~~FOR OFFICIAL USE ONLY~~

Audit Report

INFORMATION ASSURANCE CHALLENGES–
A SUMMARY OF AUDIT RESULTS REPORTED
DECEMBER 1, 1998, THROUGH MARCH 31, 2000

Report No. D-2000-124 May 15, 2000

Office of the Inspector General
Department of Defense

~~FOR OFFICIAL USE ONLY~~

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

May 15, 2000

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)

SUBJECT: Audit Report on Information Assurance Challenges-A Summary of Audit Results Reported December 1, 1998, through March 31, 2000 (Report No. D-2000-124)

This summary report is provided for your information and use. This report contains no recommendations, no written comments were required, and none were received.

Questions on the report should be directed to [redacted] at (703) 604-[redacted] (DSN 664-[redacted] ([redacted]@dodig.osd.mil) or [redacted] at (703) 604-[redacted] (DSN 664-[redacted] ([redacted]@dodig.osd.mil). See Appendix E for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

~~FOR OFFICIAL USE ONLY~~

Office of the Inspector General, DoD

Report No. D-2000-124 May 15, 2000
(Project No. 0AS-6104.01)

Information Assurance Challenges–A Summary of Audit Results Reported December 1, 1998, through March 31, 2000

Executive Summary

Introduction. Information assurance is emerging as a critical component of DoD operational readiness. When effective, information assurance enables the systems and networks composing the Defense information infrastructure to provide protected, continuous, and dependable service in support of both warfighting and business missions. On December 30, 1999, the Deputy Secretary of Defense issued a memorandum, "Department of Defense Information Assurance Vulnerability Alert," which stated that information assurance is an essential element of operational readiness and can no longer be relegated to a secondary concern.

Objectives. The objective of this report is to summarize information assurance findings in audit reports issued by the General Accounting Office; Office of the Inspector General, DoD; and Air Force Audit Agency from December 1, 1998, through March 31, 2000.

Results. Achieving information assurance continues to pose significant challenges to the Department. Twenty-one reports (see Appendix B) show that information assurance continues to vary among DoD organizations because security measures are not consistently implemented. The reports show that varied problems exist in the following areas:

- limiting inappropriate access to computer systems, programs, and data (11 reports);
- certifying and accrediting of the security posture of a system (6 reports);
- contingency planning (8 reports);
- assessing risks (10 reports); and
- security training (8 reports).

Although the DoD Chief Information Officer undertook many initiatives to mitigate information assurance risks, the DoD Chief Information Officer did not promulgate updated DoD policy requirements for minimum protection standards. Further, DoD still needs to devise a methodology to measure the status and progress of information

assurance, to estimate information assurance budget requirements, and to evaluate the return on investments made in information assurance. Unless the DoD Chief Information Officer undertakes additional measures at the DoD enterprise level to better manage DoD-wide information assurance risks and the investments to better mitigate those risks, DoD Components' mitigation efforts will continue to be inconsistent, localized, and short-lived.

Management Comments. We provided a draft of this report on March 31, 2000. Because the report contained no recommendations, written comments were not required, and none were received. Therefore, we are publishing this report in final form.

Table of Contents

Introduction

Information Assurance. Information assurance is emerging as a critical component of DoD operational readiness. When effective, information assurance enables the systems and networks composing the Defense information infrastructure to provide protected, continuous, and dependable service in support of both warfighting and business missions. Availability, identification and authentication, confidentiality, integrity, and non-repudiation are the fundamental attributes of information assurance.

- **Availability.** Timely, reliable access to data and services for authorized users.
- **Identification and Authentication.** The process an information system uses to recognize an entity. Authentication is a security measure designed to establish the validity of a transmission, message, or originator, or to verify an individual's authorization to receive specific categories of information.
- **Confidentiality.** Assurance that information is not disclosed to unauthorized persons.
- **Integrity.** Protection against unauthorized modification or destruction of information.
- **Non-repudiation.** Assurance that the sender of the data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

FY 1999 DoD Annual Statement of Assurance. The statement reports that information assurance is a systemic weakness in the DoD, and that numerous computer system intrusions occurred over the last several years that highlighted the vulnerability of DoD information systems to attack. DoD dependence on information systems makes information assurance a critical readiness issue. Although many corrective actions have been implemented, intrusions continue to occur.

The FY 1998 DoD Chief Information Officer Annual Information Assurance Report, May 1999. The annual report states that information is indispensable to all aspects of mission planning and execution. Further, if mission participants cannot accurately exchange information in a timely manner and ensure the availability, integrity, and, in some cases, the confidentiality of that information, missions will fail. The timely availability of information is universally acknowledged within DoD as critical to mission accomplishment in all operations.

The annual report outlines 11 major DoD information assurance initiatives and other actions taken to address the persistent problem of securing DoD information systems. The report also acknowledges that the efforts will not solve the problem, but they will put in place a process for responding to changing threats and conditions. The report states that the DoD initiatives and

ongoing actions will continuously "raise the bar" against potential adversaries and will enable military forces to gain and maintain information superiority. Appendix C summarizes the 11 initiatives.

The FY 1999 DoD Chief Information Officer Annual Information Assurance Report, February 2000. The annual report describes recent DoD initiatives, their accomplishments and issues. The annual report notes that numerous Government Accounting Office reports, DoD Inspector General reports, and DoD-sponsored studies, both internal and external, pointed out deficiencies and vulnerabilities in the protection of these systems and the information contained within.

The annual report states that the past year has been one of significantly increased activity in the information assurance arena. Investments and programs initiated in previous years were beginning to show excellent results, with progress being made in addressing complex issues. The document reports on 12 major DoD-wide initiatives and activities at 15 Components, as well as activities at the unified and specified commands and 3 special-interest communities. Appendix D summarizes the 12 initiatives.

Background

Information Assurance Vulnerability Alert (IAVA). On December 30, 1999, the Deputy Secretary of Defense issued a memorandum, "Department of Defense (DoD) Information Assurance Vulnerability Alert (IAVA)," which stated that information assurance is an essential element of operational readiness and can no longer be relegated to a secondary concern.

The IAVAs issued by the Defense Information Systems Agency (DISA) are generated whenever a critical vulnerability exists that poses an immediate threat to the DoD and where acknowledgement and compliance of corrective action must be tracked. The IAVAs are intended to provide positive control of the vulnerability notification and corrective action process within DoD.

Proposed Government Information Security Act of 1999. The bill was introduced in November 1999. The primary objective of the bill is to update existing statutory requirements for information security to address the management challenges associated with operating in the current interconnected computing environment. If passed, Section 2 of the bill would amend Section 3535 of Chapter 35 of Title 44 U.S.C., and would require agencies to perform an annual independent evaluation of their information security program and practices. Inspectors General would be responsible for performing those annual evaluations, either in-house or by using an independent external auditor.

Critical Infrastructure Protection. Presidential Decision Directive 63, "Protecting America's Critical Infrastructure," May 1998, established the President's policy for producing a workable and innovative framework for critical infrastructure protection. The Presidential Directive builds on the recommendations of the President's Commission on Critical Infrastructure Protection, which called for a national effort to ensure the security of the United States' increasingly vulnerable and interconnected infrastructures, including essential Government services.

The Presidential Directive set a goal for a reliable, interconnected, and secure information system infrastructure by 2003 and for significantly increased security to Government systems by 2000. The Presidential Directive requires the Federal Government to serve as a model to the rest of the country on how to attain infrastructure protection.

The DoD issued "The Department of Defense Critical Infrastructure Protection (CIP) Plan," November 18, 1998. The plan responds to Presidential Decision Directive 63, describing the way in which DoD is to organize, identify, and protect DoD-owned infrastructure assets, and how DoD is to interact with entities in the national program to effect that protection. The plan addresses how DoD will protect its portion of Federal Government critical infrastructure.

The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) [ASD(C^3I)] is the DoD Chief Infrastructure Assurance Officer and the Critical Infrastructure Protection Functional Coordinator for National Defense. In these roles, the ASD(C^3I) is responsible for protecting DoD critical infrastructure and for participating in the national program.

DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997. The DITSCAP establishes a standard process, a set of activities, general task descriptions, and a management structure to certify and accredit information technology (IT) systems that will maintain the security posture of the Defense information infrastructure. The DITSCAP applies not only to DoD Components, but also to DoD contractors and agents. The DITSCAP is to be applied to the acquisition, operation, and sustainment of DoD IT systems. Further, the DITSCAP is to be applied to the development of new IT systems, the incorporation of IT systems into an infrastructure, the incorporation of IT systems outside the infrastructure, the development of prototype IT systems, the reconfiguration or upgrade of existing systems, and legacy systems.

