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

NOV 5 2002

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 Security Technical Guidance

A team of experts from the Combatant Commands, the Services and Defense Agencies (C/S/A) under the joint leadership of the Defense-wide Information Assurance Program (DIAP) office and the Defense Information Systems Agency (DISA) is developing a DoD Instruction (DoDI 8550.bb) to be published in the first half of CY 2003 that will define and implement a Department-wide ports, protocols and services (PPS) management process. Technical guidance will be an important part of that process and will be formally issued as a part of the instruction to all DoD NIPRNET users. It will also be provided to other government agencies (e.g., USCG, FAA), and selected commercial contractors. The technical guidance will support several important DoD goals, including helping to ensure interoperability across the NIPRNET, mitigating
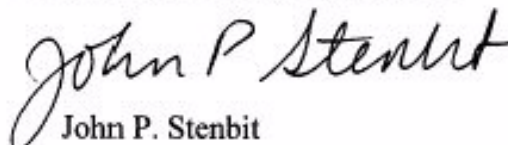
shared risk within the NIPRNET user community, and promoting the creation of a common development environment. The draft guidance at Attachment 1 was developed with input and comment from experts who represent most of the NIPRNET user community.

Attachment 2 is the text of a message dispatched by the Joint Staff (J6K) on September 27, 2002 (DTG 251706Z SEP 02) that provides guidance on firewall "best practices." It also encourages development of a common set of PPS for use across DoD to help ensure security and interoperability while meeting the needs of the C/S/As.

Attachment 1 is the initial effort to develop a common set of PPS for use across DoD. It is being forwarded in advance of formal coordination for implementation where possible in support of Attachment 2, and for further comment. It identifies recommended combinations of PPS for perimeter defense (firewalls, etc.) of enclaves connected to the NIPRNET and for approved direct connections from enclaves to the Internet. It also includes recommended security countermeasures for minimizing the vulnerabilities of risky PPS that that must be used for essential applications.

The technical guidance is intended to improve NIPRNET interoperability by initiating and advocating standard configurations for PPS that may be used with confidence by application owners, application users, and enclave security administrators. I strongly encourage all DoD Components to follow the draft guidance now in order to begin providing common configurations for PPS used to communicate with other users on the NIPRNET. I am aware that following the guidance will result in situations where concessions will have to be made by both functional application developers and enclave owners but, with proper coordination and cooperation, there is much to be gained now at acceptable levels of risk and the lessons learned will greatly assist in developing the formal guidance.

Where the guidance cannot be followed, please provide feedback so that necessary adjustments may be made before formal coordination of the DoD instruction in early CY 2003. My points of contact for this effort are David Basel at DISA, baseld@ncr.disa.mil and CDR Bernadette Semple at the DIAP, bernadette.semple@osd.mil.

John P. Stenbit

Attachments
As stated