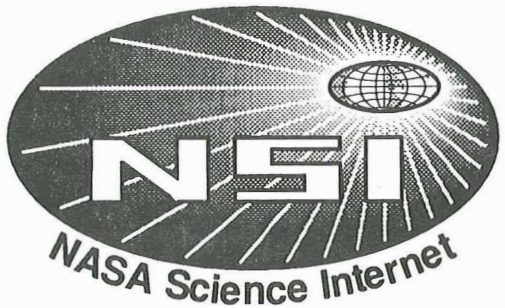

NSI SECURITY TASK
-OVERVIEW-

RON TENCATI

NSI SECURITY MANAGER

NSI USERS' WORKING GROUP

FEBRUARY 1991

SAN MATEO, CA

NSI SECURITY TASK

AS FUNDED FOR FY90:

POLICIES AND SECURITY DOCUMENTATION
RISK ANALYSIS AND MANAGEMENT
COMPUTER EMERGENCY RESPONSE TEAM
INCIDENT HANDLING
TOOLKIT DEVELOPMENT
USER CONSULTING
WORKING GROUPS/CONFERENCES/COMMITTEES

NSI SECURITY TASK

FY90 STRUCTURE:

Reports to NSIPO/ARC Administration

Separate Task Assigned to GSFC

STAFFING:

Security Administrator, NSIPO/ARC - Yvonne Russell

Security Manager, GSFC - Ron Tencati

Other staffing as required by task by either NASA or contractor personnel.

NSI SECURITY TASK

POLICIES AND DOCUMENTATION

The Network Policies and Procedures Define the Official Security Requirements for Computer Systems Comprising NSI.

- Official Policy
- Security Guidelines (UNIX, VMS, DECnet, TCP/IP, X.25)

Allows for the establishment of a "Security Baseline" for the network consistent with Federal Laws and NASA Regulations.

Will Draw Upon Existing Documentation Where Applicable.

NSI SECURITY TASK

RISK ANALYSIS AND MANAGEMENT

Produce NSI Risk Analysis Document. Perform a NETWORK Risk Analysis.

Require Periodic Risk Analysis of Constituent Systems Through Project MOUs. Provide Assistance Where Necessary.

The Computer Security Act of 1987 requires all Federal Computer Systems to perform Risk Assessments at least once every 5 years. Sooner for more sensitive systems.

NIST is under contract with NSI and Code NTD to provide NSI with guidance and assistance in establishing a network risk analysis and management plan.

NSI SECURITY TASK

COMPUTER EMERGENCY RESPONSE TEAM (CERT)

Formed after Morris and WANK Worms hit NSI component networks.

Implements NSI-CERT for distribution of security-related notices, alerts and bulletins, as well as provides for coordinated distribution of software patches.

- Identifies Site Security Contacts
- EMAIL, PHONE and FAX Communication Possible

Interfaces with NASA-wide CERT activity at HQ (Code NTD)

NSI is charter member of Cert System, an International group of Government, Agency and Corporate CERTs.

NSI SECURITY TASK

INCIDENT HANDLING

Provide investigation, coordination, reporting and follow-up for Security incidents.

Provide a place where system managers can report incidents or receive help regardless of operating system.

Interface with NASA Inspector General and other Federal agencies as necessary

NSI SECURITY TASK

SECURITY TOOLKIT SOFTWARE

Provide user community with a set of self-audit tools to improve the security of their systems

Operating -System independent (Two sets of equivalent tools for UNIX and VMS)

Usage endorsed by NSI, recommended by Policy Documentation, but not required for membership in NSI.

FY90: NSI-approved tools first, NSI-developed (maybe) later.

NSI SECURITY TASK

USER CONSULTING

Provide help for users with specific security problems. Receive referrals from NSI User Support Office.

WORKING GROUPS/CONFERENCES/COMMITTEES

Ensure that the security interests of NASA Science Networking are represented as appropriate.

NSI SECURITY TASK

EXTERNAL CONTACTS

Work with, and provide support to other Agencies and NASA Codes to facilitate a common Agency-wide approach to computer security.

NIST:

Under contract by NSI and Code NTD to assist NASA in addressing various computer security issues.

- Analyze NSI and SPAN Risk Management Plans, Recommend modifications to allow NSI approach to match NASA AIS Program.
- Idenfify network threats, survey existing toolkits (NSI and public domain, make recommendation for NSI strategy.
- Review NASA Incident Response Capabilities, assist in the establishment of a NASA agency-wide CERT Capability.

NSI is being used as the model for NASA networks