Security Readiness Review Process. In 1994, DISA created a task force to assess the security posture of its Defense Megacenters. The task force created an inspection checklist and a database and conducted system and environment reviews to identify security and infrastructure deficiencies. This process evolved into the Security Readiness Review Process. Megacenters and other DISA facilities have a vested interest in the Security Readiness Review Process because the result directly effects the site Certification and Accreditation Process. The Security Readiness Review Process specifically evaluates the security readiness of various DoD activities, as it relates to information systems security and ability of the various responsible organizations to properly protect DISA information resources and assets from attack and/or compromise.

Revision of Office of Management and Budget Circular No. A-130. The Office of Management and Budget is revising Circular No. A-130, "Management of Federal Information Resources," to implement provisions of the Information Technology Management Reform Act of 1996 and for other purposes.

Chairman of the Joint Chiefs of Staff. The Office of the Joint Chiefs of Staff is rewriting Chairman of the Joint Chiefs of Staff Instruction 6510.01B, "Defense Information Operations Implementation," August 22, 1997, to be titled "Information Assurance Implementation (Defense-In-Depth)." The revision will focus on policy and responsibilities for implementing the information assurance Defense In-Depth Strategy. In addition, computer network defense policy and guidance will be incorporated into the instruction for the first time.

Audit and Other Oversight on Information Assurance

Office of the Inspector General, DoD, Report No. D-2000-077, "Statement of the Deputy Inspector General, Department of Defense, Before the Subcommittee on Budget, House of Representatives on Defense Management Challenges," February 17, 2000. The Deputy Inspector General, DoD, stated that the DoD internal audit community, the General Accounting Office (GAO), and other reviewers had outlined DoD information assurance challenges in numerous reports. To meet those challenges, DoD needs to:

- adapt lessons learned from the year 2000 conversion effort;
- consolidate and update policy guidance;
- establish better management control over the many separate efforts now under way or planned;
- develop reasonable program performance measures;
- ensure full attention to information assurance concerns in new system development and electronic commerce initiatives;
- intensify on-site information security inspection and audit efforts; and
- improve training across the board for technical personnel, security officers, and systems users.

The DoD is turning increased attention to these matters, but a sustained effort will be needed for the foreseeable future.

GAO/T-AIMD-00-72, "Critical Infrastructure Protection-Comments on the National Plan for Information Systems Protection," February 1, 2000. In his testimony before the Subcommittee on Technology, Terrorism, and Government Information, Committee on the Judiciary, U.S. Senate, the Director for Governmentwide and Defense Information Systems Accounting and Information Management Division, GAO, stated that although many factors had contributed to weak Federal information security-for example, insufficient understanding of risks, technical staff shortages, and a lack of system and security architectures-the fundamental underlying problem is poor security program management. In essence, management needs to take a systematic approach.

Government Accounting Office, Report No. AIMD-99-139, "Information Security Risk Assessment-Practices of Leading Organizations," August 1999. The report states that Federal agencies did not adequately protect their automated operations and electronic data against threats such as malicious actions, inadvertent user errors, and natural and man-made disasters. One of the major underlying problems was poor risk management, which provides the foundation for the other elements in the risk-management cycle. To assist Federal agencies in meeting risk-assessment challenges, the GAO studied four organizations that institutionalized practical risk-assessment methods.

All risk assessments, regardless of type, generally included:

- identifying threats and the likelihood that those threats would occur;
- identifying and ranking critical assets and operations;
- estimating the potential loss or damage;
- identifying cost-effective actions to mitigate or reduce the risk; and
- documenting the assessment findings and action plan.

The report identified common critical success factors that were important to the efficient and effective implementation of an organization's information security risk-assessment programs. Some of these factors were focal point designation, procedures definition, and business unit accountability. All of the organizations developed tools such as tables, questionnaires, standard report forms, and lists of threats and controls to facilitate their risk assessments. Those tools helped to ensure a consistent and standardized approach throughout the organization. Risk-assessment programs help to ensure that the greatest risks to business operations are identified and addressed on a continuing basis and to increase an organization's understanding of risks and controls.

Office of the General Inspector, DoD, Report No. 99-069, "Summary of Audit Results–DoD Information Assurance Challenges," January 22, 1999. The report summarized Defense organizations' information assurance weaknesses that were identified in 75 audit reports issued by the GAO; the Office of the Inspector General, DoD; the Army Audit Agency; the Naval Audit Service; and the Air Force Audit Agency from January 1, 1995, through November 30, 1998. The report grouped the weaknesses into 14 categories, which include the 11 minimum security requirements identified in DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988. The report states that, while audit attention will be given to information assurance, all DoD automated system owners and users must perform a more rigorous self-assessment of their controls than in the past. In addition, the report summarized the following three publications that provide Government organizations with guidance on security management and security implementation: Report No. AIMD-98-68, "Executive Guide Information Security Management Learning From Leading Organizations," May 1998; National Institute of Standards and Technology Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology," September 1996; and National Institute of Standards

and Technology Special Publication 800-12, "An Introduction to Computer Security: the National Institute of Standards and Technology Handbook," October 1995.

Objectives

The objective of this report is to summarize information assurance findings in audit reports issued by GAO; the Office of the Inspector General, DoD; and the Air Force Audit Agency from December 1, 1998, through March 31, 2000. See Appendix A for a discussion of the scope. Appendix B contains a summary of each report and the corrective actions taken.

Information Assurance Management

Achieving information assurance continues to pose significant challenges to the Department. Twenty-one reports (see Appendix B) issued since Office of the General Inspector, DoD, Report No. 99-069, "Summary of Audit Results-DoD Information Assurance Challenges," January 22, 1999, show that information assurance continues to vary among DoD organizations because security measures were not consistently implemented by DoD organizations. The reports show that varied problems exist in the following areas:

- limiting inappropriate access to computer systems, programs, and data (11 reports);
- certifying and accrediting of the security posture of a system (6 reports);
- contingency planning (8 reports);
- assessing risks (10 reports); and
- security training (8 reports).

Although the DoD Chief Information Officer (CIO) undertook many initiatives to mitigate information assurance risks (see Appendix C and Appendix D), the DoD CIO did not promulgate updated DoD policy requirements for minimum protection standards. Further, DoD still needs to devise a methodology to measure the status and progress of information assurance, to estimate information assurance budget requirements, and to evaluate the return on investments made in information assurance. Unless the DoD CIO undertakes additional measures at the DoD enterprise level to better manage DoD-wide information assurance risks and the investments to better mitigate those risks, DoD Component mitigation efforts will continue to be inconsistent, localized, and short-lived.

Access Controls

Access controls, by limiting inappropriate access to computer systems, programs, and data, protect those resources from unauthorized modification, destruction, and disclosure. Access controls authenticate users and restrict their access to certain data, programs, transactions, or commands, based on their job responsibilities. Segregation-of-duties controls ensure that users do not have access to control a transaction from beginning to end. DoD Directive 5200.28 requires all automated information systems to have an access control policy in place, including features or procedures to enforce that policy. Report No. AIMD-99-107, "DoD Information Security-Serious Weaknesses Continue to Place Defense Operations at Risk," August 1999, states that DoD users were granted access to computer resources that exceeded those required to carry out their job responsibilities, including sensitive system privileges. Periodic review

of user access privileges and monitoring of security violations and the use of powerful commands, utilities, and changes to sensitive files and records are essential to prevent and detect unauthorized activity. DISA: (b) (7)(E) [redacted] the Defense Finance and Accounting Service (DFAS), and several Air Force commands. (See Reports No. 1, 2, 3, 5, 6, 7, 9, 10, 13, 17, and 18 in Appendix B.)

Certification and Accreditation

The objective of the certification and accreditation process is to certify that an IT system meets the DITSCAP accreditation requirements and that the system will continue to maintain the accredited security posture throughout its life-cycle.

Certification is a comprehensive evaluation of the technical and nontechnical security features of an IT system and other safeguards that is made in support of the accreditation process to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Accreditation is the formal declaration by the Designated Approving Authority that the IT system is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation of an information system should be supported by a certification plan approved by the Designated Approving Authority in compliance with the DITSCAP; a risk analysis of the information system in its operational environment; a security safeguard evaluation; and a certification report.

DISA: (b) (7)(E) [redacted] One report, Project No. 98066024, "Certification of Standard Systems," September 30, 1999, reviewed six Air Force systems and found that all six were properly certified. (See Reports No. 4, 5, 12, 14, 17, and 18 in Appendix B.)

