

Audit

Report



DOD COMPLIANCE WITH THE INFORMATION
ASSURANCE VULNERABILITY ALERT POLICY

Report No. D-2001-013

December 1, 2000

Office of the Inspector General
Department of Defense

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

DTIC QUALITY INSPECTED &

20001211 030

AQI01-03-0496

Additional Copies

To obtain additional copies of this audit report, visit the Inspector General, DoD, Home Page at www.dodig.osd.mil or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2885

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ASD(C ³ I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
C/S/A	Commanders in Chief, Services, and Defense agencies
CERT	Computer Emergency Response Team
DISA	Defense Information Systems Agency
IAVA	Information Assurance Vulnerability Alert
OSD	Office of the Secretary of Defense



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

December 1, 2000

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND,
CONTROL, COMMUNICATIONS, AND
INTELLIGENCE)
ASSISTANT SECRETARY OF THE AIR FORCE
(FINANCIAL MANAGEMENT AND COMPTROLLER)
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Audit Report on DoD Compliance With the Information Assurance
Vulnerability Alert Policy (Report No. D-2001-013)

We are providing this report for review and comment. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. As a result of management comments, we revised Recommendation 1.b. so that the Information Assurance Vulnerability Alert implementation plan will address training. We also added Recommendation 1.c. to the Assistant Secretary relating to finalizing issuance of an internal Office of the Secretary of Defense instruction on the Information Assurance Vulnerability Alert process. The Army and Air Force did not provide comments on draft Recommendation 3., renumbered Recommendation 2. in this final report. Therefore, we request that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) provide comments on Recommendations 1.b. and 1.c. and that the Army and Air Force provide comments on Recommendation 2. by January 30, 2001.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Mr. Robert K. West at (703) 604-8983 (DSN 664-8983) (rwest@dodig.osd.mil) or Ms. Eleanor A. Wills at (703) 604-8987 (DSN 664-8987) (ewills@dodig.osd.mil). See Appendix F for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2001-013

December 1, 2000

(Project No. D2000AS-0086.003)
(formerly Project No. OAS-6104.03)

DoD Compliance With the Information Assurance Vulnerability Alert Policy

Executive Summary

Introduction. The Deputy Secretary of Defense issued an Information Assurance Vulnerability Alert (IAVA) policy memorandum on December 30, 1999. Recent events demonstrated that widely known vulnerabilities exist throughout DoD networks, with the potential to severely degrade mission performance. The policy memorandum instructs the Defense Information Systems Agency to develop and maintain an IAVA database system that would ensure a positive control mechanism for system administrators to receive, acknowledge, and comply with system vulnerability alert notifications. The IAVA policy requires the Commanders in Chief, Services, and Defense agencies to register and report their acknowledgement of and compliance with the IAVA database. According to the policy memorandum, the compliance data to be reported should include the number of assets affected, the number of assets in compliance, and the number of assets with waivers. The policy memorandum provided for a compliance review by the Inspector General, DoD.

Objectives. The audit objective was to evaluate the progress that DoD made in complying with the Deputy Secretary of Defense policy memorandum on IAVA.

Results. As of August 2000, DoD progress in complying with the Deputy Secretary of Defense IAVA policy memorandum had not been consistent. At that time, all 9 Commanders in Chief, 4 Services, and 14 Defense agencies had registered as reporting entities with the IAVA database, but 4 other DoD Components had not. Also, information contained in the database for the alerts posted in 2000 showed that of the Components that had registered, only four Commanders in Chief, one Service, four Defense Agencies, and two other DoD Components had reported compliance in accordance with the IAVA policy. As of November 2000, however, DoD had made significant progress in IAVA implementation. The four DoD Components that had not registered were reporting through the Office of the Secretary of Defense point of contact and are no longer required to register separately. All Commanders in Chief, 2 of the 4 Services, and 13 of the 14 Defense agencies were now reporting in compliance with IAVA policy. The Defense Security Service, the one remaining Defense agency that had not fully complied with the reporting requirements, was working to put an infrastructure in place for reporting in accordance with the policy. Of the other DoD components, the Office of the Secretary of Defense was not yet reporting compliance in accordance with IAVA policy; however, it planned to be fully compliant by April 2001. Compliance by the Office of the Secretary of Defense is critical because 20 other DoD organizations will be reporting through it. Effective implementation of IAVA policy will help ensure that DoD Components take appropriate mitigating actions against vulnerabilities to avoid serious compromises to DoD computer system assets that would potentially degrade mission performance.

Summary of Recommendations. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) revise and expedite the release of the DoD IAVA Instruction, develop a DoD IAVA implementation plan, and finalize and approve the internal instruction for the Office of the Secretary of Defense that outlines the roles and reporting responsibilities of DoD organizations that will report IAVA compliance through the Office of the Secretary of Defense point of contact.

We recommend that the Secretaries of the Army and Air Force; the Commandant of the Marine Corps; the Commanders of the U.S. European Command, U.S. Southern Command, U.S. Special Operations Command, U.S. Transportation Command, and U.S. Strategic Command; the Directors of the Ballistic Missile Defense Organization, Defense Advanced Research Projects Agency, Defense Commissary Agency, Defense Contract Audit Agency, Defense Finance and Accounting Service, Defense Intelligence Agency, Defense Prisoner of War/Missing Personnel Office, Defense Security Service, Defense Threat Reduction Agency, Joint Staff, National Imagery and Mapping Agency, and National Reconnaissance Office report compliance by stating the number of assets affected, the number of assets in compliance, and the number of assets with waivers, as stated in the Deputy Secretary of Defense policy memorandum.

Management Comments. The Director, Information and Infrastructure, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), concurred with the recommendation on developing the DoD IAVA instruction and concurred that details about IAVA implementation needed to be addressed. However, the Director stated that an implementation plan was not required because the DoD Instruction on Information Assurance Vulnerability Reporting and Mitigation would address those details. The Deputy Director, Defense Network Operations, Office of the Assistant Secretary, provided comments that addressed the IAVA internal process of the Office of the Secretary of Defense. The management comments concurred with the recommendation to report compliance in accordance with the Deputy Secretary of Defense policy memorandum. However, the Army and Air Force did not comment on the recommendation and, as of November 6, 2000, they were still not reporting in accordance with policy. A discussion of management comments is in the Finding section of the report and the complete text is in the Management Comments section.

Audit Response. The comments that we received were fully responsive. As a result of comments from the Joint Staff, we revised the recommendation on developing and disseminating an implementation plan for IAVA to include training in addition to registration, reporting, and compliance guidance. Also, based on the Deputy Director, Defense Network Operations' comments, we added a recommendation that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) finalize the internal instruction for the Office of the Secretary of Defense relating to the IAVA process. Therefore, in response to the final report, we ask that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) comment on the recommendations by January 30, 2001. Also, the Army and Air Force did not comment on the draft report; therefore, we request that they provide comments on the final report by January 30, 2001.

Table of Contents

Executive Summary	i
--------------------------	---

Introduction

Background	1
Objectives	2

Finding

DoD Compliance with the Information Assurance Vulnerability Alert Policy	3
--	---

Appendixes

A. Audit Process	
Scope and Methodology	13
Prior Coverage	14
B. Commanders in Chief, Services, Defense Agencies, and other DoD Components Required to be Registered Users	15
C. Acknowledgement of the Information Assurance Vulnerability Alerts Issued in 2000	18
D. Compliance With the Information Assurance Vulnerability Alerts Issued in 2000	20
E. Information Assurance Vulnerability Alert Process	22
F. Report Distribution	23

Management Comments

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)	
Director, Infrastructure and Information Assurance	27
Deputy Director, Defense Network Operations	31
U.S. Southern Command	35
Defense Advanced Research Projects Agency	36
Defense Commissary Agency	38
Defense Contract Audit Agency	40
Defense Finance and Accounting Service	41
Defense Security Service	43
Defense Threat Reduction Agency	45
Joint Staff	46
Department of Defense Education Activity	48
Washington Headquarters Services	50

Background

Information assurance is an essential element of operational readiness and is based on the need for accurate and timely exchange of information. With the advances in information technology, new vulnerabilities to the critical infrastructure are evolving. On February 15, 1998, the Deputy Secretary of Defense issued a classified memorandum, "Information Assurance," which instructed the Defense Information Systems Agency (DISA), with the assistance of the Military Departments, to develop an alert system that ensured positive control of information assurance. According to the memorandum, the alert system should:

- identify a system administrator to be the point of contact for each relevant network system,
- send alert notifications to each point of contact,
- require confirmation by each point of contact acknowledging receipt of each alert notification,
- establish a date for the corrective action to be implemented, and
- enable DISA to confirm whether the correction has been implemented.

In another memorandum, February 19, 1998, the Deputy Secretary of Defense directed DoD Components to develop an action plan to detect cyber intrusion. Each Component's action plan should include a process for correcting existing vulnerabilities and for providing formal training and certification of the network operators, system administrators, and information system security officers. The action plan should also include a process for conducting periodic analysis and assessing information assurance vulnerabilities.

Information Assurance Vulnerability Alert Policy Memorandum. On December 30, 1999, the Deputy Secretary of Defense issued an Information Assurance Vulnerability Alert (IAVA) policy memorandum requiring all the Commanders in Chief (CINC), the Services, and Defense agencies (C/S/A) to register and comply with the IAVA process. The IAVA policy establishes the roles and responsibilities for the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD[C³I]) and the Defense Components. The policy memorandum tasked the ASD(C³I) with the responsibility to implement the IAVA process.

The policy memorandum tasked DISA with the responsibility to manage the IAVA process and distribute the alerts to the C/S/As. Each C/S/A will designate a primary and secondary point of contact responsible for acknowledging receipt of the IAVA notifications and for reporting compliance. Each C/S/A is also responsible for disseminating the notifications to all personnel who can implement and manage the technical responses to the IAVAs.

In addition, according to the policy memorandum, a DoD Instruction will be developed to formalize the IAVA process. Meanwhile, the memorandum provided for a compliance review by the Inspector General, DoD.

The 1999 DoD Chief Information Officer Annual Information Assurance Report. The report, which was issued to Congress in February 2000, stated that DISA had an operational system that disseminates vulnerability alerts and tracks DoD Component compliance with the alerts. The report also stated that a DoD Instruction was being developed to formalize the notification process.

Objective

Our audit objective was to evaluate the progress that DoD made in complying with the Deputy Secretary of Defense policy memorandum on IAVA. See Appendix A for a discussion of the audit scope and methodology.

Information Assurance Vulnerability Alert Policy

In August 2000, when we issued the draft audit report, DoD progress in complying with the Deputy Secretary of Defense policy memorandum had not been consistent. At that time, all 9 CINCs, 4 Services, and 14 Defense agencies had registered as reporting entities with the IAVA database, but 4 other DoD Components had not. Also, information contained in the IAVA database for the alerts posted in 2000, showed that of those Components that had registered, only four CINCs, one Service, four Defense agencies, and two other DoD Components had reported compliance in accordance with the IAVA policy. Adequate implementation and compliance with the Deputy Secretary of Defense policy memorandum, dated December 30, 1999, was lacking because the ASD (C³I) had not:

- finalized a DoD Instruction to formalize the IAVA process, and
- developed a DoD implementation plan to require the CINCs, Services, and Defense agencies to register, report, and comply with IAVA notifications.

