DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY
REFER TO: Mission Assurance (MA)

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Interim Guidance for the Utilization of Network
Address Translation in the JRSS architecture

Reference: DoD Instruction 8500.01

DoD Instruction 8500.01 tasks DISA "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cyber security policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders" and DoD Component heads "ensure that all DoD IT under their purview complies with applicable STIGs, security configuration guides, and SRGs.".

Under the authority of DoD Directive 8500.01, DISA is releasing an interim security guidance for the implementation of network address translation (NAT) in the JRSS architecture. NAT, if properly implemented and with adequate log retention and access, does not significantly add risk to the network. The primary concern is rapid attribution of network activity to identify the source or target of attack activity. As stated in current DoD STIGS, NAT is authorized for use on NIPRNet as long as NAT logs are maintained and available to Cyber Defenders. The security benefits of using NAT to mask networks from outside probing are minimal and relatively easy to bypass and should not be considered as a significant part of the DoD security architecture. Use of NAT with JRSS is an acceptable risk.

The above configuration guidance will be included in the STIGs supporting JRSS implementation. This memo serves as interim STIG guidance authorizing NAT as part of the JRSS implementation.

Point of contact for this action is FSO STIG Support Desk, email: disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil.

MARK S. ORNDORFF
Mission Assurance Executive