Continuity of Operations Planning

Directive 5200.28 requires that contingency plans be developed and tested in accordance with Circular A-130 to ensure that automated information system security controls function reliably and that adequate backup functions are in place to ensure that security functions are maintained continuously during interrupted service. Procedures must be in place to recover data if it is modified or destroyed.

DISA: (b) (7)(E) [redacted] (See Reports No. 1, 2, 4, 5, 7, 8, 17, and 18 in Appendix B.)

Risk Assessment and Management

Risk assessment is the process of analyzing threats to, and vulnerabilities of, an IT system, and the potential impact that the loss of information or capabilities of a system would have on national security. The resulting analysis is used as a basis for identifying appropriate and effective measures. Risk management is the process concerned with the identification, measurement, control, and minimization of security risks in IT systems to a level commensurate with the value of the assets protected.

Some reports showed incomplete or inadequate risk management programs. The DoD organizations did not adequately assess risks, use risk assessment to select controls, promote risk awareness, evaluate control effectiveness, or coordinate their security programs through a central focal point. These weaknesses increased the risk of severe disruption and corruption to DoD computer-based infrastructure. (See Reports No. 1, 4, 5, 7, 11, 15, 16, 17, 19 and 20 in Appendix B.)

Security Training

An adequate security training and awareness program is essential to ensure that all system administrators are aware of proper operational and security related procedures and risks. DoD Directive 5200.28 requires all persons accessing an automated information system to have completed a security training and awareness program. Administrators and users should receive specialized training on their responsibilities and the system or application rules before they are granted access to the system.

Chairman of the Joint Chiefs of Staff Draft Instruction "Information Assurance Implementation (Defense-In-Depth)," states that security education, training, and awareness are essential to a successful information assurance program. Mandatory training and/or certification programs for personnel conducting the five "critical" information assurance functions should be established. The five functions are:

- system administration/network administration and operations,
- computer/network crime,
- threat and vulnerability assessments,
- computer emergency response, and
- web security.

Although several of the audited DoD systems had security training and awareness programs in place, inadequate guidance, documentation, and oversight resulted in users not receiving adequate training before they were granted access to sensitive computer systems, data, and programs. As a result, DoD systems were at risk from unauthorized system intrusion and data corruption. (See Reports No. 5, 6, 7, 10, 12, 19, 20 and 21 in Appendix B.)

Conclusion

As illustrated in the 21 reports issued during 1999 since our first summary of audit results on DoD information assurance challenges (Report No. 99-069), the information assurance problem continues to pose significant challenges to the DoD. It remains a horizontal IT problem to the DoD still-vertical organization. As outlined in the FY 1999, DoD CIO Annual Information Assurance Report, the CIO started many DoD-wide initiatives to better manage and mitigate the information assurance risks. However, to adequately meet the information assurance challenge, the CIO needs to finalize a management strategy that answers the following fundamental questions.

- What must be protected?
- What are the minimum protection standards?
- How will the status and progress of information assurance be measured?
- How will budget requirements be estimated for information assurance?
- How will resource investments be measured for payback?

Without a framework containing those answers, risk mitigation efforts will continue to be inconsistent among DoD Components, localized, and short-lived.

Appendix A. Audit Process

Scope

This report summarizes DoD information assurance weaknesses identified in 21 audit reports issued by the General Accounting Office; the Office of the Inspector General, DoD; and the Air Force Audit Agency from December 1, 1998, through March 31, 2000. The Army Audit Agency and the Naval Audit Service did not issue any reports on this subject within the given time frame. In addition, we summarized management's corrective action.

DoD-wide Corporate Level Government Performance and Results Act (GPRA) Coverage. In response to the GPRA, the Secretary of Defense annually establishes DoD-wide corporate level goals, subordinate performance goals, and performance measures. This report pertains to achievement of the following goals.

FY 2001 DoD Corporate Level Goal 2: Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the Revolution in Military Affairs, and reengineer the Department to achieve a 21st century infrastructure. **(01-DoD-2)**

DoD Functional Area Reform Goal. Most DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objective and goals:

- **Information Technology Management Area.** **Objective:** Ensure DoD vital information resources are secure and protected. **Goal:** Build information assurance framework. **(ITM-4.1)**

- **Information Technology Management Area.** **Objective:** Ensure DoD vital information resources are secure and protected. **Goal:** Build information assurance architecture and supporting services. **(ITM-4.2)**

- **Information Technology Management Area.** **Objective:** Ensure DoD vital information resources are secure and protected. **Goal:** Assess information assurance posture of DoD operational systems. **(ITM-4.4)**

General Accounting Office High Risk Area. The General Accounting Office has identified several high-risk areas in the DoD. This report provides coverage of the Information Management and Technology high-risk area.

Appendix B. Summary of Prior Coverage

General Accounting Office

1. Report No. AIMD-99-107, "DoD Information Security-Serious Weaknesses Continue to Place Defense Operations at Risk," August 1999. The report addresses the status of corrective actions that DoD has taken to address specific weaknesses identified in GAO 1996 reports on information security weaknesses in DoD. The report states that serious weaknesses in DoD information security continued to provide hackers and unauthorized users with the opportunity to modify, steal, inappropriately disclose, and destroy sensitive data. These weaknesses impaired the ability of DoD to:

- control physical and electronic access to its systems and data;
- ensure that software is properly authorized, tested, and functioning as intended;
- limit an employee's ability to perform incompatible functions; and
- resume operations in the event of a disaster.

As a result, system attacks and fraud already have adversely affected numerous Defense functions, including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll.

The report states that DoD had initiated some corrective actions in response to the GAO 1996 reports. Further, progress in correcting the specific control weaknesses identified in the reports was inconsistent across the various DoD Components involved, and weaknesses persisted in every area of general controls. The report reaffirmed the recommendations made in the GAO 1996 reports.

The report states that the DISA Security Readiness Review Process, which assesses the security posture of DISA Defense Megacenters, had steadily increased the number of security reviews performed. By the end of November 1998, DISA completed 542 Security Readiness Reviews, generated a total of 14,860 findings, and reported that 11,418 of these findings were corrected. In addition, DISA began drafting technical guidance for individual systems, known as Security Technical Implementation Guides, which specify minimum standards for managing system software security. However, additional action is needed to improve DISA oversight of information security. The audit tested 55 deficiencies that were "accepted-as-fixed" in the System Readiness Review database and determined that about 25 percent had not been corrected.

Finally, the report states that the DIAP implementation plan provided the framework for a DoD-wide information security program. However, because DoD had not implemented the DIAP, it could not determine whether it would ultimately succeed in ensuring adequate security throughout the DoD.

In addition to the reaffirmed recommendations, the report recommended that the Secretary of Defense take the following actions to realize the full potential and maximize the effectiveness of the DISA security oversight programs, the DIAP, and other DoD information assurance initiatives.

- Direct the DISA Director to expand the Security Readiness Review process to include timely and independent verification of the corrective actions reported by Defense Megacenters and other responsible parties.

- Direct the DoD CIO to ensure that the DIAP defines how its efforts will be coordinated with the Joint Task Force and other related initiatives.

The ASD(C^3I) stated that DoD was actively working to correct the deficiencies cited in the report and to reduce the risks to DoD information systems. The continued development of the DIAP and the work of two DoD integrated process teams would yield further benefits to strengthen the DoD information system security posture.

Beginning in May 1999, DISA modified its Defense Megacenter Security Readiness Review audit procedures to include timely and independent verification of entries made on previously documented Security Readiness Reviews. The revised procedures required the Defense Megacenter facility directors to be notified of any incorrect entries and to be notified of any repeat findings. DISA expanded the use of Security Readiness Reviews beyond the Defense Megacenters to include other operating locations and systems, the unified commands, and DoD staff.

The ASD(C^3I) stated that the DIAP and other initiatives in DoD, such as the Joint Task Force Computer Network Defense, would address the computer control weaknesses cited in the report. As of October 1, 1999, the Joint Task Force Computer Network Defense aligned under the Commander-In-Chief, U.S. Space Command, and the DIAP participated in working groups that developed an implementation plan. The DIAP and the Joint Task Force Computer Network Defense meet frequently and work issues through the Joint Staff on a normal and recurring basis.

