



COMMAND, CONTROL  
COMMUNICATIONS, AND  
INTELLIGENCE

**ASSISTANT SECRETARY OF DEFENSE  
6000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-6000**

JAN 28 2003

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  
COMMANDERS OF THE COMBATANT COMMANDS  
ASSISTANTS TO THE SECRETARY OF DEFENSE  
DIRECTOR, ADMINISTRATION AND MANAGEMENT  
DIRECTORS OF THE DEFENSE AGENCIES  
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE  
DIRECTORS OF THE DOD FIELD ACTIVITIES  
CHIEF INFORMATION OFFICERS OF THE MILITARY  
DEPARTMENTS AND SERVICES  
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS  
AND COMPUTER SYSTEMS, JOINT STAFF  
CHIEF INFORMATION OFFICERS OF THE DEFENSE  
AGENCIES

SUBJECT: DoD Ports, Protocols, and Services - Increasing Security at the  
Internet/DISN Boundary

As we contend with ever-increasing information assurance (IA) challenges, it is imperative that we continue to take measures to minimize the risk to DoD information systems by regulating access between the Internet and defense networks by implementing positive technical controls. Initial (draft) technical guidance for this effort was provided in my November 5, 2002 Memorandum, Subject: DoD Ports, Protocols, and Services Security Technical Guidance.

As the next step in managing the use of ports, protocols and services affecting the security of the Department's information systems and networks, US Strategic Command (USSTRATCOM) has approved the preparation and execution of an action plan to incrementally block selected ports at the gateways between the Internet and the



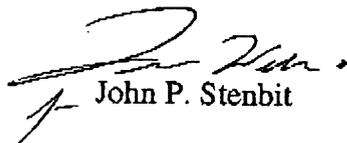
Non-classified Internet Protocol Router Network (NIPRNet). Initial efforts will focus on ports 0-1024. Exceptions will be made for ports approved for routine or emergency use under procedures to be established in the action plan. Initially, the following ports and protocols will be excepted from this blocking:

File transfer protocol data, 20  
File transfer protocol control, 21  
Secure shell, 22  
Simple mail transfer protocol, 25  
Domain Name Service, 53  
http, 80  
Secure http, 443

Within 15 days of the date of this memorandum, addressees are to provide USSTRATCOM's, JTF-CNO POC listed below with a primary and an alternate POC (Name, Organization, Phone, NIPRNet/SIPRNet Address), as well as a list of any additional proposed exceptions, with justification and an assessment of the operational impact if the exceptions are not granted. Initial blocking will begin on or about February 19, 2003. USSTRATCOM, through the Commander, JTF-CNO, will publish a message providing initial implementation guidance.

This action was coordinated with the Joint Staff, USSTRATCOM, the Defense Information Systems Agency (DISA), and the Global Network Operations and Security Center (GNOSC). I ask all addressees to provide their full cooperation in ensuring that all measures directed are expeditiously accomplished in order to minimize the impact of these port closures on your operations

My points of contact for this activity are Mr. Dana Foat in the DIAP at 703-602-9974, dana.foat@osd.mil, and Mr. David Basel at DISA, 703-882-1553, BaselD@ncr.disa.mil. The JTF-CNO POC is the watch officer, DSN: 327-4583, COMM: 703-607-4583, jtfwo@jtfeno.ia.smil.mil.

  
John P. Stenbit

CF:  
US Department of State  
US Department of Justice  
US Department of Commerce  
US Department of Transportation  
General Accounting Office  
General Services Administration  
Federal Aviation Administration  
American Red Cross