DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

30 DEC 1998

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Department of Defense (DoD) Information Assurance Vulnerability Alert (IAVA)

Recent events continue to demonstrate that widely known vulnerabilities exist throughout DoD networks, with the potential to severely degrade mission performance. Our increasing reliance on the accurate and timely exchange of information mandates that information assurance no longer be relegated to a secondary concern. Information assurance is an essential element of operational readiness.

To protect DoD networks against potential vulnerabilities, we must increase emphasis on the Information Assurance Vulnerability Alert (IAVA) process, instituted in 1998 to provide positive control of vulnerability notification and corresponding corrective action within DoD. The Defense Information Systems Agency (DISA) shall manage the IAVA process and distribute alerts to all Commander-in-Chief (CINC), Military Service and Defense Agency (C/S/A) points of contact. All C/S/As shall comply with the IAVA process and with the guidance provided in the attachment, IAVA Requirements and Responsibilities.

Mitigation of information assurance vulnerabilities is a concern at the highest levels and the status of compliance with IAVA notifications shall be reported periodically to the Secretary of Defense. The DoD Inspector General shall make compliance with IAVA notifications a priority review area. Additionally, a DoD Instruction will be promulgated to formalize the IAVA process and the full information assurance vulnerability reporting and mitigation program.

Implementation of this policy will ensure that DoD components take the required mitigating actions against new system vulnerabilities so that a serious compromise of DoD assets is avoided. I have given the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) overall responsibility for the implementation of

U19377 /99

the IAVA policy and procedures across all DoD CINCs, Services, and Agencies. My point of contact is Mr. Richard Schaeffer, Director, Infrastructure and Information Assurance, at (703) 695-8705.

John Hamre

John J. Hamre

Attachment

Information Assurance Vulnerability Alert (IAVA) Requirements and Responsibilities

1. Information Assurance Vulnerability Alerts (IAVAs) are generated whenever a critical vulnerability exists that poses an immediate threat to the DoD and where acknowledgment and corrective action compliance must be tracked. Not all identified vulnerabilities and threats will warrant an IAVA.

a. IAVAs are issued by the Defense Information Systems Agency (DISA), in coordination with the Joint Task Force – Computer Network Defense (JTF-CND), and are pre-coordinated with the Service/Agency Computer Emergency Response Teams (CERTs).

b. IAVAs are promulgated via organizational messaging. The message is for notification only and directs recipients to check the DoD CERT web site (http://www.cert.mil) for technical specifics and corrective action.

c. IAVAs will expire after three years unless otherwise specified and may be modified or superceded as more technical information becomes available.

2. Each Commander-in-Chief (CINC), Military Service and Defense Agency (C/S/A) shall:

a. Designate a primary and secondary point of contact (POC) responsible for IAVA acknowledgment and reporting.

b. Acknowledge receipt of the IAVA notification within five days of the date of the AUTODIN message or within the timeframe specified in the message itself.

c. Disseminate the IAVA via command channels to all program managers (joint and/or C/S/A specific), system administrators, and/or other personnel responsible for implementing and managing technical responses to IAVAs.

d. Report compliance with an IAVA notification via the appropriate IAVA web site within 30 days of the date of the message, or as specified in the individual message. C/S/A-specific program manager reports will be included in the C/S/A overall report. Compliance information shall include at a minimum: number of assets affected, number of assets in compliance and number of assets with waivers. For reporting purposes, assets include all components (i.e., hardware and software) of information systems comprising or accessing a networked environment.

e. Maintain positive configuration control of all information systems/assets under their purview.

f. Maintain configuration documentation that identifies specific system/asset owners and system administrator(s), including applicable electronic addresses.

g. Manage and administer networked assets in a manner allowing for both chain-of-command and authorized independent verification of corrective actions.

h. Modify all DoD asset management contracts to reflect the above requirements. This includes contracts in development that are information technology (IT)-related and/or affect Defense Information Infrastructure (DII) assets (utilizes, administers, or integrates IT and/or communication assets into the DII).

i. Establish a process to periodically review any waivers prior to their expiration date.

3. Designated POCs shall:

a. Register with DISA for assignment of user-ID and password.

b. Enter their organization's acknowledgment and compliance data into the IAVA database.

4. Waivers. Designated Approval Authorities (DAAs) have the authority to waive compliance with a specific IAVA notification, if appropriate, following a risk assessment and determination of other risk mitigating actions. Waivers shall be for the minimum length of time required to achieve compliance with the IAVA notification.

5. Specific technical questions regarding individual IAVAs should be addressed to the DoD CERT via email at cert@cert.mil.