2. Report No. HR-99-1, "High Risk Series-An Update," January 1999. The GAO first designated information security as a Government-wide, high-risk area in February 1997, because of the evidence indicating that controls over computerized operations were not effective and information that risks were increasing. The report states that systems and data supporting critical Federal operations were not adequately protected. Those weaknesses make it easier for individuals and groups with malicious intentions to intrude into inadequately protected systems and use such access to obtain sensitive information, commit fraud, or disrupt operations; for example, the report cites a September 1998 GAO report that reviewed two cases of Air Force vendor payment fraud. The GAO stated that computer security weaknesses continued to make the Air Force vulnerable to such incidents. The GAO found striking similarities in the control weaknesses across their audits. The most widely reported weakness was poor control over access to sensitive data and systems, such as providing overly broad access privileges to very large user groups, shared passwords, and

inadequate monitoring of users' activities. Other types of weaknesses pertained to mitigating and recovering from unplanned interruptions in computer service, adequately segregating duties, and preventing the implementation of unauthorized software.

The report endorsed the May 1998 GAO executive guide, "Information Security Management: Learning From Leading Organizations," (GAO/AIMD-98-68), which was based on the best practices of organizations noted for superior security programs. The report recommends agencies proactively manage risks and states that strong Government leadership is important to ensure that executives understand their risks, monitor agency performance, and resolve issues affecting multiple agencies.

Office of the Inspector General, DoD

3. Report No. D-2000-058, "Identification and Authentication Policy," December 20, 1999. The audit reviewed DoD Component policies on using identification and authentication controls to access information systems. The report states that DoD Components' and the Office of the Secretary of Defense policies governing the use of identification and authentication to control access to information systems have significant variations. Nonuniform practices proliferated because the ASD(C^3I) did not issue standard security policy to respond to the changing technology and consolidate existing policies. The outdated information security policies and the lack of guidance that specifically established uniform security requirements hampered DoD efforts to reduce the vulnerability of the information infrastructure.

The report recommended that the ASD(C^3I) provide specific interim policy guidance to establish minimum security requirements covering identification and authentication. It also recommended that ASD(C^3I) accelerate the reissuance of a governing DoD Directive.

The Senior Civilian Official, ASD(C^3I), issued a memorandum on "Year 2000 and the Importance of Adherence to Department of Defense Information Security Policy," May 5, 1999, and asked that all personnel using DoD systems comply with the guidance in AI-26, Chapter 11, particularly Section 5.1.1. The report stressed the need for a uniform set of DoD identification and authentication requirements. Additionally, the Global Information Grid policy memorandum on information assurance was in final coordination, as of February 2, 2000. The Office of the ASD(C^3I) stated that as soon as the document was signed, it would undertake to develop and issue a DoD Directive governing information assurance.

4. Report No. 00-009, "Information Assurance for the Joint Total Asset Visibility System at the U.S. Pacific Command," October 14, 1999. The objective of this audit was to evaluate information assurance for the Joint Total Asset Visibility-In-Theatre system at the Pacific Command and to evaluate the management control program as it applied to the system. The report states that the certification authority did not perform adequate certification and did not follow DITSCAP procedures. Specifically, the certification authority did not perform a thorough system security test and evaluation, did not perform an adequate risk analysis, and did not issue a certification report or

recommendation to the Designated Approving Authority. As a result, the decision to accredit was flawed; risk to the Joint Total Asset Visibility-In-Theatre system, data, and the missions it supports had not been minimized. Also, the Joint Total Asset Visibility Objective system, planned for implementation in January 2000, was subject to the same or greater risk. Additionally, the Pacific Command did not establish a contingency plan as required by DoD Directive 5200.28.

Management partially concurred with the finding. Subsequent to the issuance of the final draft, discussion between management and the audit team led to agreement on the nature of responsive corrective action.

5. Report No. 00-005, "Information Assurance for the Joint Total Asset Visibility System," October 8, 1999. The overall audit objective was to evaluate the adequacy of information assurance for the Joint Total Asset Visibility Program. The report states that information assurance for the Joint Total Asset Visibility Program needed improvement in the areas of qualified computer security experts assigned to the Joint Total Asset Visibility Office, security incorporated into the system's life-cycle management process, risk analysis, and coordination to ensure the minimum security requirements of DoD Directive 5200.28 were implemented. As a result, DoD exposure to unacceptable risks could not be fully assessed and minimized, and the Joint Total Asset Visibility system and data could have been compromised. The report states that at the European Command, passwords did not expire and Joint Total Asset Visibility personnel did not require users to obtain new passwords after 6 months. However, a future release of the Joint Total Asset Visibility software was to include features that require password expiration and allow users to change their passwords. Although the finding and recommendation was addressed in Report No. 00-009, the report states that the Joint Total Asset Visibility Office did not coordinate with the Joint Staff to ensure that the European Command and Pacific Command accreditations were complete and up-to-date. Finally, neither the European Command nor the Pacific Command had a contingency plan for their local area networks where the Joint Total Asset Visibility data was processed, stored, and transmitted or for the buildings that housed the system.

The report recommended that the Director, Defense Logistic Agency direct the Joint Total Asset Visibility Office to:

- augment its security In-Process Reviews and Engineering Reviews to include all key information assurance representatives;
- appoint a Government employee with technical expertise in information assurance to the Joint Total Asset Visibility Office;
- establish information assurance training; and
- implement information assurance using life-cycle management.

The report also recommended that the Deputy Under Secretary of Defense (Logistics); the Director, Joint Staff; and the Director, Defense Logistics Agency, complete information assurance memorandums of agreement with each Joint Total Asset Visibility operational site. The report also recommended that

the Senior Civilian Official, ASD(C^3I), and the Director, Joint Staff, coordinate to establish responsibility to govern and enforce information assurance for DoD automated information systems and networks.

Management comments and actions were responsive to the report recommendations, with the exception of the ASD(C^3I), who nonconcurred with the draft recommendation on memorandums of agreement, and stated that the Defense Logistics Agency should manage the process to identify Joint Total Asset Visibility sites and complete memorandums of agreement. As a result, the recommendation was redirected to the Deputy Under Secretary of Defense (Logistics). The Deputy Under Secretary of Defense (Logistics) recognized that the Defense Logistics Agency and the Joint Staff needed to work together to develop all required memorandums once the Joint Total Asset Visibility System sites had been identified. The comments from the Deputy Under Secretary of Defense (Logistics) were considered responsive.

6. Report No. 99-233, "General Controls for the General Accounting and Finance Systems," August 17, 1999. The General Accounting and Finance System is the primary accounting system used by the Air Force to support its financial statements. The audit objective was to evaluate whether the general and application controls in the General Finance and Accounting System were reliable for data processed through the system and used to prepare Air Force financial statements. Because the General Finance and Accounting System general controls needed improvement, the report did not evaluate the application controls. The report states that general controls were limited and could not provide reasonable assurance that the program and data files were protected from unauthorized access and modification. The report noted that DFAS security over the General Finance and Accounting System had the following limitations.

- DFAS security guidance on the Information System Security Officer (ISSO) was not commensurate with the ISSO functional responsibilities mandated by DoD Directive 5200.28.
- The Denver Center Designated Approving Authority and the General Finance and Accounting System ISSO did not fully execute the DFAS General Finance and Accounting System security program.
- Security Readiness Reviews identified numerous access and system security weaknesses in the operating system software supporting General Finance and Accounting System.
- Limited penetration tests of the communication network used by General Finance and Accounting System showed that the communication network was vulnerable to unauthorized access.

Consequently, general controls could not provide reasonable assurance over the integrity, confidentiality, and availability of data entered in or extracted from the General Finance and Accounting System. Further, financial statement auditors may not be able to rely on General Finance and Accounting System information without substantial verification when reviewing the Air Force financial statements.

The report recommended that the Director, DFAS provide the General Finance and Accounting System ISSO with the authority and training to effectively enforce security policy. Further, the report recommended that the ISSO conduct security reviews in accordance with General Finance and Accounting System security requirements. The report also recommended that the Director, DISA, require penetration testing as part of their annual Security Readiness Reviews at each Defense Megacenter. Management comments were responsive to the recommendations. The DFAS Director, Information Technology, stated changes to DFAS Regulation 8000.1-R were expected to address the ISSO issues expressed in the report. The Chief, Field Security Operations, stated that DISA revised procedures to include separate penetration testing [redacted] DISA: (b) (7)(E) [redacted]

7. Report No. 99-225, "Electronic Data Processing General Controls for the Defense Property Accountability System," July 29, 1999. The Office of the Inspector General, DoD, contracted with KPMG, LLP to review the electronic data processing general controls over the Defense Property Accountability System. The Defense Property Accountability System is the DoD migratory system for all real and personal property. Because the responsibility of the Defense Property Accountability System is divided among three organizations, the audit examined the adequacy of controls at each organization. Identified weaknesses were presented by organization of primary responsibility, which included the Defense Property Accountability System Program Management Office and the DISA Regional Support Activity Dayton. Some of the findings and recommendations contained sensitive information and have been summarized. KPMG, LLP identified 18 reportable conditions in the following areas: DISA: (b) (7)(E) [redacted]. None of the reportable conditions were considered material weaknesses.