As of November 2000, DoD had made significant progress in IAVA implementation. The four DoD Components that had not registered were reporting through the Office of the Secretary of Defense (OSD) point of contact and are no longer required to register separately. All CINCs, 2 of the 4 Services, and 13 of the 14 Defense agencies were now reporting in compliance with IAVA policy. The Defense Security Service, the one remaining Defense agency that had not fully complied with the reporting requirements, was working to put an infrastructure in place for reporting in accordance with the policy. Of the other DoD Components, OSD was not yet reporting compliance in accordance with IAVA policy; however, OSD planned to be fully compliant by April 2001. Compliance by OSD is critical because 20 other DoD organizations will be reporting through it (see Appendix B).

Complete implementation of IAVA policy will help ensure that DoD Components take appropriate mitigating actions against vulnerabilities to avoid serious compromises to DoD computer system assets that would potentially degrade mission performance.

IAVA Policy Requirements

The IAVA policy memorandum requires each C/S/A to register in the IAVA database located on the IAVA website, acknowledge receipt of IAVA notifications, and report compliance.

Registration. To register in the IAVA database, each point of contact should contact DISA to obtain a DISA Form 41. When DISA receives the completed form, it will issue a user identification name and password so that the point of contact can gain access to the IAVA database.

According to the Director, Infrastructure and Information Assurance Directorate, Office of ASD (C³I), the IAVA policy applies to all DoD Components. In August 2000, at the time of the issuance of our draft audit report, all 9 CINCs, 4 Services, and 14 Defense agencies had registered as reporting entities, but 4 other DoD Components had not registered. As of November 2000, all DoD Components were effectively registered because OSD had decided that the four organizations that had not registered are reporting through OSD and, therefore, will not be required to register separately. Appendix B provides a detailed list of the DoD Components and also identifies those that will not register separately but will report through OSD.

Acknowledgement of Receipt. Once a point of contact is registered with the IAVA database, DISA notifies the point of contact by electronic mail when an IAVA is issued. The electronic mail message directs the point of contact to access the DoD Computer Emergency Response Team (CERT) website and review the posted IAVA notification. Each point of contact is to acknowledge receipt of the IAVA notification to the IAVA database within 5 days, unless specified otherwise. Appendix C shows DoD Components' acknowledgement to the alerts posted in 2000. As of November 2000, all DoD Components were complying with the acknowledgement requirements.

Report Compliance. The points of contact are to implement the corrective action necessary to fix the vulnerability and report the status of compliance to the IAVA database within 30 days, unless specified differently in the IAVA message. The policy memorandum requires that compliance information must include the number of assets affected, the number of assets in compliance, and the number of assets with waivers. As of August 2000, only four CINCs, one Service, four Defense agencies, and two other DoD Components had reported compliance in accordance with IAVA policy. However, information extracted from the IAVA database on November 6, 2000, showed significant improvement. All CINCs, 2 of the 4 Services, and 13 of 14 Defense agencies were now reporting in compliance with IAVA policy. Of those categorized as other DoD Components, OSD was not yet reporting compliance in accordance with IAVA policy, but was taking actions to become fully compliant. Appendix D shows DoD Components' compliance to the alerts posted in 2000.

CINCs. We obtained information from the IAVA database to determine whether the nine CINCs had complied with the IAVA policy for the three alerts

posted in 2000. At the time of the issuance of our draft audit report in August 2000, four CINCs reported compliance data as outlined in the IAVA policy. As of November 2000, all CINCs were reporting compliance data in accordance with the policy.

Services. We contacted the Services to determine whether they were implementing the IAVA policy and disseminating the IAVA notifications to all program managers, system administrators, and other personnel responsible for implementing and managing technical responses.

The Services had implemented a positive control mechanism for ensuring compliance with IAVA notifications. The Services stated that they had developed a process to receive alert notifications and to disseminate the alerts to the lowest level.

At the time of the issuance of our draft report, only the Navy was reporting compliance data to the IAVA database in accordance with the standards set forth in the IAVA policy memorandum. As of November 2000, the Marine Corps was also reporting correctly. The Army and Air Force were still not reporting in accordance with policy. The Army was reporting compliance in the form of percentages, and the Air Force was reporting compliance by stating that it was in compliance.

Defense Agencies. At the time of the issuance of our draft report, only four Defense agencies reported compliance in terms of number of assets affected, number of assets in compliance, number of waivers requested, and number of waivers approved or by indicating that the IAVA was not applicable to their assets. The remaining Defense agencies reported compliance data by stating either that they were compliant or they did not indicate any form of compliance. As of November 2000, the reporting situation had improved. Only one Defense agency, the Defense Security Service, had not complied with the reporting requirements, but it was working to put an infrastructure in place for reporting in accordance with the policy.

Other DoD Components. At the time of the draft report, the IAVA database indicated that two other Components (Washington Headquarters Services and the Inspector General) reported compliance data in accordance with the policy memorandum. The remaining three other DoD components that were registered (OSD, Joint Staff, and Defense Prisoner of War/Missing Personnel Office) reported by stating either that they were compliant or they did not indicate any form of compliance. OSD had not acknowledged receipt of IAVA notifications or reported compliance in accordance with IAVA policy because a formal internal compliance process had not been finalized and personnel had not been trained. OSD developed a draft IAVA implementation plan and a draft IAVA instruction, but both documents needed to be approved by ASD(C3I) before OSD would be able to comply with the IAVA policy tasking. OSD set a tentative date of February 5, 2001, to train all personnel and establish a process for reporting compliance with the IAVA policy.

As of November 2000, OSD was acknowledging receipt of IAVA notifications, but was not yet reporting compliance in accordance with IAVA policy.

However, the Deputy Director, OSD Network Operations, stated that the IAVA system would be fully implemented within OSD in April 2001. At that time, all OSD umbrella organizations (those organizations that would report IAVA compliance through OSD) would register all assets affected, the number of assets in compliance, and the number of assets with waivers and, therefore, be able to report in accordance with the IAVA policy. Additional audit work since the issuance of the draft report disclosed that the Joint Staff was now reporting compliance in accordance with the IAVA policy memorandum. The Defense Prisoner of War/Missing Personnel Office is an OSD umbrella organization that will report to OSD.

OSD Umbrella Organizations. The OSD umbrella organizations that will report directly to OSD include the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Under Secretary of Defense for Policy; the Under Secretary of Defense (Comptroller and Chief Financial Officer); the Under Secretary of Defense for Personnel Readiness; the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence); the Assistant Secretary of Defense for Health Affairs; the Assistant Secretary of Defense for Intelligence Oversight; the Assistant Secretary of Defense for Legislative Affairs; the Assistant Secretary of Defense for Public Affairs; the Assistant Secretary of Defense for Reserve Affairs; the General Counsel; the Executive Secretary of the Department of Defense; the Director, Operational Test and Evaluation; the Director, Program Analysis and Evaluation; the Director, American Forces Information Services; the Director, Defense Prisoner of War/Missing Personnel Office; the Director, DoD Education Activity; the Director, DoD Human Resources Activity; the Director, Office of Economic Adjustment; and the Director, TRICARE Management Activity.

The Deputy Director, OSD Network Operations, stated that the draft OSD instruction for the umbrella organizations, "OSD Information Assurance Vulnerability Assessment," was provided to ASD(C³I) for coordination and approval in July 2000; however, as of November 2000, the instruction was not finalized. The draft instruction outlines the roles and responsibilities for the OSD umbrella organizations to report compliance through the IAVA Desk Officer within the OSD Information Technical Directorate.

Implementation of the IAVA Policy

We attributed the poor implementation status of the IAVA process at the time of our draft report to the lack of implementation of the Deputy Secretary of Defense IAVA policy memorandum. As of November 2000, the ASD(C³I) had not issued a final Instruction formalizing the IAVA process and had not developed an implementation plan for IAVA compliance.

Status of Instruction. According to the IAVA policy memorandum, a DoD Instruction was to be developed to formalize the IAVA process. However, as of November 2000, the Instruction was still in draft form. The draft Instruction

states that the policy is applicable to all the information systems managed or used by DoD Components. However, the Instruction defines roles and responsibilities for only the C/S/As; it does not include the roles and responsibilities of other DoD Components. The draft IAVA Instruction is also vague in defining the common methodology for the Designated Approval Authorities to assess risk when granting waivers and in who may be designated as a C/S/A point of contact. Also, the draft Instruction does not require the Designated Approval Authorities to document their assessment of an asset's risk. The draft Instruction states that DISA will periodically report the compliance status of the C/S/As and waivers to the Deputy Secretary of Defense. Therefore, Designated Approval Authorities should maintain proper documentation for risk assessments explaining why a waiver was granted for a system asset. Also, the draft Instruction does not address how a system asset will be monitored if a waiver is granted, so that the vulnerability is not exploited before the corrective action is implemented. The draft Instruction states that each C/S/A should designate a primary and secondary point of contact, but it does not state the type of position or training that should be held by the points of contact.

Status of Implementation Plan. The IAVA policy memorandum gave the overall responsibility to ASD(C³I) to implement the IAVA policy to all the C/S/As. As of November 2000, an overall DoD implementation plan had not been developed. Without an overall DoD implementation plan, no set guidelines were being followed or issued to the DoD Components on how to register, report, and comply with the IAVA database in accordance with the policy memorandum. Also, according to the Director, Infrastructure and Information Assurance Directorate of ASD(C³I), the Directorate does not have the authority to enforce the requirement that DoD Components register and report compliance in accordance with the IAVA policy. The Infrastructure and Information Assurance Directorate is responsible only for implementing the IAVA policy.

Management of the IAVA Process

DISA Responsibilities. DISA is responsible for developing and maintaining the IAVA process. The IAVA database system is used to track compliance and statistics. Each DoD Component must register a point of contact in the database to obtain a user identification name and password to ensure receipt of the IAVA notification. The IAVA process provides DoD Components with a positive control mechanism to ensure that system administrators receive, acknowledge, and comply with alert notifications. Also, it should provide a method to measure risk avoidance within the overall risk management framework. See Appendix E for an explanation of the IAVA process.

IAVA Notification. The CERT is responsible for the integrity and availability of elements and applications of the Defense Information Infrastructure. When

the CERT becomes aware of a vulnerability to DoD computer system assets, it conducts research to determine:

- the type of operating system affected,
- the vulnerability of the application affected,
- the ease of access to the system,
- the type of threat imposed,
- whether the infrastructure will be affected, and
- whether the vulnerability has already been exploited.

