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

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

August 22, 1999

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

SUBJECT: Increasing the Security Posture of the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet)

The security of the Department of Defense's (DoD) information infrastructure is related to protection of the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) against intrusion and malicious activity. Intrusion attempts are expected to increase as hackers may be tempted to masquerade their activities as Year 2000 (Y2K) bugs. Information assurance and network protection efforts hinge on identification, control and management of NIPRNet connections. Of particular interest and concern are the multitude of interconnections between the NIPRNet and the Internet. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988, requires all DoD information systems, including networked computers, to comply with minimum security requirements. These security requirements pertain to any information technology (IT) system(s), regardless of the classification of the data processed.

Defense-in-Depth is the DoD approach to the protection of information systems. This memorandum describes the requirement for a significant piece of the overall DoD Defense-in-Depth strategy. However, DoD Components are cautioned that the protections described in this memorandum are only one layer of Defense-in-Depth and are not in and of themselves sufficient. Components must implement other protections per the Defense-in-Depth strategy as well. The use of firewalls or other technologies to provide higher levels of security between NIPRNet user enclaves is highly recommended.

The guidelines provided in Chairman of the Joint Chiefs of Staff memorandum CM-510-99, "Information Operations Condition" (INFOCON), March 10, 1999, require certain actions to be taken to increase the readiness posture for Information Warfare. Positive control of military connections to the Internet is required to support the setting of INFOCON conditions. This memorandum establishes the DoD policy that the only authorized access to the Internet is via the

NIPRNet. Certain situations may exist where a CINC, Service, or Agency may require a direct connection to the Internet or where near-term migration to the NIPRNet may not be feasible. Therefore, a waiver process shall be established that will consider each exception request individually and allow for the migration of systems to the NIPRNet over time.

The Defense Information Systems Agency (DISA) has established a number of NIPRNet gateways to the Internet, which will be protected and controlled by firewalls and other technologies. The level of protection provided by these, or equivalent, gateways can be increased in response to rising INFOCON conditions. All connections to the Internet, to include those that are provided by NIPRNet or those that have an OSD waiver, must meet or exceed the minimum security requirements contained in the implementation guidance to this memorandum.

Positive control of all NIPRNet-Internet connections is an absolute requirement. All connections to the NIPRNet will comply with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) and be approved via the NIPRNet connection approval process. The implementation guidance accompanying this memorandum recognizes the Defense Information Systems Network (DISN) Security Accreditation Working Group (DSAWG) as the body representing the DISN Designated Approval Authorities for security issues. Chaired by DISA and with representation from the Joint Staff, DISA, Defense Intelligence Agency, National Security Agency, Services, and the Joint Task Force – Computer Network Defense (JTF-CND), the DSAWG will set and maintain firewall policy, protocol controls, and overall minimum network security standards.

Unless specifically excluded below, Components shall terminate all direct connections to the Internet and establish connectivity to the Internet via the NIPRNet. Components shall develop a list of all direct connections with a suggested schedule for transitioning these connections by September 1, 1999. Working with DISA and ASD(C3I), Components will prepare a definitive transition plan by September 30, 1999, though implementation of portions of the plan can begin as early as feasible and agreed to. The goal is to have the transition complete and other protections in place by December 15, 1999, while avoiding operational degradation. Internet connections that cannot be terminated prior to December 15, 1999 or meeting one of the stated exclusions will need a waiver. Waiver requests shall explain how the non-NIPRNet-Internet connections meet the minimum security standards established by the DSAWG and be accompanied by a plan to transition the connection to the NIPRNet. Waiver requests and associated transition plans must be submitted to the DSAWG by October 15, 1999. The Components and DISA will brief the ASD(C3I) on progress and issues on a monthly basis beginning in August 1999. Detailed formats for reporting and waiver requests will be published in the implementation guidelines.

This directive does not apply to direct Internet connections for educational (off-duty or non-duty related) or morale, welfare, and recreational activities. These activities are not required to obtain Internet access via the NIPRNet. However, none of the Internet-connected networks, AISs, or individual computers used at these activities will be further connected to the NIPRNet. Direct connections to the Internet to support electronic commerce are permitted so long as those systems have a waiver or are not also connected to the NIPRNet.

This directive does not prohibit properly protected dial-in or dial-out modem pools, nor does it prohibit properly documented, protected connections to other networks that meet the security requirements of DoD Directive 5200.28 and this memorandum's implementation guidance. For example, interconnections between AISs where the Designated Approval Authorities for each AIS have completed a Memorandum of Agreement that details the interface security requirements are permitted. However, neither modem pools nor connections to other networks can be allowed to introduce backdoors (cross connections between the Internet and the NIPRNet) that weaken the intent of this memorandum. Connections are not permitted to interfere with the JTF-CND's visibility into and control of department connections to the Internet.

Uncontrolled Internet connections pose a significant and unacceptable threat to all DoD information systems and operations. Your continuous and active support is directed in eliminating this threat to the security and operational readiness of the Department. My point of contact in the Technical Services Directorate of the Year 2000 Program Office is Mr. Walter P. Benesch, telephone (703) 602-0983 ext. 129, email: beneschw@osd.pentagon.mil.

Arthur L. Money
Senior Civilian Official