The report found that, with the exception of the reported weaknesses, the Defense Property Accountability System was operating effectively enough to provide reasonable assurance that the program and data files were protected from unauthorized access and modification. The report states that reported weaknesses required management attention in order to strengthen the overall control environment.

The report recommended that the Defense Property Accountability System program managers keep security documentation up-to-date and reinforce security awareness for all users. The report also recommended that the Director, DISA Regional Support Activity Dayton:

- establish a site-level security plan;
- implement policies and procedures for security and configuration management;
- develop a proper training program for security personnel;
- review the Defense Property Accountability System World Wide Server for sensitive information;
- correct identified network and system vulnerabilities;

- reassess the responsibilities of the security and database administrators; and

- test the business continuity plan.

Comments from the Defense Property Accountability System Program Management Office were responsive to the recommendations in the report. The DISA Regional Support Activity Dayton concurred, and initiated the recommended corrective actions.

8. Report No 99-215, "Year 2000 Computing Issues: Defense Logistics Agency-Standard Automated Material Management System," July 16, 1999. The Standard Automated Materiel Management System provides support for the management of consumable items for Defense Logistics Agency. The overall audit objective was to evaluate whether Defense Logistics Agency was adequately planning for and managing Y2K risks to avoid undue disruption to its supply mission. The audit also assessed additional areas of the DoD Year 2000 Management Plan, including information assurance. The report states that Defense Logistics Agency had developed programs and procedures to help protect the mainframe, mid-tier, and personal computers data processing systems from improper intrusion or data corruption resulting from an information warfare threat to the Defense information infrastructure and Standard Automated Materiel Management System.

9. Report No. 99-128, "Computer Security for the Defense Civilian Pay System," April 8, 1999. The primary audit objective was to determine whether security software controls over the Defense Civilian Pay System adequately safeguarded the data integrity of employee payroll records. The report states that DFAS and DISA needed to improve computer security over the Defense Civilian Pay System and its mainframe computers. Specifically, the report states that:

- DISA: (b) (7)(E) [redacted]
- DISA: (b) (7)(E) [redacted]
- DISA: (b) (7)(E) [redacted]

The report recommended that DISA perform a DISA: (b) (7)(E) [redacted] computers that support the civilian pay application, implement standard system controls in accordance with agency guidance, designate all positions requiring sensitive access as critical-sensitive, and complete background investigations on all personnel in these positions. The report also recommended that DFAS

require users with access to the pay application to change their passwords every 90 days, review and delete inactive users who no longer need access, modify user authentication, establish procedures for issuing and resetting passwords, and restrict password reset capability.

DFAS concurred with the recommendations, but stated it would permit nonexpiring passwords for agencies that interact with the application only through batch interfaces. DISA Mechanicsburg and the Systems Support Office, Dayton, DISA: (b) (7)(E) on all personnel and designated all sensitive positions as critical sensitive in accordance with DoD Directive 5200.28.

10. Report No. 99-107, "Computer Security for the Defense Civilian Pay System," March 16, 1999. The Defense Civilian Pay System is the migratory civilian pay system for the DoD. The primary objective of this audit was to determine whether security software controls over the Defense Civilian Pay System adequately safeguarded the data integrity of the employee payroll records. The report states that computer security over the Defense Civilian Pay System application needed improvement. Specifically, the report states that:

- The appointed ISSO for the Defense Civilian Pay System application did not have the authority, system access, or training necessary to enforce security policies and safeguards on all personnel with access to the application;
- Security was not uniformly implemented for other key DFAS financial applications; and
- DISA: (b) (7)(E)

Inadequate guidance issued by DFAS resulted in problems with the Defense Civilian Pay System ISSO at DFAS Pensacola and inconsistent security implementation within DFAS. The Dayton Systems Support Office had not reviewed and limited DFAS Financial Systems Activity Pensacola personnel to Defense Civilian Pay System resources when support responsibilities transferred to DISA. The report states that DFAS needed to strengthen security controls to ensure the integrity of the Defense Civilian Pay System and protect Federal information assets.

The report recommended that DFAS appoint qualified personnel as ISSOs and include the functional responsibilities mandated by DoD Directive 5200.28, "Security Requirements for Automated Information Systems," March 21, 1988, in the position description. It also recommended that specific instructions be incorporated in DFAS Regulation 8000.1, "Information Management Policy and Instructional Guidance," August 21, 1996, to ensure that security officers were given adequate training, the proper authority and responsibility, and placement at the highest level within the organization to ensure independence from the operational elements. The report also recommended that the sensitive security administrative authority be restricted to the DISA personnel responsible for computer mainframe maintenance and support.

Management concurred or partially concurred with the recommendations. DFAS defined the responsibilities and qualification standards for ISSOs in their security regulation, incorporated security responsibilities into position descriptions, and required annual security compliance reviews. DFAS agreed to revise DFAS Regulation 8000.1-R to include procedures for establishing a line of authority between the ISSO and each security administrator servicing the ISSO application in the same way that contracting officers establish authority over contracting officer representatives. DFAS agreed to review and restrict all sensitive administrative authority to the civilian pay systems.

Air Force Audit Agency

11. Project No. 99066019, "Information Protection-Implementing Controls Over Known Vulnerabilities in Air Force Materiel Command Computers," March 2, 2000. The report states that the Air Force Materiel Command did not implement all needed countermeasures to publicized vulnerabilities, thereby rendering the networked computers and related devices vulnerable to a variety of attacks. Specifically, the audit identified over 16,000 devices (personal computers, routers, servers, and printers) with open vulnerabilities. The report explained that if the vulnerabilities associated with these devices are exploited, not only the computer under attack but also the entire connected network becomes vulnerable. The report states that three locations using contractors to support base-wide computer operations did not consistently implement Air Force Computer Emergency Response Team advisories.

One of several factors contributing to the vulnerabilities identified was that system administrators were not required to implement Air Force Computer Emergency Response Team advisories issued before June 1998. Additionally, the Air Force Materiel Command Director of Communications and Information did not establish:

- controls to ensure base-level managers loaded the most recent vendor software patches,
- a methodology or a requirement to use available software to detect vulnerabilities, and
- a policy requiring contract statements of work for computer operations support to include specific performance criteria related to securing computers and networks and closing known vulnerabilities.

Additionally, the Air Force Materiel Command assistance programs did not specifically target the use of vulnerability detection tools. The report recommended addressing the causes, and management concurred and took or planned to take action.

12. Project No. 99066013, "Certification and Accreditation of Pacific Air Forces Information Systems," March 1, 2000. The report states that Pacific Air Forces did not properly certify and accredit operational information systems. Although management was aware of certification and accreditation problems at Pacific Air Forces locations, it did not provide solutions. Base

personnel at the six locations reviewed did not properly complete or update certification and accreditation for systems with previously completed development certification packages. Specifically:

- only 1 of 16 certification and accreditation packages reviewed for 3 Air Force standard systems and 2 Pacific Air Forces unique systems was up-to-date and complete;
- base personnel did not properly complete site certification and accreditation packages for 25 of 27 systems reviewed for systems that were developed by Pacific Air Forces or by other organizations and did not have development certification packages; and
- five of six locations performed only limited manual or automated assessments of vulnerabilities.

The report states that the conditions occurred because Pacific Air Forces did not adequately train personnel on certification and accreditation procedures. Also, Pacific Air Forces did not include guidance in the command policy for systems delivered without certification packages, which required automated tools to help identify system vulnerabilities prior to operation. Finally, the Pacific Air Forces did not effectively plan the certification and accreditation process and develop an effective method to track the certification and accreditation status of systems operating in the Pacific Air Forces. In response to the report recommendations, the Director of Communications and Information agreed to:

- issue policy requiring personnel involved in the certification and accreditation process to attend the appropriate training;
- issue policy requiring bases to establish procedures for using automated tools, including Internet Scanner, in developing local systems certification and accreditation packages;
- develop a tracking method, such as an accurate database of systems operating in Pacific Air Forces, to track system certification and accreditation status; and
- in coordination with the bases, establish procedures that tie completion of system certification and accreditation packages to realistic timeframes.

