SCIS (ARNe) Audit Vulnerability Scan Policy

1.0 Purpose
The purpose of this agreement is to set forth our agreement regarding network security scanning offered by the RU IT to the ARNe. RU IT shall utilize open source software to perform electronic scans of ARNe networks and/or firewalls or on any system at ARNe.

Audits may be conducted to:
- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents ensure conformance to ARNe security policies
- Monitor user or system activity where appropriate.

2.0 Scope
This policy covers all computer and communication devices owned or operated by ARNe. This policy also covers any computer and communications device that are present on ARNe premises, but which may not be owned or operated by ARNe. The RU IT will not perform Denial of Service activities.

3.0 Policy
When requested, and for the purpose of performing an audit, consent to access needed will be provided to members of RU IT ARNe hereby provides its consent to allow [Audit organization] to perform the scans authorized in this agreement. ARNe shall provide protocols, addressing information, and network connections sufficient for RU IT to utilize the software to perform network scanning.

This access may include:
- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on ARNe equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on ARNe networks.

3.1 Network Control.
If Client does not control their network and/or Internet service is provided via a second or third party, these parties are required to approve scanning in writing if scanning is to occur outside of the ARNe’s LAN. By signing this agreement, all involved parties acknowledge that they authorize of RU IT to use their service networks as a gateway for the conduct of these tests during the dates and times specified.

3.2 Service Degradation and/or Interruption. Network performance and/or availability may be affected by the network scanning. ARNe releases RU IT of any
and all liability for damages that may arise from network availability restrictions caused by the network scanning, unless such damages are the result of RU IT’s gross negligence or intentional misconduct.

3.3 Client Point of Contact During the Scanning Period. ARNe shall identify in writing a person to be available if the result of RU IT Scanning Team has questions regarding data discovered or requires assistance.

3.4 Scanning period. ARNe and RU IT Scanning Team shall identify in writing the allowable dates for the scan to take place.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History
Version 1.0 9/1/2005
Version 2.0 11/30/2005