



# **NASA Standard Operating Procedure**

## **NASA's Target Vulnerability Selection Procedures**

**ITS-SOP-002**

**Effective Date: June 2003**

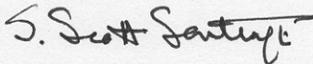
**Expiration Date: July, 2007**

**Responsible Office: AO / Chief Information Officer**

## NASA Target Vulnerability Selection Procedures

The following procedure is used by the CCITS to produce the NASA Vulnerabilities list for the quarterly vulnerability assessment scans used for the Agency-wide IT security vulnerability elimination/mitigation program:

1. Review security bulletins and alerts from SANS, CERT, Security Focus, and NASIRC data and determine what new exploits would most like impact NASA systems. Compare this information to the list of new high vulnerability exploits checks have been added to ISS Internet Scanner since the previous quarter.
2. From these exploits, select those that meet the following criteria:
  - Allows remote attackers to execute commands on the system or gain administrator or root access (e.g., buffer overflows).
  - Does not require administrator privilege to determine if the system is vulnerable.
  - Does not cause a system crash, application crash or denial of service.
3. Review the list from the previous quarter and determine if any vulnerabilities should be removed. Usually vulnerabilities will be removed when all Centers have reported that the vulnerability has been eliminated or mitigated.
4. Once a draft has been compiled, the list is emailed to the Agencywide, [security-tools@lists.arc.nasa.gov](mailto:security-tools@lists.arc.nasa.gov) mailing list for review and comment from the NASA Centers.
5. After comments have been taken into consideration, a final list is produced and is sent to the IT Security managers email list, [itsm@atlas.arc.nasa.gov](mailto:itsm@atlas.arc.nasa.gov), by the CCITS Manager.



S. Scott Santiago  
Acting Deputy Chief Information Officer –IT Security