13. Project No. 98054032, "Internal Controls Over Purchases of Goods and Services," February 23, 2000. The report states that the Assistant Secretary of the Air Force, Financial Management and Comptroller, and DFAS officials improved payment system access controls during the audit. Specifically, the officials reduced the number of expired or unauthorized access codes allowing system entry; individuals with concurrent write access to the Integrated Accounts Payable System and Integrated Paying and Collecting System; and certifying officers with system write access. However, the paying offices needed to further reduce payment system access. Specifically, access codes of transferring personnel not traceable to specific individuals were making data vulnerable to improper disclosure, modification, or destruction.

The report recommended that DFAS Denver coordinate with the Assistant Secretary of the Air Force, Financial Management and Comptroller, to implement a feedback process for the DFAS systems offices and supervisors at DFAS paying offices and the financial service offices to ensure that transferred personnel are removed from system access. The report suggested that supervisors at DFAS paying offices and financial service offices initiate at least a biweekly follow-up on transferred personnel and recommended that the Assistant Secretary of the Air Force, Financial Management and Comptroller, instruct financial service office supervisors on procedures to delete access codes for transferred personnel and monitor system access. Management concurred with the report recommendations.

14. Project No. 98066024, "Certification of Standard Systems," September 30, 1999. Standard systems are information systems operating at multiple locations and must be certified to meet information protection requirements. The objective of this audit was to determine whether Air Force management properly certified standard systems during development or reengineering. The audit reviewed six systems at the Standard Systems Group and the Electronic Systems Center, two primary development activities for standard information systems. The report states that management had established an adequate certification process, controlled implementation of the process, and properly certified all six newly developed and re-engineered systems. The report contained no recommendations.

15. Project No. 99066015, "Followup Audit, Information Protection-Implementing Controls Over Known Vulnerabilities in Air Combat Command Computers," September 29, 1999. This was a follow-up review to determine whether Air Combat Command network managers effectively implemented management controls to correct known vulnerabilities and monitored countermeasure implementation. The report states that Air Combat Command network managers did not have adequate management controls for assessing and correcting known vulnerabilities. Management controls were lacking because Air Combat Command personnel failed to coordinate on-line surveys of network systems, track and implement countermeasures as required, and verify that Air Combat Command units implemented countermeasures. As a result, the risk of unauthorized users comprising Air Combat Command networks and computer systems was increased.

The report recommended that Air Combat Command Director of Communications and Information should implement management controls, oversight procedures, and processes to identify and correct known vulnerabilities in networked computers. The report also recommended the Director of Communications and Information advise commanders at all levels to ensure system administrators receive Air Force Computer Emergency Response Team advisories and implement required countermeasures. Management implemented the management controls recommended in the report. The Director of Communications and Information also advised commanders to ensure that system administrators receive Air Force Computer Emergency Response Team advisories and implement the required countermeasures.

16. Project No. 99066005, "Information Protection-Implementing Controls Over Known Vulnerabilities in Air Mobility Command Computers," September 27, 1999. The overall audit objective of this report was to determine whether Air Mobility Command network managers implemented countermeasures to known vulnerabilities in networked computers. The report concluded the following.

- The Air Mobility Command network managers did not implement countermeasures to well-publicized vulnerabilities, thereby rendering the networked computers vulnerable to a variety of attacks.

- Network managers and end users did not effectively protect Air Mobility Command computer systems from malicious computer virus software. As a result, a substantial number of Air Mobility Command's Windows computers were vulnerable to malicious software infection.

- None of the four Air Mobility Command locations using Dynamic Host Configuration Protocol software could use the software to identify the hardware associated with a specific Internet protocol address. As a result, system administrators could not trace vulnerabilities to individual computers or determine which computers may have been involved in illegal operations or subjected to hacker activity.

To improve network security within the Air Mobility Command, the report recommended that the Air Mobility Command Director of Communications and Information ensure that computer users run anti-virus software, update the anti-virus signature files, and improve guidance for using the Dynamic Host Configuration protocol to assign and track Internet protocol addresses. Management officials agreed with the audit results and completed actions were responsive to the issues and recommendations in the report.

17. Project No. 98054015, "Controls Within the Automated Computation Travel System," June 14, 1999. The Air Force Reserve Command designed the Automated Computation Travel System to accomplish the procedures associated with payment processing. The overall objective of the audit was to determine whether the Automated Computation Travel System included adequate general and application controls to meet the financial system control requirements. The GAO and the Joint Financial Management Improvement Program set standards for Federal financial systems.

The report states the Automated Computation Travel System adequately met 7 of 12 general and application control categories. However, the Air Force Reserve Command did not establish effective general control requirements within the Automated Computation Travel System for accreditation, separation of duties, and access control. Effective controls are necessary to minimize system risks. Further, Air Force Reserve Command officials had not completed system certification, prepared contingency plans, or completed a risk analysis. Also, the Air Force Reserve Command did not establish application control requirements within the Automated Computation Travel System for transaction controls and accounting conformance. The Air Force Reserve Command did not ensure that local travel pay unit commanders established contingency plans

for the continuation of operations in the event of an emergency or ensure that local commanders accomplished all required risk analysis. During the audit, the Air Force hired a contractor to prepare a system life-cycle contingency plan. The contractor also issued a threat/vulnerability assessment and risk analysis report.

The report recommended that the Air Force Reserve Command establish procedures addressing physical access control requirements and ensure that local commanders establish adequate physical access controls over the Automated Computation Travel System. It also recommended that the Air Force Reserve Command establish system edits to prevent or detect potential duplicate travel dates and claims. Management agreed with overall audit results, and took or planned actions responsive to the issues and recommendations.

18. Project No. 98054007, "Personnel Data System-Military Financial Controls," May 14, 1999. The report states that the Personnel Data System-Military met 8 of 12 general and application system control requirements. However, the Air Force Personnel Center did not adequately fulfill general control requirements associated with the Personnel Data System-Military for accreditation, Information Processing Management System reporting, and access controls. As a result, the Air Force Personnel Center could not minimize system risks relating to emergency situations and protect data against fraud and unauthorized access. The report also states that the Air Force Personnel Center needed to improve its controls for audit trails.

Additionally, the report recommended that the Air Force Personnel Center Commander:

- assume or delegate Designated Approving Authority duties and establish interim accreditation for the system;
- establish an alternative processing site for Air Force Personnel Center operations, request DISA to provide documentation and procedures for system recovery, and develop a disaster recovery plan;
- direct the equipment custodian for Personnel Data System-Military to remove invalid codes and equipment from the Information Processing Management System and update it to include accreditation control numbers;
- direct Military Personnel Flight to periodically review user identifications for need and duplication, and issue unique identifications and passwords for individuals with a proven valid need;
- ensure that personnel system managers periodically review user identifications for validity of need and duplication; and

- modify the Personnel Data System-Military transaction histories to include the name of the preparer and allow system edits to reject transactions without a source document reference.

Management took or planned actions responsive to the recommendation contained in the report.

19. Project No. 98066014, "Information Protection-Implementing Controls Over Known Vulnerabilities in United States Air Forces in Europe Computers," March 26, 1999. The report states that U. S. Air Forces in Europe managers did not implement adequate countermeasures for the vulnerabilities identified in Air Force Computer Emergency Response Team advisories and on-line surveys. Initially, the vulnerabilities were not corrected because the Director of Communications and Information failed to inform managers of the need to implement appropriate countermeasures. When the managers were told to implement countermeasures to the vulnerabilities, the controls were still not entirely effective, mainly because of the lack of effective feedback procedures and the lack of sufficient training for system administrators. As a result, the risk of attack and the subsequent compromise or destruction of stored information was increased. The report recommended that the United States Air Forces in Europe Director of Communications and Information should:

- change the checklists that inspectors use to include steps for verifying that computer vulnerabilities have been closed,

- formally certify that system administrators have been trained to operate their computer system and that they understand the application of U.S. Air Forces in Europe information protection policy to their system as a prerequisite to performing network administration duties,

- develop formal agreements with the Designated Approving Authority of computers connected to base area networks that establish security criteria for remaining systems connected to the United States Air Forces in Europe networks, and

- identify needs to segregate advisories by computer platform and identify discrete tasks to close vulnerabilities.

Management officials agreed with the audit results and took or planned actions that were responsive to the issues and recommendations.

20. Project No. 98066018, "Information Protection-Implementing Controls Over Known Vulnerabilities in Air Education and Training Command Computers," March 8, 1999. The audit determined whether Air Education and Training Command network managers implemented countermeasures to known computer vulnerabilities. The report states that the Air Education and Training Command countermeasure implementation for known vulnerabilities required more management attention. Network managers at six of the seven bases reviewed did not correct the known vulnerabilities identified in Air Force Computer Emergency Response Team advisories and Air Education and

Training Command on-line survey reports. The conditions had multiple causes, including the following:

- servers were not centrally located at the network control center,
- Air Education and Training Command personnel did not perform a follow-up on-line survey to ensure that vulnerabilities were corrected, and
- a tracking system was not established to ensure that all system administrators implemented countermeasures.