Based on the results of the its research, the CERT will decide whether to issue an IAVA, an Information Assurance Vulnerability Bulletin, or a Technical Advisory. An IAVA is generated when a vulnerability is considered to be severe and a known corrective action is available. An IAVA requires DoD Components to acknowledge receipt of the alert notification and to report the status of compliance within the specified timeframe. A Bulletin requires an acknowledgment of alert notifications; it is issued for a vulnerability that is not an immediate threat but which, if not corrected, could escalate to a more severe problem. An Advisory does not have reporting requirements because it is considered to be low risk.

When the type of alert has been determined, the CERT develops the IAVA message and posts it on the CERT website. The IAVA message contains technical specifics about the vulnerability and the corrective action to be taken. DISA then disseminates an electronic message to all registered points of contact who disseminate the IAVA throughout their organizations and report compliance to the IAVA database within the established timeframe.

Effects of IAVA Noncompliance

For the IAVA policy to be effective, all DoD Components must register with the IAVA database and report compliance in accordance with specific guidance outlined in the IAVA policy memorandum. Without effective implementation of the IAVA policy, DoD Components cannot be assured of taking mitigating actions to avoid serious compromises to computer system assets. As a result, the reliability and effectiveness of the computer systems that are needed to ensure successful mission performance could be potentially degraded. Not maintaining positive control of vulnerability notifications and not applying the necessary corrective actions increase risks to the DoD infrastructure.

Summary

The IAVA policy requires DoD Components to register with the IAVA database and report compliance to IAVA notifications. The compliance information must be reported by stating the number of assets affected, the number of assets in compliance, and the number of assets with waivers. As of November 2000, all DoD Components that were required to register with the IAVA database had registered. Furthermore, all DoD Components with the exception of the Army, the Air Force, the Defense Security Service, and OSD, were reporting compliance in accordance with the December 30, 1999, IAVA policy memorandum. Both the Defense Security Service and OSD were working to become fully compliant. ASD(C³I) was developing an Instruction to formalize the IAVA process within DoD, but as of November 2000, the DoD Instruction was still in draft form. In addition, ASD(C³I) had not finalized and approved an internal OSD instruction outlining the IAVA process within OSD and its umbrella organizations. Finalization of both instructions will help ensure effective implementation of IAVA policy within DoD.

Recommendations, Management Comments, and Audit Response

Revised, Added, Deleted, and Renumbered Recommendations. As a result of the Joint Staff comments, we revised draft Recommendation 1.b to include training as part of the DoD implementation plan. We added Recommendation 1.c. to require the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) to finalize the internal OSD Information Assurance Vulnerability Alert Instruction. We deleted draft Recommendation 2. because those organizations will report their compliance through the Office of the Secretary of Defense. Draft Recommendation 3. has been renumbered as Recommendation 2.

1. We recommend that the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence, as DoD Chief Information Officer:

a. Revise and expedite the release of the DoD Information Assurance Vulnerability Alert Instruction to include language to define:

(1) The roles and responsibilities for DoD Components.

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments. The Director, Infrastructure and Information Assurance, concurred and stated that the draft DoD Instruction O-8530.bb, "Support to Computer Network Defense," addresses the responsibilities of the Assistant Secretary of Defense (Command, Control,

Communications and Intelligence) for vulnerability analysis, assessment notification, reporting, and coordination. Once this draft instruction has been signed, a separate DoD Instruction on Information Assurance Vulnerability Reporting and Mitigation will be developed that will contain specific language to define the roles and responsibilities of DoD Components.

The Deputy Director, OSD Network Operations, provided comments concurring with the report and specifically addressing implementation of the IAVA process within the Office of the Secretary of Defense.

(2) The types of positions and skills needed by the primary and secondary points of contact for DoD Components.

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments. The Director concurred and stated that any unique skills or training required to implement the vulnerability reporting and mitigation program will be identified.

(3) A common methodology of risk assessment for the Designated Approval Authorities to document the risk-assessment monitoring process when granting a waiver for an asset.

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments. The Director concurred with the intent of defining a common methodology for risk assessment, but stated that a separate risk assessment monitoring process was not required or appropriate because it is covered under DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process," December 30, 1997.

Audit Response. The Director's comments meet the intent of the recommendation. No further comments are required.

(4) A methodology for the Designated Approval Authorities to monitor systems so that vulnerabilities may not be exploited.

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments. The Director concurred with the intent of the recommendation, but stated that monitoring systems for vulnerabilities is not part of the Information Assurance Vulnerability Alert process. Draft DoD Directive 0-8530.aa states that an effective Computer Network Defense is predicated upon robust infrastructure and information assurance practices, including regular and proactive vulnerability analysis and assessment, and implementation of identified improvements. The Directive is scheduled to be signed prior to December 15, 2000.

Audit Response. The Director's comments meet the intent of the recommendation. No further comments are required.

b. Develop and disseminate a DoD implementation plan to DoD Components that will provide full Information Assurance Vulnerability Alert registration, reporting, training, and compliance guidance.

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments. The Director concurred that details about Information Assurance Vulnerability Alert registration, reporting and compliance needed to be addressed, but stated that an implementation plan was not required because the DoD Instruction on Information Assurance Vulnerability Reporting and Mitigation will address those details.

Audit Response. The Director's comments meet the intent of the recommendation, providing the instruction adequately addresses the requirements for Information Assurance Vulnerability Alert registrations, reporting, and compliance. Based on the Joint Staff comments, we revised the recommendation to include training.

c. Finalize and approve the Office of the Secretary of Defense instruction that outlines the roles and reporting responsibilities of the DoD Components that will be reporting through the Office of the Secretary of Defense.

2. We recommend that the Secretaries of the Army and Air Force; the Commandant of the Marine Corps; the Commanders of the U.S. European Command, U.S. Southern Command, U.S. Special Operations Command, U.S. Transportation Command, and U.S. Strategic Command; the Directors of the Ballistic Missile Defense Organization, Defense Advanced Research Projects Agency, Defense Commissary Agency, Defense Contract Audit Agency, Defense Finance and Accounting Service, Defense Intelligence Agency, Defense Security Service, Defense Threat Reduction Agency, Joint Staff, National Imagery and Mapping Agency, and National Reconnaissance Office report compliance by stating the number of assets affected, the number of assets in compliance, and the number of assets with waivers, as stated in the Deputy Secretary of Defense policy memorandum.

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments. Although not required to comment, the Director, Infrastructure and Information Assurance, stated that this requirement will be specifically addressed in the DoD Instruction on Information Assurance Vulnerability Reporting and Mitigation.

U.S. Southern Command Comments. The Commander of the U.S. Southern Command concurred and stated that due to operator error, the automated report for Information Assurance Vulnerability Alert 2000-A-0003 was not submitted. However, the report has since been submitted and the U.S. Southern Command is fully compliant.

Defense Advanced Research Projects Agency Comments. The Defense Advanced Research Projects Agency concurred and stated that it had completed corrective actions and reported compliance for the three Information Assurance Vulnerability Alerts identified in the report. However, it felt that the response

time between incident identification and Information Assurance Vulnerability Alert issuance needed to be reduced. The Defense Advanced Research Projects Agency suggested measures that provide a proactive information security intelligence gathering activity through both open sources and polling easily accessible adversarial sources, rapid response to paid security vendor alerts, and widespread informal liaison with other government, civilian, academic, and commercial organizations.

Defense Commissary Agency Comments. The Defense Commissary Agency concurred and stated that it had complied with the Information Assurance Vulnerability Alerts issued in 2000 and will continue the process when new Information Assurance Vulnerability Alerts are issued.

Defense Contract Audit Agency Comments. The Defense Contract Audit Agency responded that as of October 4, 2000, it was in compliance with the Information Assurance Vulnerability Alerts issued in 2000 and asked that the updated compliance status be included in the final report. The Defense Contract Audit Agency suggested that the Information Assurance Vulnerability Alert database contain a field to identify whether an alert is open or closed.

Audit Response. We updated Appendix D in the final report to reflect the updated compliance status.

Defense Finance and Accounting Service Comments. The Defense Finance and Accounting Service concurred and stated that it had updated the database and complied with the Information Assurance Vulnerability Alert process in accordance with the Deputy Secretary of Defense policy memorandum, December 30, 1999.

Defense Security Service Comments. The Defense Security Service concurred and stated that it was in the process of defining the agency's strategy for complying with the Deputy Secretary of Defense policy memorandum. The strategy will include establishing a Designated Approving Authority structure that will grant accrediting authority to Regional Directors and help in expediting Information Assurance Vulnerability Alerts to the regions. Another part of the strategy is to implement a hierarchical structure of Information System Security Officers, who will report the number of systems affected under their purview to the agency's Information Assurance Vulnerability Alert point of contact. The final aspect of the strategy is to appoint Information System Security Managers, who will provide support and oversight of the Information Assurance Vulnerability Alert process.

Defense Threat Reduction Agency Comments. The Defense Threat Reduction Agency stated that compliance was reported for the first two Information Assurance Vulnerability Alerts issued in 2000; however, for reasons unknown, those entries were not reflected in the Information Assurance Vulnerability Alert database. Since the draft report was issued, the Defense Threat Reduction Agency reentered the information and complied with the third Information Assurance Vulnerability Alert for 2000. The Defense Threat Reduction Agency

also noted that ongoing confusion existed concerning the information entry requirements and database problems with the Information Assurance Vulnerability Alert reporting system.

Joint Staff Comments. The Director, Joint Staff, concurred and stated that, in June 2000, at the direction of the Chairman, Joint Chiefs of Staff, a comprehensive review of the Commanders in Chief, Services, and Defense agencies Information Assurance Vulnerability Alert compliance was conducted. The review led to an increased awareness of the Information Assurance Vulnerability Alert reporting and compliance requirements by the Commanders in Chief, Services, and Defense agencies and an increased compliance. Any discrepancies noted in the review were corrected and, as of August 2000, the Joint Staff was fully compliant. The Director suggested that our recommendation on the IAVA Implementation Plan be expanded to include training. The Director also mentioned that, in coordination with the Defense Information Systems Agency and the U.S. Space Command, a determination was being made to decide the feasibility of including the Joint Task Force-Computer Network Defense in the Information Assurance Vulnerability Alert process.

Audit Response. In response to the Director's comments, we revised Recommendation 1.b. to include training.

DoD Education Activity. The DoD Education Activity concurred and stated that it was now in compliance with the Deputy Secretary of Defense policy memorandum.

Army Comments. The Army did not comment on the recommendation. We request that the Army provide comments in response to the final report.

Air Force Comments. The Air Force did not comment on the recommendation. We request that the Air Force provide comments in response to the final report.

Other Management Comments. The Marine Corps, the U.S. European Command, the U.S. Special Operations Command, the U.S. Transportation Command, the U.S. Strategic Command, the Ballistic Missile Defense Organization, the Defense Intelligence Agency, the National Imagery and Mapping Agency, the National Reconnaissance Office did not comment on a draft of this report. However, since the Information Assurance Vulnerability Alert database, of November 6, 2000, showed that those organizations have now reported compliance in accordance to the Deputy Secretary of Defense policy memorandum, no further response is required from those organizations.

