforts	Representative from the Office of the Director of Central Intelligence	February 12, 1999

[a]The CIO Council also included the Principal Director for Information Management, Office of the Deputy Assistant Secretary of Defense for Command, Control, and Communications, as the Executive Secretary. For the CIO Executive Council, this representative was eliminated and the Executive

Secretary role was assigned to the Deputy CIO of DOD. In another change, the Under Secretary for Acquisition and Technology on the CIO Council was replaced by the Under Secretary for Acquisition, Technology and Logistics on the CIO Executive Board.

Figure 1: Key Entities Interacting With DIAP and Their Relationships



DIAP Staff Responsibilities According to the DIAP Implementation Plan

DIAP's Program Development and Integration Team

The Program Development and Integration Team (PDIT) is responsible for overseeing, coordinating, and integrating departmental information assurance (IA) resources. Specifically, PDIT is responsible for

- developing broad, easily understood, operationally oriented DIAP categories;
- developing input to the Defense planning guidance for DIAP components;
- overseeing component participation in the Planning, Programming, and Budgeting System (PPBS);
- continually monitoring the IA plans, activities, and resource investments of the components and, in conjunction with the Critical Asset Assurance Program, assessing the adequacy of resources necessary to ensure the continual operational readiness of the Defense information infrastructure;
- preparing IA program guidance on behalf of the DOD Chief Information Officer (CIO);
- correlating responses to IA program queries from the Congress, the Undersecretary of Defense (Comptroller), and the Office of Planning, Analysis, and Evaluation;
- preparing and coordinating the DOD CIO's annual IA assessment;
- developing, coordinating, and supporting DOD-wide program and resource issues for submission by the Director of Information Assurance to the Senior DIAP Steering Group, and providing support to the Office of Planning, Analysis, and Evaluation as part of the Defense Resources Board process;
- reviewing and recommending, as appropriate, adjustments to the component program objective memorandums to support the integrated priority lists of the unified combatant commanders;
- preparing, in coordination with the Information Systems Security Program staff, the DIAP *Congressional Justification Book*;
- working with staff of the Undersecretary of Defense (Comptroller) and the Office of Planning, Analysis, and Evaluation to design and implement appropriate budget exhibits for collecting, monitoring, and reporting DIAP resources; and
- developing and coordinating input for the IA portion of the DOD Information Technology Strategic Plan.

DIAP's Functional Evaluation and Integration Team

The Functional Evaluation and Integration Team (FEIT) is responsible for overseeing, coordinating, and integrating departmental IA activities and for providing a means to measure their effectiveness. Specifically, FEIT's staff is responsible for

- serving as principal evaluators for each of FEIT's functional areas (see below);
- ensuring integration of their particular functions with the other functions of FEIT;
- providing continual evaluation of component IA programs to ensure the Defense-wide application of FEIT's capabilities;
- ensuring that their functions are consistently implemented, integrated, efficient, and programmatically supported;
- developing solutions, such as program recommendations, when components fail to provide necessary resources for their IA programs;
- supporting presentations of DIAP issues to the Defense Resources Board and Joint Requirements Oversight Council;
- developing Defense-wide IA performance goals, standards, and metrics; and
- providing functional oversight and ensuring coherent integration throughout DOD.

The eight functional areas of FEIT are readiness assessment, human resources, policy integration, security management, operations environment, architecture standards and transformation strategies, acquisition support and product development, and research and technology. Detailed descriptions of the functional areas are provided below.

Readiness Assessment

The readiness assessment area is responsible for providing data needed to accurately assess IA readiness and for focusing plans, programs, and decisions within PPBS. Specific responsibilities include addressing

- IA requirements identification,
- vulnerability and threat assessments, and
- Defense-wide IA-related standards and metrics for military readiness reporting.

Human Resources

The human resources area is responsible for providing for sufficient, adequately trained and educated personnel to conduct IA functions throughout the department. Specific responsibilities include addressing

- human resources development;
- education, training, and awareness; and
- manpower.

Policy Integration

The policy integration area is responsible for providing consistent implementation of DOD IA-related policies throughout the department. Specific responsibilities include addressing national security, federal government, and IA policies and priorities.

Security Management

The security management area is responsible for providing for the incorporation of appropriate security services that allow and promote global interoperability while preserving legitimate law enforcement and national security purposes. Specific responsibilities include addressing

- key management,
- workstation security,
- virtual private networks,
- tools and security management applications, and
- development of an integrated security management infrastructure.

Operational Environment

The operational environment area is responsible for providing for the continual visibility of the department's and the intelligence community's IA operational readiness postures through appropriate monitoring of the enterprise information systems and through other intelligence and law enforcement sources. Specific responsibilities include addressing

- operational monitoring and network management,
- intrusion detection,
- incident response,
- defensive information operations, and
- attack sensing and warning.

Architectural Standards and System Transformation

The architectural standards and system transformation area is responsible for providing for the integration of adequate IA technologies, products, and supporting procedures in the information technologies (IT), systems, and networks acquired by the department. Specific responsibilities include addressing

- enterprisewide standards and conformance,
- implementation and incremental improvement,
- modernization of legacy systems,
- survivability of common infrastructures,
- accreditation and readiness standards,
- multilevel security, and
- embedded IA capabilities.

Acquisition Support and Product Development

The acquisition support and product development area is responsible for providing for continual improvement in the department's IA readiness posture through disciplined, performance-based investments in security-enabled IT acquisitions. Specific responsibilities include addressing

- development of IA-related acquisition guidance;
- integration of mission need statements and operational requirements documents;
- review of departmental protection profiles;
- identification of technology, product, and acquisition trends and the development of strategies for dealing with those trends; and
- product evaluation, validation, and integration guidance.

Research and Technology

The research and technology area is responsible for providing for the research and development of IA technologies and techniques consistent with current and anticipated DOD mission needs and changes in IT. Specific responsibilities include addressing

- leveraging of DOD, government, commercial, and academic research;
- anticipation of new technologies;
- development of synchronized IA solutions;
- budget categories; and
- leveraging of existing research coordination activities.

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. 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

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

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
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.

Orders by Internet:
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

To Report Fraud, Waste, or Abuse in Federal Programs

Contact one:

- **Web site: http://www.gao.gov/fraudnet/fraudnet.htm**
- **e-mail: fraudnet@gao.gov**
- **1-800-424-5454 (automated answering system)**

PRINTED ON RECYCLED PAPER

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

Official Business
Penalty for Private Use $300

Address Correction Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00