These vulnerabilities increased the risk that unauthorized users could compromise Air Education and Training Command computer systems. The report recommended that headquarters Air Education and Training Command, Director of Communications and Intelligence should:

- determine the cost-effectiveness of centralizing control of base servers and request funding if cost-effective,
- require personnel to identify network connections and the owner of those connections and to develop a complete database of systems connected to the base network,
- establish a tracking system to ensure the implementation of known countermeasures,
- establish a policy involving unit and tenant commanders when system administrators do not report compliance with Air Force Computer Emergency Response Team advisories,
- request Air Force Computer Emergency Response Team identify the vulnerable operating software or hardware in each advisory, and modify the advisories to provide discrete, traceable action items with instructions,
- require the system administrator to complete proper training prior to receiving a system administrator account and password on the network system,
- provide the on-line survey report to the wing commander for action, and
- perform a followup, on-line survey within 120 days to ensure that previously identified vulnerabilities are corrected.

Management actions planned or taken were responsive to the issues and recommendations in this report.

21. Project No. 97066031, "Information Protection-Security Awareness, Training, and Education," January 29, 1999. The Security Awareness, Training, and Education Program covers communications security, computer security, and computer signal emissions security disciplines. The purpose of this audit was to determine the effectiveness of the base-level Security Awareness, Training, and Education Program. The report states that managers had not established effective procedures to implement security awareness, training, and education policies and procedures. Specifically, managers had not appointed and trained unit security awareness, training, and education managers, prepared or supported security awareness, training, and education utilization reports, or performed staff assistance visits. These conditions occurred because the major commands and field operating agencies had not provided adequate management oversight for base Security Awareness, Training, and Education programs. As a result, the risk of systems intrusions and compromise of sensitive information was increased.

The report recommended that the Air Force Safety Center revise the Information Protection Assessment and Assistance Program and the Air Force Communications Form 13, Information Protection Criteria. The Air Force Safety Center complied and made the recommended revisions.

Appendix C. FY 1998 DoD Information Assurance Initiatives

The FY 1998 DoD CIO Annual Information Assurance Report, May 1999, outlined 11 major DoD information assurance initiatives and other DoD activities to address the persistent problem of securing DoD information systems. The following summarizes the 11 initiatives.

Defense-wide Information Assurance Program Implementation. The DIAP was created to provide for the planning, coordination, integration, and oversight of DoD information assurance activities and resources. The DIAP resides within the Infrastructure and Information Assurance Directorate of the ASD(C^3I) and is staffed with personnel from the Defense agencies, the active and reserve forces, and the intelligence community.

Intelligence Community Cooperation. The Implementation of the DIAP presented an opportunity to initiate a similar cooperative effort in the intelligence community to ensure consistency of effort and emphasis. An intelligence community coordinator position was established in the DIAP to facilitate a close working relationship.

Defense In-Depth Strategy. The Defense In-Depth Strategy recognizes the diversity of technologies, solutions, adversaries, and vulnerabilities that pervade DoD information systems and infrastructures. The Defense information infrastructure encompasses local area networks, hosts (servers and clients), applications, and data, as well as underlying wide-area transport capabilities that interconnect the resources. The Defense In-Depth Strategy recognizes that no single element or component of security can provide adequate assurance and invokes the use of layered security solutions.

Implementation of the Defense In-Depth Strategy construct involves directing DoD information assurance initiatives at several critical focus areas. Further, implementation of Defense In-Depth Strategy must also recognize that in a shared-resource environment, any single system or network cannot be adequately protected unless all interconnected systems and networks are protected adequately.

National Security Incident Response Center. The National Security Incident Response Center is the National Security Agency's computer incident response capability in support of the national computer network defense needs. The National Security Incident Response Center provides timely warning of threats against U.S. information systems and expert assistance to U.S. Government organizations in isolating, containing, and eliminating incidents that threaten national security systems.

Joint Task Force-Computer Network Defense. The Secretary of Defense established the Joint Task Force-Computer Network Defense as the focal point for coordinating the defense of DoD computer networks. It monitors incidents and potential threats, and coordinates across the DoD to formulate and direct

actions to stop or contain damage and restore network functionality. Computer network defense employs the information assurance organization, procedures, tools and trained workforce to defend DoD computer networks.

Public Key Infrastructure. Public key infrastructure refers to the framework and services that provide for the generation, production, distribution, control, and accounting of public key certificates. Public key infrastructure is just one part of the Defense In-Depth Strategy, but it is important to enabling end-to-end protection in the DoD networked environment. The DoD public key infrastructure must:

- avoid the significant duplication of effort and costs that are incurred by unique and noninteroperable systems;
- enable the outsourcing of appropriate public key infrastructure activities and functions to achieve economies of scale;
- satisfy major program and operational requirements;
- support the recovery of encryption keys as it traverses the network and while at rest; and
- comply with and support applicable DoD policies.

To accomplish these objectives, the Senior Civilian Official, OASD(C^3I), signed a memorandum to DoD, which directed the development of the following three key documents: DoD X.509 Certificate Policy, DoD Certification Practice Statement, and the DoD Public Key Infrastructure Roadmap.

Web Security Initiative. By authorizing the establishment of web sites, Component heads assume a management responsibility that extends into the realm of operational security and force protection. Component heads are responsible for enforcing the application of risk management procedures to ensure that the considerable mission benefits gained by using the Web are carefully balanced against the potential security and privacy risk created by having aggregated DoD information more readily accessible to a world-wide audience. In September 1998, the Deputy Secretary of Defense directed steps to mitigate the vulnerabilities of the Web within DoD. The steps included:

- establishing a task force under ASD(C^3I) to develop policy and procedural guidance to address the operational, public affairs, acquisition, technology, privacy, legal, and security issues associated with use of the DoD web sites;
- conducting comprehensive, multi-disciplinary security assessments of DoD web sites and establishing an annual requirement for continuance of such assessments; and
- accelerating the development and implementation of an architecture to enhance the protection of sensitive, unclassified information.

The task force directed additional actions including a review of DoD ability to safeguard sensitive, unclassified information in its electronic commerce systems and inclusion of web site administration policy and procedures in the formal DoD publication system.

Training and Certification. The DoD had begun to actively address the issues surrounding the technical proficiency, career development, and retention of its military and civilian employees engaged in information assurance and information technology activities. However, many individuals using DoD computer systems or performing the duties of system administrators and maintainers lacked a sufficient level of training to ensure the adequate protection of DoD information resources. Because adequate levels of information assurance skills directly relate to operational readiness and mission accomplishment, effort was underway to address overall information assurance training and professional needs.

Red Team Methodology. Several Components conducted or sponsored a number of "Red Team" assessments of their operational readiness to protect against, detect, and react to potential adversarial information operations. The DoD, in gauging the information assurance component of unit and force operational readiness, intends to conduct additional periodic assessments of the information assurance processes, systems, and organizations.

Information Assurance Vulnerability Alert (IAVA) Process. The results of both real world incidents and exercises point out the lack of timely notification to system administrators of identified vulnerabilities and the procedures to correct these vulnerabilities. To address this problem, the DoD developed the IAVA process to provide positive control of the vulnerability notification and corrective action process within the DoD. The DISA is the designated agency for execution of the process and has a standing requirement to disseminate vulnerability information to combatant commands and Service/Agency points of contact (the IAVA Process is further described in the Background section of the report).

Critical Infrastructure Protection. On May 22, 1998, Presidential Decision Directive (PDD) 63, Critical Infrastructure Protection, was issued in response to the findings and recommendations of the President's Commission on Critical Infrastructure Protection. The Directive called for each Federal department or agency to develop, by November 18, 1998, a plan to protect its portion of the Federal Government's critical infrastructure and to implement its plan within 2 years (critical infrastructure protection is further described in the Background section of the report).

Appendix D. FY 1999 Information Assurance Initiatives

The FY 1999 DoD CIO Annual Information Assurance Report, February 2000, reported on 12 major DoD-wide initiatives and activities at 15 Components, as well as activities at the unified and specified commands and 3 special-interest communities. Further, several issues addressed in the 1998 report are not reported in a separate section but are included in the report of the component with primary responsibility. The following summarizes the 12 initiatives.