Appendix A. Audit Process

Scope and Methodology

Work Performed. We conducted research on DoD Component compliance to the IAVA notifications, as directed by the Deputy Secretary of Defense IAVA policy memorandum, issued December 30, 1999. We reviewed the Deputy Secretary of Defense IAVA policy memorandum; the DoD draft IAVA Instruction, dated January 18, 2000; and the DISA IAVA Process Handbook, dated December 6, 1999.

We reviewed the actions taken by the Infrastructure and Information Assurance Directorate in implementing the IAVA policy. We also reviewed DISA actions to manage the IAVA process and disseminate IAVA notifications to the C/S/As. We assessed the 31 DoD Components only to determine whether they registered in the IAVA database and whether DoD Components, including the C/S/As, are reporting compliance in the manner set forth in the IAVA policy. Our review covered the periods from February 1998 through November 2000. During the audit, we interviewed and contacted personnel from the Office of the ASD(C³I), the Defense Information Assurance Program Office, and DISA.

Limitations to Scope. Our scope was limited because the IAVA policy had not been fully implemented by all DoD components, and the DoD components were not being required to report compliance in accordance to the IAVA policy memorandum. We did not review the overall compliance to the IAVA notifications; therefore, we did not include tests of management controls.

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. Although the Secretary of Defense has not established any goals for Information Assurance, the General Accounting Office lists it as a high risk area. This report pertains to Information Assurance as well as to achievement of the following goals, subordinate performance goals, and performance measures:

- **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)
- **FY 2001 Subordinate Performance Goal 2.5:** Improve DoD financial and information management. (01-DoD-2.5)
- **FY 2001 Performance Measure 2.5.3:** Qualitative Assessment of Reforming Information Technology Management. (01-DoD-2.5.3)

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

- **Information Technology Management. Objective:** Ensure DoD vital information resources are secure and protected. **Goal:** Build information assurance framework. (ITM-4.1)
- **Information Technology Management. 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 Department of Defense. This report provides coverage of the Information Management and Technology high-risk area.

Use of Computer-Processed Data. We did not evaluate the general and application controls of the DISA IAVA database that process DoD Component compliance to the IAVA notifications, although we relied on data produced by the database to conduct the audit. We did not evaluate the controls because the focus of the audit was on the effectiveness of the implementation of the IAVA policy. Not evaluating the controls did not affect the results of the audit.

Audit Type, Dates, and Standards. We performed this economy and efficiency audit from March 2000 through November 2000, in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available on request.

Prior Coverage

No prior coverage has been conducted on the subject during the last 5 years.

Appendix B. Commanders in Chief, Services, Defense Agencies, and Other DoD Components Required to be Registered Users

Commanders in Chief

U.S. Central Command
U.S. European Command
U.S. Pacific Command
U.S. Southern Command
U.S. Joint Forces Command
U.S. Special Operations Command
U.S. Space Command
U.S. Strategic Command
U.S. Transportation Command

Services

Air Force
Army
Marine Corps
Navy

Defense Agencies

Ballistic Missile Defense Organization
Defense Advanced Research Projects Agency
Defense Commissary Agency
Defense Contract Audit Agency
Defense Finance and Accounting Service
Defense Information Systems Agency
Defense Intelligence Agency

Defense Agencies (Cont'd)

Defense Logistics Agency

Defense Contract Management Agency*

Defense Security Cooperation Agency

Defense Security Services

Defense Threat Reduction Agency

National Imagery and Mapping Agency

National Reconnaissance Office

National Security Agency/Central Security Service

Other DoD Components

Inspector General, DoD

Joint Staff

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics*

Under Secretary of Defense for Policy*

Under Secretary of Defense (Comptroller and Chief Financial Officer)*

Under Secretary of Defense for Personnel and Readiness*

Assistant Secretary of Defense (Command, Control, Communications and Intelligence)*

Assistant Secretary of Defense for Health Affairs*

Assistant Secretary of Defense for Intelligence Oversight*

Assistant Secretary of Defense for Legislative Affairs*

Assistant Secretary of Defense for Public Affairs*

Assistant Secretary of Defense for Reserve Affairs*

General Counsel*

Defense Legal Services Agency*

Executive Secretary of the Department of Defense*

Operational Test and Evaluation*

Office of the Secretary of Defense (Cont'd)

Program Analysis and Evaluation*

American Forces Information Services*

Defense Prisoner of War/Missing Personnel Office*

DoD Education Activity*

DoD Human Resources Activity*

Office of Economic Adjustment*

TRICARE Management Activity*

Washington Headquarters Services

*Note: The Defense Contract Management Agency; Under Secretary of Defense for Acquisition, Technology, and Logistics; Under Secretary of Defense for Policy; Under Secretary of Defense (Comptroller and Chief Financial Officer); Under Secretary of Defense for Personnel and Readiness; Assistant Secretary of Defense (Command, Control, Communications and Intelligence); Assistant Secretary of Defense for Health Affairs; Assistant Secretary of Defense for Intelligence Oversight; Assistant Secretary of Defense for Legislative Affairs; Assistant Secretary of Defense for Public Affairs; Assistant Secretary of Defense for Reserve Affairs; General Counsel; Executive Secretary of the Department of Defense; Operational Test and Evaluation; Program Analysis and Evaluation; the Defense Legal Services Agency; American Forces Information Services; Defense Prisoner of War/Missing Personnel Office; DoD Education Activity; DoD Human Resources Activity; Office of Economic Adjustment; and TRICARE Management Activity report compliance through other agencies; therefore, they do not need to register with the IAVA database.

Appendix C. Acknowledgement of the Information Assurance Vulnerability Alerts (IAVA) Issued in 2000

This appendix illustrates DoD Component acknowledgement of the three IAVAs issued in 2000. The data was obtained from the Non-secure Internet Protocol Routing Network IAVA database website (as of November 2000) and Secure Internet Protocol Router Network IAVA database website (as of November 2000).

Information Assurance Vulnerability Alert Numbers

	2000-A-0001.0.0-01	2000-A-0002.0.0-01	2000-A-0003.0.0-01
	<u>Acknowledged</u>	<u>Acknowledged</u>	<u>Acknowledged</u>
Commanders in Chiefs			
U.S. Central Command	Yes	Yes	Yes
U.S. European Command	Yes	Yes	Yes
U.S. Joint Forces Command	Yes	Yes	Yes
U.S. Pacific Command	Yes	Yes	Yes
U.S. Southern Command	Yes	Yes	Yes
U.S. Space Command	Yes	Yes	Yes
U.S. Special Operations Command	Yes	Yes	Yes
U.S. Strategic Command	Yes	Yes	Yes
U.S. Transportation Command	Yes	Yes	Yes
Services			
Air Force	Yes	Yes	Yes
Army	Yes	Yes	Yes
Marine Corps	Yes	No	Yes
Navy	Yes	Yes	Yes
Defense Agencies			
Ballistic Missile Defense Organization	Yes	Yes	Yes
Defense Advanced Research Projects Agency	Yes	Yes	Yes
Defense Commissary Agency	Yes	Yes	Yes
Defense Contract Audit Agency	Yes	Yes	Yes
Defense Finance and Accounting Service	Yes	Yes	Yes
Defense Information Systems Agency	Yes	Yes	Yes
Defense Intelligence Agency	Yes	Yes	Yes
Defense Logistics Agency	Yes	Yes	Yes
Defense Security Cooperation Agency	Yes	Yes	Yes
Defense Security Services	Yes	Yes	Yes
Defense Threat Reduction Agency	Yes	Yes	Yes
National Imagery and Mapping Agency	Yes	Yes	Yes
National Reconnaissance Office	Yes	Yes	Yes
National Security Agency/Central Security Service	Yes	Yes	Yes

Information Assurance Vulnerability Alert Numbers			
	2000-A-0001.0.0-01	2000-A-0002.0.0-01	2000-A-0003.0.0-01
	<u>Acknowledged</u>	<u>Acknowledged</u>	<u>Acknowledged</u>
Other DoD Components			
Inspector General, DoD	Yes	Yes	Yes
Joint Staff	Yes	Yes	Yes
Office of Secretary of Defense	Yes	Yes	Yes
Washington Headquarters Services	Yes	Yes	Yes

Appendix D. Compliance With the Information Assurance Vulnerability Alerts (IAVA) Issued in 2000

This appendix illustrates DoD Component compliance with the three IAVAs issued in 2000. The data was obtained from the Non-secure Internet Protocol Routing Network IAVA database website (as of November 2000) and Secure Internet Protocol Router Network IAVA database website (as of November 2000).

Information Assurance Vulnerability Alert Numbers			
	2000-A-0001.0.0-01	2000-A-0002.0.0-01	2000-A-0003.0.0-01
	Compliance Reported in Accordance to IAVA Policy	Compliance Reported in Accordance to IAVA Policy	Compliance Reported in Accordance to IAVA Policy
Commanders in Chiefs			
U.S. Central Command	Yes	Yes	Yes
U.S. European Command	Yes	Yes	Yes
U.S. Joint Forces Command	Yes	Yes	Yes
U.S. Pacific Command	Yes	Yes	Yes
U.S. Southern Command	No	Yes	Yes
U.S. Space Command	Yes	Yes	Yes
U.S. Special Operations Command	Yes	Yes	No
U.S. Strategic Command	Yes	Yes	Yes
U.S. Transportation Command	Yes	Yes	Yes
Services			
Air Force*	No	No	No
Army*	No	No	No
Marine Corps	Yes	Yes	Yes
Navy	Yes	Yes	Yes
Defense Agencies			
Ballistic Missile Defense Organization	Yes	No	Yes
Defense Advanced Research Projects Agency	Yes	Yes	Yes
Defense Commissary Agency	Yes	Yes	Yes
Defense Contract Audit Agency	Yes	Yes	Yes
Defense Finance and Accounting Service	Yes	Yes	Yes
Defense Information Systems Agency	Yes	Yes	Yes
Defense Intelligence Agency	Yes	Yes	Yes
Defense Logistics Agency	Yes	Yes	Yes
Defense Security Cooperation Agency	Yes	No	Yes
Defense Security Service**	No	No	Yes
Defense Threat Reduction Agency	No	Yes	Yes
National Imagery and Mapping Agency	Yes	No	Yes
National Reconnaissance Office	Yes	Yes	Yes

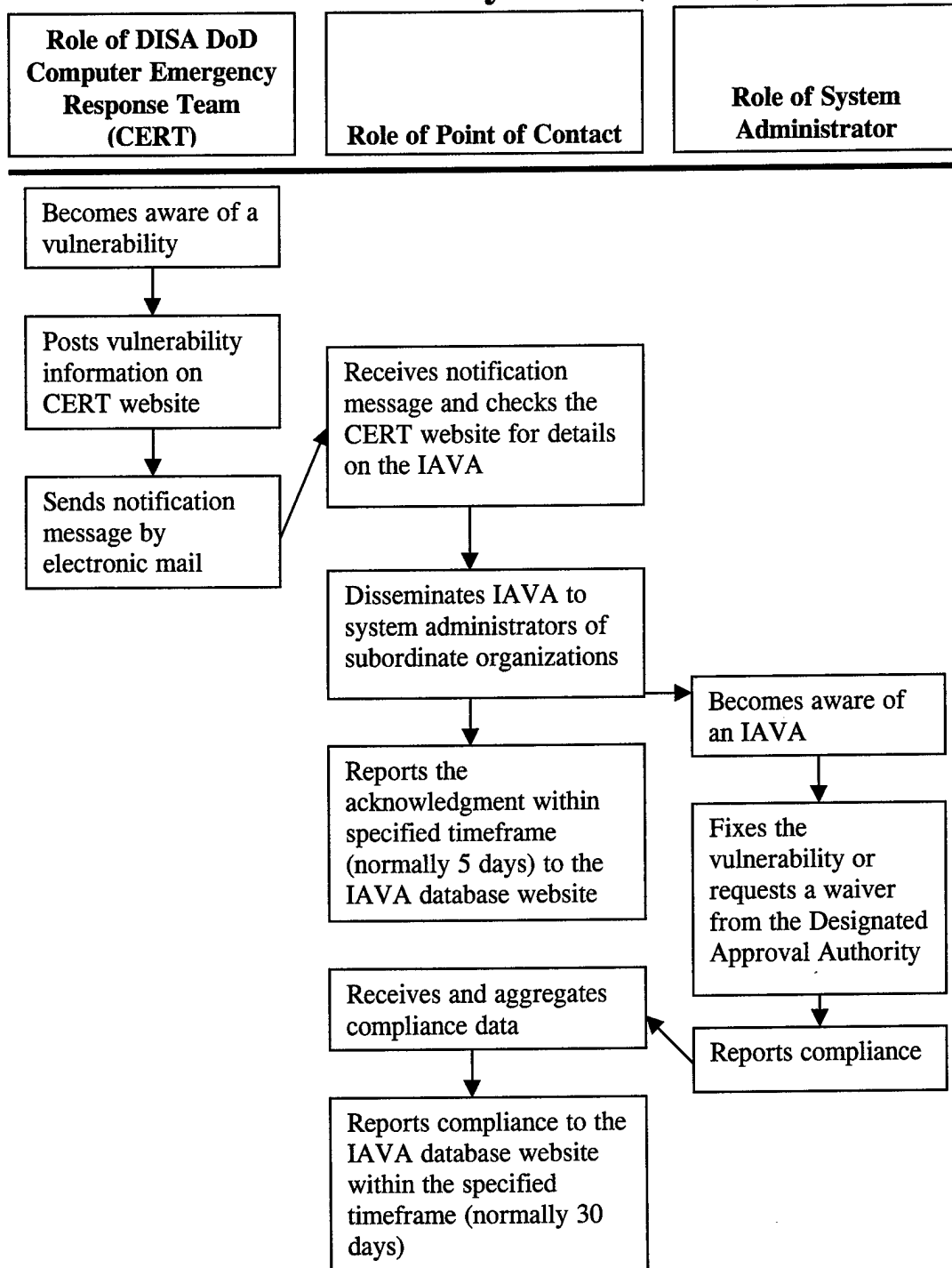
* DoD Components not complying with the Deputy Secretary of Defense IAVA policy memorandum.

** Defense Security Service is working to put an infrastructure in place to report the number of systems affected by the Information Assurance Vulnerability Alerts.

Information Assurance Vulnerability Alert Numbers			
	2000-A-0001.0.0-01	2000-A-0002.0.0-01	2000-A-0003.0.0-01
	Compliance Reported in Accordance to <u>IAVA Policy</u>	Compliance Reported in Accordance to <u>IAVA Policy</u>	Compliance Reported in Accordance to <u>IAVA Policy</u>
Defense Agencies (cont'd)			
National Security Agency/Central Security Service	Yes	Yes	Yes
Other DoD Components			
Inspector General, DoD	Yes	Yes	Yes
Joint Staff	Yes	Yes	Yes
Office of Secretary of Defense***	No	No	No
Washington Headquarters Services	Yes	Yes	Yes

*** The Office of the Secretary of Defense indicates in the Information Assurance Vulnerability Alert database that statistics will be reported after January 2001.

Appendix E. The Information Assurance Vulnerability Alert (IAVA) Process



Appendix F. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense (Comptroller)
 Deputy Chief Financial Officer
 Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
 Deputy Assistant Secretary of Defense (Deputy Chief Information Officer)

Joint Staff

Director, Joint Staff

Department of the Army

Auditor General, Department of the Army
Chief Information Officer, Department of Army

Department of the Navy

Commandant, Marine Corps
Naval Inspector General
Auditor General, Department of the Navy
Chief Information Officer, Department of Navy

Department of the Air Force

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

Unified Commands

Commander in Chief, U.S. European Command
Commander in Chief, U.S. Pacific Command
Commander in Chief, U.S. Joint Forces Command
Commander in Chief, U.S. Southern Command
Commander in Chief, U.S. Central Command
Commander in Chief, U.S. Space Command
Commander in Chief, U.S. Special Operations Command

Unified Commands (cont'd)

Commander in Chief, U.S. Transportation Command
Commander in Chief, U.S. Strategic Command

Other Defense Organizations

Director, Ballistic Missile Defense Organization
Director, Defense Advanced Research Projects Agency
Director, Defense Commissary Agency
Director, Defense Contract Audit Agency
Director, Defense Contract Management Agency
Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Director, Defense Intelligence Agency
 Inspector General, Defense Intelligence Agency
Director, Defense Legal Services Agency
Director, Defense Logistics Agency
Director, Defense Security Cooperation Agency
Director, Defense Security Service
Director, Defense Threat Reduction Agency
Director, National Security Agency
 Inspector General, National Security Agency
Director, National Imagery and Mapping Agency
Director, National Reconnaissance Office
Director, American Forces Information Services
Director, Defense Prisoner of War/Missing Personnel Office
Director, Department of Defense Education Activity
Director, Department of Defense Human Resources Activity
Director, Office of Economic Adjustment
Director, TRICARE Management Activity
Director, Washington Headquarters Services

Non-Defense Federal Organizations

Office of Management and Budget
 Office of Information and Regulatory Affairs

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

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), Infrastructure and Information Assurance Comments



COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

31 OCT 2000



MEMORANDUM FOR DoD INSPECTOR GENERAL

SUBJECT: Audit Report on DoD Compliance with the Information Assurance Vulnerability
Alert Policy (Project No. D2000AS-0086.003)

Office of the Assistant Secretary of Defense (Command, Control, Communications, and
Intelligence) (OASD(C3I)) comments on the subject report are provided as an attachment.

Please direct any questions to Ms. Marti Pickens of the Defense-wide Information Assurance
Program (DIAP) staff. She can be reached at 703-602-9981 or by email to
pickensm@osd.pentagon.mil.

Richard C. Schaeffer
Director, Infrastructure and
Information Assurance

Attachment



**OASD(C3I) Response to
Audit Report on
DoD Compliance with the Information Assurance
Vulnerability Alert Policy
(Project No. D2000AS-0086.003)**

Recommendation:

1. That ASD(C3I), as DoD Chief Information Officer:

a. Revise and expedite the release of the DoD Information Assurance Vulnerability Alert Instruction to include:

- (1) Language to define the roles and responsibility for DoD Components.**
- (2) Language to define the types of positions and skills needed by the primary and secondary points of contact for DoD Components.**
- (3) Language to define a common methodology of risk assessment for the Designated Approval Authorities to document the risk assessment monitoring process when granting a waiver for an asset.**
- (4) Language to define how the Designated Approval Authorities should monitor systems so that vulnerabilities may not be exploited.**

DoD Response

The establishment of a Defense-wide Information Assurance Vulnerability Analysis and Assessment notification, reporting, and coordination process is a responsibility assigned to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) in draft DoD Instruction O-8530.bb, "Support to Computer Network Defense (CND)." Also, Enclosure 6 to that Instruction, "Information Assurance Vulnerability Alert (IAVA)," specifically formalizes the guidance provided in the December 1999 policy memorandum. Once the CND Instruction is signed, a separate DoD Instruction will be developed to formalize a DoD Information Assurance Vulnerability Reporting and Mitigation Program. This Instruction will include vulnerability reporting guidance currently provided in Chairman of the Joint Chiefs of Staff Instruction 6510.01B, "Defense Information Operations Implementation," August 22, 1997, and its replacement (CJCSI 6510.01C, "Information Assurance Implementation (IA Defense in Depth and Computer Network Defense)") as well as specific guidance on vulnerability mitigation (to include the IAVA process).

Concur with Recommendation 1.a.(1). The DoD Instruction on Information Assurance Vulnerability Reporting and Mitigation will include specific language that defines the roles and responsibilities of DoD Components.

Attachment

Concur with Recommendation 1.a.(2). Any unique skills or training required to implement the vulnerability reporting and mitigation program will be identified. This will include only specific skills or training above those currently required for Information Assurance (IA) certification of system administrators (which already includes knowledge of local IAVA procedures as a performance item).

Concur with the intent of Recommendation 1.a.(3).

While we agree with the intent of defining a common methodology for risk assessment, this is already covered to a degree under DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997. A separate, specific risk assessment monitoring process for granting waivers to IAVAs is not required or appropriate.

It should be noted that most IAVA waivers are granted based on one (or more) of the following reasons (i.e., at times, each could be considered as subsets of the others; at other times, must be considered as stand-alone items):

- A risk management decision;
- Change Control Board review pending (i.e., issues affecting the Global Command and Control System (GCCS), Global Command Support System (GCSS), etc.);
- Systems where, because of age, it is not practical or possible to implement the change;
- Systems where the recommended change conflicts with the application the system is dedicated to, and;
- Systems where a tooling change within the system would be required to implement the change.

Concur with the intent of Recommendation 1.a.(4). However, monitoring systems for vulnerabilities is not part of the IAVA process. Draft DoD Directive O-8530.aa specifically states that effective CND is predicated upon robust infrastructure and information assurance practices, including regular and proactive vulnerability analysis and assessment, and implementation of identified improvements. This draft Directive has completed formal coordination, is in the comment reconciliation phase, and should be signed prior to 15 December 2000.

b. Develop and disseminate a DoD implementation plan to DoD Components that will provide full Information Assurance Vulnerability Alert registration, reporting, and compliance guidance.

DoD Response

Concur with the intent of Recommendation 1.b. The DoD Instruction on Information Assurance Vulnerability Reporting and Mitigation to be developed (see response to Recommendation 1.a.(1)) will address the details of IAVA registration, reporting, and compliance. No separate implementation plan is required.