Public Key Infrastructure. Public key infrastructure is introduced in the FY 1998 DoD CIO Annual Information Assurance Report. The DoD is taking major steps to reform its paper-based processes by transitioning to an environment of electronic information interchange. The DoD public key infrastructure enables the information assurance security services of data integrity, user-identification and authentication, user nonrepudiation, and data confidentiality for electronic information interchange.

The Public Key Infrastructure Implementation Plan for DoD, the DoD Public Key Infrastructure Roadmap, the DoD X.509 Certification Policy, and the DoD Certification Practice Statement are the guiding documents for establishing the enterprise-wide end state for the DoD public key infrastructure.

Information Assurance Research Activities. The Information Security Research Council coordinates, collaborates, and influences information assurance research within DoD as well as non-DoD Federal agencies. The Council has conducted various activities including the sponsoring of "hot topics" in information assurance research to educate Senior DoD leadership on the status of the information assurance research and/or hard problems and their potential solutions.

Information Assurance Training and Certification. The Information Assurance and Information Technology Human Resources Integrated Process Team Report presents 19 distinct recommendations to improve the way in which the DoD manages its IT workforce. The most significant finding was that information assurance and information technology management personnel readiness is more problematic than simply providing training opportunities and financial and career incentives to IT professionals. Before these strategies can be implemented, the DoD must learn the demographics of its IT population and know precisely what IT activities it is performing.

The Integrated Process Team recommended changes to the way the DoD manages its IT workforce, including recognizing specific information assurance functions that reflect current duties of the information age. In addition, the Integrated Process Team recommended coding the IT billets and all people who perform IT functions in a DoD personnel database to track career progression trends and training credits accurately. The Integrated Process Team suggested also linking standardized training and certification requirements to the coded billets and people so that no one with privileged access to information infrastructures is overlooked when preparing and sustaining critical IT education.

The FY 1999 DoD CIO Annual Information Assurance Report stated that a briefing to the Deputy Secretary of Defense was to be scheduled in early 2000, with approval to implement the many recommendations expected at that time. A detailed execution plan would be developed and monitored by the DIAP.

DoD Computer Forensics Laboratory. The DoD facility, which opened on September 24, 1999, processes computer evidence in criminal, fraud, and counterintelligence investigations for all of the Defense Criminal and Counterintelligence Investigative organizations.

Insider Threat Integrated Process Team. The ASD(C^3I) established the Insider Threat Integrated Process Team to foster the effective development of interdependent technical and procedural safeguards to reduce malicious behavior by insiders. The objective of the Integrated Process Team is to minimize the impact of the insider threat and to minimize the potential damage inflicted on DoD information and information systems. The annual report states that there are four basic sources of insider security problems:

- Maliciousness that results in compromise or destruction of information, or disruption of services to other insiders;
- Disdain of security practices that results in compromise or destruction of information or disruption of services to other trusted operations;
- Carelessness in using an information system and/or protection of DoD information; and
- Ignorance of security policy, security practices, and information system use.

Computer Network Defense Working Group. The ASD(C^3I), in coordination with the Commanders in Chief, military Services, and Defense agencies, formed a Computer Network Defense Working Group. The Working Group conducted a comprehensive study to:

- identify the core computer network Defense functions;
- recommend an integrated, Defense-wide, enterprise computer network defense policy and assign responsibilities; and
- develop a programmatic structure for computer network defense to support preparation and review of the FY02-07 Program Objective Memoranda.

The Working Group identified the core functions of computer network defense; developed a computer network defense framework; produced a draft DoD Directive for computer network defense; and produced Program Objective Memoranda preparation instructions for the FY02-07 Planning, Programming, and Budgeting System cycle.

Information Assurance Vulnerability Alert (IAVA). The IAVA process was introduced in the FY 1998 DoD CIO Annual Information Assurance Report. A DoD Instruction formalizing the full information assurance vulnerability reporting and mitigation program is in development. In 1999, DISA established a system for distributing vulnerability information to all DoD elements, issuing in the process 10 IAVAs, 3 Information Assurance Bulletins, and 19 technical advisories. The DISA also developed a database to immediately distribute vulnerability information to each system administrator and to track and report on response to the alerts.

Reserve Components Study. The Office of the Assistant Secretary of Defense for Reserve Affairs, Research, Training and Manpower chartered a study to look at Reserve Component participation in information assurance activities. The principal purpose of the study was to identify opportunities for the Reserve Component of the United States military to perform information assurance missions in support of requirements assigned to DoD. The DoD Critical Infrastructure Protection Plan occupied a central role in this study, establishing the structural scope and providing a technical framework within which information assurance functions could be defined.

Global Information Grid Information Assurance Guidance and Policy Memorandum. The Global Information Grid covers all the major aspects of IT including computing, communications and networks, interoperability, technology, and resources, as well as information assurance. The proposed Global Information Grid Information Assurance Guidance and Policy Memorandum addresses not only the confidentiality of DoD information, but also its availability, integrity, and the need for strong identification and nonrepudiation services. All Global Information Grid policies are to be issued first as DoD CIO guidance and policy memorandums, and then as formal DoD directives and instructions.

Web Security Initiative. The Web Security Initiative was introduced in the FY 1998 DoD CIO Annual Information Assurance Report. The World Wide Web can provide DoD adversaries with a potent instrument to obtain, correlate, and evaluate an unprecedented volume of aggregated information on DoD capabilities, infrastructure, personnel, and operational procedures. Such information, especially when combined with information from other sources, increases the vulnerability of DoD systems and may endanger DoD personnel and their families.

On December 7, 1998, the "Website Administration Policies and Procedures," were issued. Those policies and procedures were being staffed for inclusion in the formal DoD publication system as a DoD Directive and Manual. To mitigate the vulnerabilities of the World Wide Web, the policy:

- requires all unclassified information to be reviewed prior to being placed on DoD websites;
- provides guidance on the types of information that should not be posted on publicly accessible websites;

- identifies processes for determining vulnerabilities and provides guidance on the protection afforded by various types of security and access controls; and

- directs comprehensive, multi-disciplinary security assessments of DoD websites to be conducted and established as an annual requirement for continuance of such assessments.

To provide the ongoing operations security and threat assessments of publicly accessible component websites, the Deputy Secretary of Defense approved the concept of operations for the Joint Website Risk Assessment Cell, which began operation on March 1, 1999. During its first 6 months of operation, the Joint Website Risk Assessment Cell identified nearly 800 instances of potential policy violations, which were forwarded to the appropriate offices for correction.

Defense-Information Assurance Red Team Methodology. Red team methodology was introduced in the FY 1998 DoD CIO Annual Information Assurance Report. The DIAP requires an effective process for routinely assessing the operational readiness of DoD information systems and networks. Those independent assessments, known as red team activities, provide an impartial perspective on the vulnerabilities that could be exploited by an adversary.

In an attempt to introduce standardization to the information assurance red team process, the ASD(C^3I) developed an information assurance red team methodology through a collaborative effort involving many of the red team organizations within the information assurance community. The Defense-Information Assurance Red Team Methodology focuses on DoD requirements and is supplemented by the Information Assurance Red Team Handbook. Both provide a methodology for designing, developing, assembling, and conducting red team activities.

Information Assurance Architectural Overlay. The DoD has significant concerns at the enterprise level regarding attaining sufficient protection for its myriad of Commander in Chief, Service, and Agency or DoD Component information systems. At the enterprise level, those systems become a "system of systems," with fixed and dynamic information connections interlaced among the DoD Components to form a highly complex web of information exchanges. The ASD(C^3I) convened a quick-reaction information assurance architectural working group to assemble a recommended course of action and a detailed plan of execution to:

- Develop preliminary information assurance architectural concepts for all standard views;

- Use a communications and communication information architecture Joint Task Force-Noncombatant Evacuation Operation Scenario on which to build information assurance products; and

- Provide minimal, preferred, and unconstrained recommendations, with staff and resource estimates, to include preliminary architectural concepts, examples, and guidance.

Appendix E. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Director, Infrastructure and Information Assurance
Director, Defense Logistics Studies Information Exchange

Joint Staff

Director, Joint Staff
  Director, Operations
  Director, Command, Control, Communications, and Computers

Department of the Army

Chief Information Officer
Auditor General, Department of the Army

Department of the Navy

Chief Information Officer
Naval Inspector General
Auditor General, Department of the Navy
Superintendent, Naval Postgraduate School

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Chief Information Officer
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency
Defense Systems Management College

Non-Defense Federal Organizations

Office of Management and Budget
  Office of the Information and Regulatory Affairs
  National Security Division
General Accounting Office
  National Security and International Affairs Division
    Technical Information Center

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Committee on Science