2. We recommend that the Directors of the American Forces Information Services, DoD Education Activity, DoD Human Resources Activity, and TRICARE Management Activity register with the Information Assurance Vulnerability Alert database and report compliance in accordance with the format indicated in the Deputy Secretary of Defense Information Assurance Vulnerability Alert Policy memorandum.

DoD Response

Concur. This is an OSD Component action; no DoD action is required.

3. We recommend that the Secretaries of the Army and Air Force; Commandant of the Marine Corps; Commanders of the U.S. European Command, U.S. Southern Command, U.S. Special Operations Command, U.S. Transportation Command, and U.S. Strategic Command; Directors of the Ballistic Missile Command, Defense Advanced Research Projects Agency, Defense Commissary Agency, Defense Contract Audit Agency, Defense Finance and Accounting Service, Defense Intelligence Agency, Defense Security Service, Defense Threat Reduction Agency, National Imagery and Mapping Agency, and National Reconnaissance Office; Director, Joint Staff; and Director of the Defense Prisoner of War/Missing Personnel Office report compliance by stating the number of assets affected, number of assets in compliance, and number of assets with waivers as stated in the Deputy Secretary of Defense policy memorandum.

DoD Response

Concur. This responsibility will be specifically stated in the DoD Instruction on Information Assurance Vulnerability Reporting and Mitigation.

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), Defense Network Operations Comments



COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

30 October 2000

MEMORANDUM FOR Inspector General, Department of Defense (Auditing)
400 Army Navy Drive, Arlington, VA 22202

SUBJECT: DOD Compliance with the Information Assurance Vulnerability Alert Policy,
Project No. D2000AS-0086.003, 4 Aug 2000

The subject report and the overall findings have been reviewed. Enclosed is the response to the referenced draft report as it relates to the Office of the Secretary of Defense and its responsibility for the umbrella organizations.

The OSD point of contact is Richard Dyson, C3I Information Systems Security Officer (ISSO), 703-607-0234.


Connie L. Leonard

Deputy Director, OSD Network Operations

Enclosure



OSD Response to the DoD Inspector General Draft Report

SUBJECT: DoD Compliance with the Information Assurance Vulnerability Alert Policy,
Project No. D2000AS-0086.003, 4 Aug 2000

Recommendation 1a: Revise and expedite the release of the DOD Information Assurance Vulnerability Alert Instruction to include language to define:

(1) The roles and responsibilities for DOD components.

Response: Concur. The OSD Instruction for IAVA for the OSD umbrella organizations has been drafted. The instruction, OSD Instruction No. 5200.____, OSD Information Assurance Vulnerability Assessment was forwarded to ASD/C3I/DIAP for coordination in July 2000, therefore the document has not yet been promulgated to the OSD umbrella organizations. The OSD draft instruction for the umbrella organizations outlines the roles and responsibilities for OSD ITD, IAVA Desk Officer and the OSD umbrella organization IAVA POCs.

(2) The types of positions and skills needed by the primary and secondary points of contact for DOD components.

Response: Concur. OSD is currently working with DISA, Field Security Operations to develop the OSD IAVA handbook which outlines the positions and skills required by the primary and secondary points of contact for the DOD umbrella organizations. The handbook is scheduled to be completed by the end of November 2000.

(3) A common methodology of risk assessment for the Designated Approval Authorities to document the risk-assessment monitoring process when granting a waiver for an asset.

Response: Concur. Currently OSD has a manual reporting system in place. When an OSD umbrella organization cannot comply with an IAVA Alert or Bulletin within the allotted time, we have a security engineering staff with the expertise to perform a risk assessment as outlined in the WHS IAVA Handbook, paragraph 6.4.4.1 to establish the requirement for a waiver.

(4) A methodology for the Designated Approval Authorities to monitor systems so that vulnerabilities may not be exploited.

Response: Concur. The DAA will be an integral part of the IAVA VCTS system through their oversight role. The DAA will be able to see from the VCTS that OSD and the umbrella organizations are in compliance or if they aren't. The DAA will maintain a Certification and Accreditation database for tracking purposes. However, the DAA cannot establish a methodology to monitor systems so that vulnerabilities may not be exploited without

a Certification Authority in OSD. The DITSCAP specifically details certification activities to the CA throughout the lifecycle of an automated information system. The CA role is distinctly separate from the DAA role and will be established for OSD as soon as possible to begin the DITSCAP for OSD.

Recommendation 1b: Develop and disseminate a DOD implementation plan to DOD Components that will provide full Information Assurance Vulnerability Alert registration, reporting and compliance guidance.

Response: Concur. We have an implementation timeline (spreadsheet) in place with DISA Field Security Operations and we anticipate full compliance by 30 April 2001. At this time, we have not notified the OSD umbrella organizations officially due to the draft instruction being in coordination. However, we do have a manual e-mail system in place to notify the OSD organizations which includes AT&L, C3I, P&R, Policy, Comptroller, Executive Secretariat, IO, Legislative Affairs, Public Affairs, Reserve Affairs, Health Affairs, PA&E, General Counsel, OT&E, and the following Field Activities, American Forces Information Service (Public Affairs), Defense POW/MP Office (Policy), DOD Education Activity (P&R), DOD Human Resources Activity (P&R), Office of Economic Adjustment (AT&L), and the Tricare Management Activity (Health Affairs). The OSD IAVA Desk Officer is officially registered with the IAVA database and has been forwarding by e-mail IAVA alerts (none have been received since we put the manual system in place) and bulletins (two bulletins have been received) to the OSD umbrella organizations to acknowledge and comply. The OSD IAVA Desk Officer has officially acknowledged receipt of all 2000 IAVA Alerts and Bulletins.

Recommendation 2: We recommend that the Directors of the American Forces Information Services, the DOD Education Activity, the DOD Human Resources Activity, and the TRICARE Management Activity register with the Information Assurance Vulnerability Alert database and report compliance in accordance with the format indicated in the Deputy Secretary of Defense Information Assurance Vulnerability Alert policy memorandum.

Response: Concur. The OSD Field Activities are included in the OSD umbrella organization for reporting purposes so will not need to be registered separately in the IAVA database. The IAVA POCs throughout OSD will be registered and trained by DISA to use the Vulnerability Compliance Tracking System (VCTS) in January 2001. The VCTS will have all OSD systems registered by the IAVA POCs and this system uploads compliance statistics into the IAVA database.

Recommendation 3: We recommend that the Secretaries of the Army and Air Force; the Commandant of the Marine Corps; the Commanders of the U.S. European Command, U.S. Southern Command, U.S. Special Operations Command, U.S. Transportation Command, and U.S. Strategic Command; the Directors of the Ballistic Missile Command, Defense Advanced Research Projects Agency, Defense Commissary Agency, Defense Contract Audit Agency, Defense Finance and Accounting Service, Defense Intelligence Agency, Defense Prisoner of War/Missing Personnel Office, Defense Security Service, Defense Threat Reduction Agency, Joint Staff, National Imagery and Mapping

Deleted

Recommendation 3: We recommend that the Secretaries of the Army and Air Force; the Commandant of the Marine Corps; the Commanders of the U.S. European Command, U.S. Southern Command, U.S. Special Operations Command, U.S. Transportation Command, and U.S. Strategic Command; the Directors of the Ballistic Missile Command, Defense Advanced Research Projects Agency, Defense Commissary Agency, Defense Contract Audit Agency, Defense Finance and Accounting Service, Defense Intelligence Agency, Defense Prisoner of War/Missing Personnel Office, Defense Security Service, Defense Threat Reduction Agency, Joint Staff, National Imagery and Mapping Agency and National Reconnaissance Office report compliance by stating the number of assets affected, the number of assets in compliance, and the number of assets with waivers, as stated in the Deputy Secretary of Defense policy memorandum.

Response: Concur. When the IAVA System is fully implemented in April 2001, all OSD umbrella organizations will register via VCTS all assets affected, number of assets in compliance and the number of assets with waivers.

U.S. Southern Command Comments



REPLY TO
ATTENTION OF

DEPARTMENT OF DEFENSE
UNITED STATES SOUTHERN COMMAND
3511 NW 91ST AVENUE
MIAMI, FL 33172-1217

SCI62

2 October 2000

MEMORANDUM FOR DoD Office of the Inspector General

SUBJECT: U.S. Southern Command Response to the DoD Inspector General Audit Report

1. Reference. Draft Audit Report, DoD Office of the Inspector General, 4 August 2000, subject: DoD Compliance with the Information Assurance Vulnerability Alert Policy, Project No. D2000AS-0086.003.

2. U.S. Southern Command (USSOUTHCOM) concurs with the report and the recommendations outlined therein. Actions taken to date to correct non-compliance:

a. Updated Appendix B of SC regulation 525.22, SOUTHCOM Reporting Procedures. Corrected Information Assurance Vulnerability Alert (IAVAs) reporting in accordance with the DoD IAVA policy to include alerts, bulletins, and technical advisories.

b. The Theater Network Coordination Center (TNCC) is aggressively pursuing compliance reporting and has developed a status chart for more accurate tracking.

c. Received DISA Field Security Office Vulnerability Compliance Tracking System (VCTS) brief on 18 September 2000. The command plans to implement VCTS, with a goal to be fully operational by May 2001.

d. The command is sponsoring an Information Operations/Information Assurance conference from 23 - 27 October 2000. The goal of the staff is to train the components, direct reporting units and other theater organizations on the reporting procedures and clearly define roles and responsibilities with regard to Network Incidents, Information Conditions and IAVAs.

3. With regard to Appendix D, at the time of the report USSOUTHCOM was fully compliant with IAVA 2000-A-0002 and 0003. However, due to operator error the automated report was not submitted for 0003.

4. Points of contact are CW3 Lorie Bobzien and Mr. Larry Pettaway at DSN 567-3061/1670 or commercial (305) 437-3061/1670.

for Diana Mylunger
BENJAMIN F. FLETCHER
COL, USA
Director, J6

Defense Advanced Research Projects Agency Comments



DEFENSE ADVANCED RESEARCH PROJECTS AGENCY
3701 NORTH FAIRFAX DRIVE
ARLINGTON, VA 22203-1714

OCT 5 2000

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDITING

SUBJECT: Response to DoD IG Draft Report on Information Assurance Vulnerability Alert (IAVA) Policy

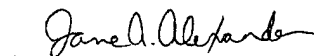
In response to the draft report entitled "DoD Compliance With the Information Assurance Vulnerability Alert Policy (IAVA)," dated August 04, 2000, (Project No. D2000AS-0086.003), the Defense Advanced Research Projects Agency (DARPA) concurs with the recommendation of the report. For the three IAVAs identified, DARPA has completed corrective actions and reported compliance. In addition, DARPA has acknowledged receipt of CY2000 bulletins and technical advisories. DARPA has also identified primary and secondary points of contact (POCs) for IAVAs. DARPA is now in full compliance with IAVA policies and practices. DARPA fully understands and supports the need for the DoD to enact protective measures, including IAVAs for all information systems under its auspices.

Given DARPA's mission and operational posture, it is subject to risks distinct from other DoD elements. DARPA mitigates those risks to its computer system assets by utilizing internal information security assets, measures, and policies.

In addition to all IAVAs provided, DARPA also utilized alert notifications from various sources, including vendor alerts, publicly accessible information security websites, internal intelligence gathering methods, and other similar sources. In all but three instances, IAVAs (alerts, bulletins, and advisories) were either days or weeks behind public and industry information security alert sources (See attachment).

DARPA will continue to use the IAVA notification and response process in conjunction with currently employed measures noted above, but recommends that action(s) be taken to reduce the time between incident identification and IAVA. Measures that DARPA suggest for consideration include: proactive information security intelligence gathering activity through both open sources and polling easily accessible adversarial sources (i.e., "black hat" hacker/cracker websites); rapid response to paid security vendor alerts (e.g., Symantec, Trend Micro, etc.); and widespread informal liaison with other government, civilian, academic, and commercial organizations. We believe these measures may be useful in improving IAVA response time.

We appreciate the opportunity to review the DoD IG draft report. My technical contact regarding this response is Mr. Scott M. Rubin and he may be reached on (703) 696-2417.


for F. L. Fernandez
Director

Attachment

Comparison between DARPA Incident Awareness and DISA IAVA Dates

IAVA #	IAVA Title	DARPA Awareness	IAVA Date	Source	Delta (days)
2000 Information Assurance Vulnerability Alerts					
2000-A-0001	Cross-Site Scripting Vulnerability	24-Mar-99	2-Feb-00	NTBugTraq	315
2000-A-0002	VBS/LOVELETTER VBScript WORM	4-May-00	4-May-00	NTBugTraq	0
2000-A-0003	Gauntlet Firewall for Unix and WebShield Cyberdaemon Buffer Overflow Vulnerability	22-May-00	24-May-00	ISS X-Force	2
2000 Information Assurance Vulnerability Bulletins					
2000-B-0001	Bind NXT Buffer Overflow	11-Nov-99	6-Mar-00	CERT/CC	116
2000-B-0002	Netscape Navigator Improperly Validates SSL Sessions	3-Apr-00	18-May-00	Neohapsis	45
2000-B-0003	Multiple Buffer Overflows in Kerberos Authenticated Services	16-May-00	19-May-00	BugTraq	3
2000-B-0004	(wu-ftpd) "Site Exec" Vulnerability and "setproctitle()" Vulnerability	29-Jun-00	10-Jul-00	SecurityFocus	11
2000-B-0005	Input Validation Problem in rpc.statd	5-Aug-00	19-Sep-00	BugTraq	45
2000-B-0006	IRIX TELNETD Vulnerability	14-Aug-00	19-Sep-00	BugTraq	36
2000 Technical Advisories					
2000-T-0001	Microsoft NT 4.0 Spoofed LPC Port Request Vulnerability	13-Jan-00	19-Jan-00	NTBugTraq	6
2000-T-0002	Microsoft "Registry Permissions" Vulnerability	9-Mar-00	28-Mar-00	NTBugTraq	19
2000-T-0003	Link View Server-Side Component Vulnerability	14-Apr-00	17-Apr-00	NTBugTraq	3
2000-T-0004	VBS.NewLove.A Worm	19-May-00	19-May-00	Symantec	0
2000-T-0005	IP Fragment Assembly Denial of Service Vulnerability	19-May-00	24-May-00	Microsoft	5
2000-T-0006	Unauthorized Cookie Access and Malformed Component Attribute Vulnerabilities	17-May-00	24-May-00	BugTraq	7
2000-T-0007	Microsoft Office 2000 UA ActiveX Control	13-May-00	2-Jun-00	Lopht	20
2000-T-0008	Microsoft SQL Server 7.0 Password Vulnerability	30-May-00	2-Jun-00	Microsoft	3
2000-T-0009	Life Stages Worm	19-Jun-00	19-Jun-00	Microsoft	0
2000-T-0010	Microsoft "IE Script" and "Office 2000 HTML Script"	13-Jul-00	19-Jul-00	Microsoft	6
2000-T-0011	Malformed E-mail Header Vulnerability	13-Jul-00	19-Jul-00	USSR Labs	6

Defense Commissary Agency Comments



DEFENSE COMMISSARY AGENCY
HEADQUARTERS
1300 E AVENUE
FORT LEE, VIRGINIA 23801-1800

REPLY TO
ATTENTION OF

IR

SEP 26 2000

MEMORANDUM FOR INSPECTOR GENERAL, ACQUISITION MANAGEMENT
DIRECTORATE, 400 ARMY NAVY DRIVE, ARLINGTON,
VA 22202-2885

SUBJECT: Audit Report on DoD Compliance With the Information Assurance Vulnerability
Alert Policy (Project No. D2000AS-0086.003)

Reference: Memorandum, DoDIG, August 4, 2000, SAB

Attached is the DeCA reply to the recommendations provided in subject report. If you
have any questions, please contact Mr. Ben Mikell at (804) 734-8103.

A handwritten signature in black ink, appearing to read "Crosby H. Johnson".

Crosby H. Johnson
Executive Director for Support

Attachment:
As stated

DEFENSE COMMISSARY AGENCY REPLY

SUBJECT: Audit Report on DoD Compliance With the Information Assurance
Vulnerability Alert Policy (Project No. D2000AS-0086.003)

RECOMMENDATION 3. We recommend that the Secretaries of the Army and Air Force; the Commandant of the Marine Corps; the Commanders of the U.S. European Command, U.S. Southern Command, U.S. Special Operations Command, U.S. Transportation Command, and U.S. Strategic Command; the Directors of the Ballistic Missile Command, Defense Advanced Research Projects Agency, Defense Commissary Agency, Defense Contract Audit Agency, Defense Finance and Accounting Service, Defense Intelligence Agency, Defense Prisoner of War/Missing Personnel Office, Defense Security Service, Defense Threat Reduction Agency, Joint Staff, National Imagery and Mapping Agency, and National Reconnaissance Office report compliance by stating the number of assets affected, the number of assets in compliance, and the number of assets with waivers, as stated in the Deputy Secretary of Defense policy memorandum.

DeCA REPLY. Concur. DeCA has now complied with the Information Assurance Vulnerability Alerts issued in 2000 and will continue this process as new ones come in.

Attachment

Defense Contract Audit Agency Comments



DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

October 4, 2000

IN REPLY REFER TO

OITN 590.14

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Audit Report on DoD Compliance with the Information Assurance
Vulnerability Alert Policy (Project No. D2000AS-0086.003)

We are providing comments to the subject audit report concerning Appendix D, Compliance with the Information Assurance Vulnerability Alerts (IAVA) Issued in 2000. As of this date, DCAA is in compliance with the three IAVAs listed in Appendix D. We would appreciate the updated compliance status be included in the final report.

DCAA is currently expanding the number of personnel who can access the IAVA web site to ensure accurate compliance reporting in the future. In one instance, IAVA 2000-A-0002.0.0-01 (VBS/Loveletter VBScript Worm), was completed in 5 days from release date but was not updated as completed until several months later due to the design of the IAVA web site. We believe the web site should contain a field to clearly identify whether an alert is open or closed.

If you have any questions about our comments, please contact David Kaiser, Network Operations Branch Chief, at 703-767-2254 or David.Kaiser@dcaa.mil.

Earl J. Newman
Earl J. Newman
Assistant Director,
Operations

Defense Finance and Accounting Service Comments



DFAS-HQ/S

DEFENSE FINANCE AND ACCOUNTING SERVICE

1931 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22240-5291
WWW.DFAS.MIL

OCT 2 2000



MEMORANDUM FOR DIRECTOR, ACQUISITION MANAGEMENT
DIRECTORATE, OFFICE OF THE INSPECTOR GENERAL,
DEPARTMENT OF DEFENSE

SUBJECT: DoD IG Draft Report, Project No. D2000AS-0086.003, "DoD Compliance
with the Information Assurance Vulnerability Alert Policy," dated
August 4, 2000

The Defense Finance and Accounting Service (DFAS) response regarding the draft audit
report, "DoD Compliance with the Information Assurance Vulnerability Alert Policy" dated
April 4, 2000, is attached.

My point of contact for this action is Kim Ponder, DFAS-HQ/SC, at (703) 607-3838.


C. Vance Kauzlarich

Director for Information and Technology

Attachment:
As Stated

cc: DFAS-HQ/F
DFAS-HQ/DI
Director, SEO-PE

**DFAS Comments on the DoD IG Draft Report,
Project No. D2000AS-0086.003**

DFAS concurs with the DoD IG Draft Report, Project No. D2000AS-0086.003, "DoD Compliance with the Information Assurance Vulnerability Alert (IAVA) Policy", dated April 4, 2000. DFAS's comments are provided below:

1. DFAS has complied with the requirement to register and comply with the IAVA process, as outlined in the Deputy Secretary of Defense Information Assurance Vulnerability Alert Policy Memorandum, dated December 30, 1999.
2. The IAVA Alerts that were audited included 2000-A-0001.0.0-01, 2000-A-0002.0.0-01, and 2000-A-0003.0.0-01. DFAS has acknowledged all three alerts on the IAVA Web site, but only 2000-A-0003.0.0-01 was reported as being compliant.
3. IAVA 2000-A-0001.0.0-01, Cross-Site Scripting Vulnerability, status: The "Web Technical Guidance Memo for DFAS Web Developers" has been finalized and is awaiting approval. The current status is as follows:

Number of assets affected: 0
Number of assets in compliance: 6
Number of assets with waivers: 0

4. IAVA 2000-A-0002.0.0-01, VBS/Loveletter VBScript WORM, status:

Number of assets affected: 23,000
Number of assets in compliance: 23,000
Number of assets with waivers: 0

Attachment

Defense Security Service Comments



DEFENSE SECURITY SERVICE
1340 BRADDOCK PLACE
ALEXANDRIA, VA 22314-1651

SEP 28 2000

MEMORANDUM FOR INSPECTOR GENERAL, DoD
Attention: Mr. Thomas F. Gimble

SUBJECT: Audit Report on DoD Compliance with the Information Assurance
Vulnerability Alert (IAVA) Policy (Project No. D2000AS-0086.003)

The Defense Security Service (DSS) has reviewed the draft audit report regarding IAVA policy compliance, and we concur with the findings and recommendations. Recently, DSS submitted a memorandum to the Defense Information Systems Agency (DISA) regarding DSS' compliance with this policy and addressed our plans in achieving full compliance with this policy. This memorandum has been attached for your review.

If you have any additional questions or concerns, please contact Ann F. Johnson, Acting Division Chief for Information Technology and Communications, at 410-865-2631.

for Judith M. Hughes
CHARLES J. CUNNINGHAM JR.
Director

Attachment



DEFENSE SECURITY SERVICE
1340 BRADDOCK PLACE
ALEXANDRIA, VA 22314-1651

SEP 1 2000

MEMORANDUM FOR DEFENSE INFORMATION SYSTEMS AGENCY
Attention: COL Larry Huffman (D33)

SUBJECT: Defense Security Service (DSS) Information Assurance Vulnerability Alert
(IAVA) Program

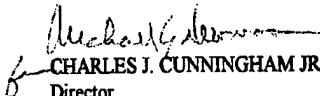
Reference: Department of Defense (DoD) Memorandum dated December 30, 1999,
"DoD Information Assurance Vulnerability Alert (IAVA)"

The purpose of this memorandum is to provide the DISA IAVA program manager with a status on DSS IAVA program implementation and to outline the agency's strategy for full compliance with the aforementioned memorandum. To date, DSS has a 100 percent compliance rate in acknowledging receipt of IAVA alerts and is working diligently to put in place an infrastructure to increase the percentage rate for reporting the number of systems that are affected by a given alert.

In order to accomplish full compliance with the DoD IAVA requirement, DSS is putting in place a Designated Approving Authority (DAA) structure at the regional level that will both grant accrediting authority to the DSS Regional Directors and help expedite IAVA issues in the regions.

DSS is in the process of implementing a hierarchical structure of Information System Security Officers (ISSOs) within each region throughout DSS. Each ISSO will report the number of systems under their purview to the agency's IAVA Point of Contact (POC) that are susceptible to a given IAVA alert. The POC will then report the total number of systems that are affected by an IAVA alert to DISA. In addition, the agency appointed Information System Security Manager (ISSM) will provide support and oversight for the overall IAVA process.

I feel that the appointment of regional DAAs, an agency ISSM, and the implementation of a DSS ISSO hierarchical structure will put in place the necessary security infrastructure to ensure DSS full compliance with the DoD IAVA requirements. If you have any additional questions or concerns, please contact Ann F. Johnson, Acting Deputy Chief of Staff for Information Technology & Communications, at (410) 865-2631.


CHARLES J. CUNNINGHAM JR.
Director

Attachment

Defense Threat Reduction Agency Comments



Defense Threat Reduction Agency
8725 John J Kingman Road MS 6201
Ft Belvoir, VA 22060-6201

2 October 2000

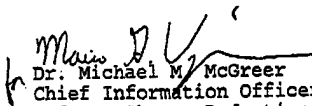
MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE, 400
ARMY NAVY DRIVE, ARLINGTON, VIRGINIA 22202-2885

SUBJECT: Audit Report on DoD Compliance With the
Information Assurance Vulnerability Alert Policy
(Project No. D2000AS-0086.003)

The Defense Threat Reduction Agency had reported compliance on items one and two of the three items reviewed. For reasons unknown, those entries were not reflected in the database. Subsequently DTRA has reentered the information as well as come into compliance for item 3, placing this agency in compliance to the extent possible.

As the IG report noted, OSD still has not issued final approval guidance for the IAVA program. It is extremely difficult to be in compliance with a program where the rules have not been approved by an executive authority and clearly defined to all affected parties.

It should be noted that there has been ongoing confusion concerning information entry requirements as well as database problems with IAVA reporting system. For example, there has been conflicting guidance as to whether an entry of -0- is required when an activity has no affected assets. In addition, earlier system access problems seem to have been resolved within the last 90 days.


Dr. Michael M. McGreer
Chief Information Officer
Defense Threat Reduction Agency

The Joint Staff Comments

Final Report
Reference



THE JOINT STAFF
WASHINGTON, DC

Reply ZIP Code:
20318-0300

DJSM-844-00
05 October 2000

MEMORANDUM FOR THE INSPECTOR GENERAL, DEPARTMENT OF
DEFENSE

Subject: DOD IG Audit Report on DOD Compliance with the Information
Assurance Vulnerability Alert (IAVA) Policy

1. Thank you for the opportunity to review the draft audit report¹ on DOD compliance with IAVA policy. The Joint Staff has reviewed the report and concurs, subject to incorporation of the comments below.

a. Page 8, Recommendation 1b. Change as follows: "Develop and disseminate a DoD Implementation Plan to DoD components that will provide full Information Assurance Vulnerability Alert registration, reporting, training, and compliance guidance."

REASON: The inclusion of training guidance to the DOD IAVA implementation plan will greatly assist the CINCs, Services, and Defense agencies (C/S/As) in correctly accessing and utilizing the IAVA Web page for compliance reporting.

b. Page 8, Recommendation 3: Comment: In Jun 00, at the direction of the Chairman of the Joint Chiefs of Staff, a comprehensive review of C/S/A IAVA compliance was conducted. This review, led by the Director, Command, Control, Communications, and Computer (C4) Systems Directorate (J-6), proved extremely beneficial for two reasons: C/S/A's overall awareness of IAVA program reporting and compliance requirements was significantly increased, and second, as a result of this attention, there was a marked increase in C/S/A IAVA compliance. Joint Staff discrepancies noted in this review have been corrected. Effective Aug 00, the Joint Staff is fully IAVA compliant.

2. The Joint Staff provides the following amplifying information to summarize additional actions taken to address the issue of IAVA compliance:

a. The Joint Staff, in coordination with DISA and USSPACECOM, is investigating the feasibility of including USSPACECOM's Joint Task Force-Computer Network Defense (JTF-CND) in the IAVA process. While DISA will continue to maintain the IAVA database, CJTF-CND, as the DOD Computer

Revised

Network Defense lead, will disseminate the IAVA message. Elevating this responsibility to the CINC level will help ensure visibility is maintained on this critical computer network defense issue.

b. To ensure wider dissemination of C/S/A IAVA compliance information to affected decision-makers, the Military Communications-Electronics Board's (MCEB) Information Assurance Panel (IAP) added a recurring IAVA compliance review to its monthly agenda. The purpose of this review is to maintain the present high level of awareness of the status of each C/S/A's IAVA compliance record. The IAP, co-chaired by the Joint Staff and the Defense Information Assurance Program with membership consisting of all of the Defense agencies and the Services, is the premier information assurance forum in the DOD and the action arm of the MCEB on information assurance issues.

3. The Joint Staff point of contact is Lieutenant Commander J.W. Beadles, 697-8896.



S. A. FRY
Vice Admiral, U.S. Navy
Director, Joint Staff

Reference:

- 1 DOD Draft Audit Report on DOD Compliance with the Information Assurance Vulnerability Alert Policy, 4 August 2000

Department of Defense Education Activity Comments



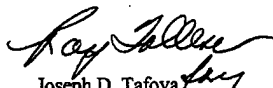
DEPARTMENT OF DEFENSE
EDUCATION ACTIVITY
4040 NORTH FAIRFAX DRIVE
ARLINGTON, VIRGINIA 22203-1635

OCT - 5 2000

MEMORANDUM FOR DIRECTOR, ACQUISITION MANAGEMENT DIRECTORATE
INSPECTOR GENERAL, DOD

SUBJECT: Draft of a Proposed Audit Report, "DoD Compliance With the Information
Assurance Vulnerability Alert Policy," (Project No. D2000AS-0086.003),
August 4, 2000

Thank you, for the opportunity to review and provide our comments on the subject draft audit report. We concur with the report's finding and recommendation that DoDEA register with the Information Assurance Vulnerability Alert database. Moreover, we appreciate your efforts in bringing this oversight to our attention. The attached memorandum from the Chief, Information Technology Division, DoDEA, reflects that the necessary corrective actions are complete. If you have any questions in this regard, please contact Mr. George E. Hanby, Office of Review and Compliance, at 703-696-9051, extension 2443.


Joseph D. Tafoya
Director

Attachment:
As stated



DEPARTMENT OF DEFENSE
EDUCATION ACTIVITY
4040 NORTH FAIRFAX DRIVE
ARLINGTON, VIRGINIA 22203-1635

September 29, 2000

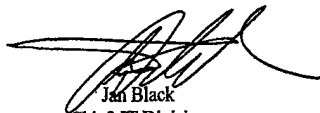
MEMORANDUM FOR ASSOCIATE DIRECTOR FOR MANAGEMENT

SUBJECT: DoD Compliance with the Information Assurance Vulnerability Alert (IAVA) Draft Audit Report dated August 16, 2000.

Reference, memorandum from the Associate Director for Management dated August 16, 2000, subject as above.

In accordance with Reference (a), the subject report was reviewed, and we are currently in compliance with the memorandum from Deputy Secretary of Defense, Subject: Department of Defense Information Assurance Vulnerability Alert, dated December 30, 1999. The IT Division submitted the DISA Form 41 to DISA and registered DoDEA in the official IAVA database. DoDEA received its user identification name and password on September 28, 2000.

Mr. Valerian E. Stasik is the DoDEA primary point of contact for IAVA database. Please Contact Mr. Stasik at (703) 696-1420, extension 2705, if you have any questions.



Jan Black
Chief, IT Division

cc: Chief, Office of Review and Compliance

Washington Headquarters Services Comments

Final Report
Reference



DEPARTMENT OF DEFENSE
WASHINGTON HEADQUARTERS SERVICES
DIRECTORATE FOR INFORMATION OPERATIONS AND REPORTS
1215 JEFFERSON DAVIS HIGHWAY, SUITE 1204
ARLINGTON, VA 22202-4302

AUG 28 2000

MEMORANDUM FOR THE DIRECTOR, ACQUISITION MANAGEMENT, DoD IG

Subject: Audit Report on DoD Compliance With the Information Assurance
Vulnerability Alert Policy (Project No. D2000AS-0086.003)

The purpose of this memorandum is to provide a couple of corrections to the subject report regarding Washington Headquarters Services (WHS).

At the bottom of page 3, the draft report states that "the Defense Legal Services Agency (DLSA) compliance is reported by Washington Headquarters Services" and again on page 12 shows DLSA under WHS. In actuality, DLSA is covered under the General Counsel in the Office of the Secretary of Defense. We have confirmed this with DLSA and understand from Mr. Carryer that they have an active IAVA account at this time.

We found the report to be most useful and rewarding to our personnel who have worked so hard to get us where we are on IAVA. Thank you for the opportunity to comment and please let me know if you need more information.

A handwritten signature in cursive script, reading "Robert S. Drake".

Robert S. Drake
WHS CIO

cc: Director, WHS
Director, RE&F
OGC (Mr. R. Carryer)

Revised
Pages 3 and
18

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report.

Thomas F. Gimble
Mary L. Ugone
Robert K. West
Eleanor A. Wills
Lois J. Wozniak
Kelli M. Burkewitz

INTERNET DOCUMENT INFORMATION FORM

A. Report Title: DOD Compliance with the Information Assurance Vulnerability Alert Policy

B. DATE Report Downloaded From the Internet: 12/07/00

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ Preparation Date 12/07/00

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.