

Security Plan for the Network Control Center, NCC 98

April 1998



National Aeronautics and
Space Administration

————— Goddard Space Flight Center —————
Greenbelt, Maryland

Security Plan for the Network Control Center, NCC 98

April 1998

Prepared by:



Jon Arneson 4/14/98 Date
Senior Principal Engineer
Computer Sciences Corporation

Submitted by:



Roger Clason 4/14/98 Date
NCC Management Group
Code 451

Approved by:



Ron Dill 4/16/98 Date
Consolidated Network and Mission Operations
Support (CNMOS)
Information Technology Officer
Code 450.9

Preface

This Security Plan describes the security posture of the Network Control Center, as updated by the NCC 98 Project. NCC 98 is an update of the Network Control System Data System (NCCDS). NCC 98 comprises new elements—the Service Planning Segment Replacement, the Network Protocol Gateway, the Network and System Manager, the NCC Firewall, and the Small Conversion Device—as well as updates to the Communications and Control Segment, the Service Accounting Segment, and the Automated Conflict Resolution System. NCC 98 addresses new requirements for enhanced network scheduling capability, communications via the internet protocol (IP), and security in an IP environment.

This document represents the highest-level security plan for NCC 98.

Information presented herein was prepared by the Network Control Center Management Group, Code 451.5, Goddard Space Flight Center. Any questions, recommended changes or comments should be directed to:

Network Control Center Management Group
Code 451.5
Goddard Space Flight Center
Greenbelt, Maryland 20771

Abstract

This Security Plan describes the security posture of the Network Control Center, as updated by the NCC 98 Project. NCC 98 is an update of the Network Control System Data System. NCC 98 addresses new requirements for enhanced network scheduling capability, communications via the internet protocol (IP), and security in an IP environment.

This document represents the highest-level security plan for NCC 98.

Keywords: Network Control Center, Security.

Contents

Preface

Abstract

SECTION 1— SYSTEM IDENTIFICATION

1.1 Responsible Organization.....	1-1
1.2 System Name/Title	1-1
1.3 System Category	1-1
1.4 System Operational Status.....	1-1
1.5 General Description/Purpose.....	1-1
1.6 System Environment and Special Considerations	1-1
1.7 Information Contacts	1-2

SECTION 2— SENSITIVITY OF INFORMATION HANDLED

2.1 Applicable Laws and Regulations Affecting the System	2-1
2.2 General Description of Information Sensitivity	2-1
2.2.1 Confidentiality	2-1
2.2.2 Integrity	2-1
2.2.3 Availability	2-1
2.2.4 Statement of Impact	2-2

SECTION 3— SYSTEM SECURITY MEASURES

3.1 Risk Assessment and Management	3-1
3.2 Applicable Guidance	3-1
3.3 Security Control Measures for Major Applications	3-1
3.3.1 Management Controls	3-1
3.3.2 Development/Implementation Controls	3-2
3.3.3 Operational Controls	3-3

3.3.4 Security Awareness And Training..... 3-3
3.3.5 Technical Controls 3-4
3.3.6 Complementary Controls Provided By Support Systems..... 3-4

Appendix A NCC 98 Delivery Letter [TBS]

Abbreviations and Acronyms

SECTION 1—SYSTEM IDENTIFICATION

1.1 Responsible Organization

Network Control Center (NCC) Management Group
Code 451.5
Goddard Space Flight Center
Greenbelt, MD 20771

1.2 System Name/Title

Network Control Center 1998 (NCC 98)

1.3 System Category

Major Application

1.4 System Operational Status

Undergoing Major Modification

1.5 General Description/Purpose

The Network Control Center (NCC) is an element of the National Aeronautics and Space Administration (NASA) Spaceflight Tracking Data Network (STDN). The STDN uses the Tracking and Data Relay Satellites (TDRSs) as the primary source of support for customer spacecraft. The STDN includes the TDRSs, the ground stations of the Space Network and the Ground Network. The NCC is responsible for network scheduling, acquisition support, data quality assurance, performance monitoring, and overall coordination of the STDN. The NCC is responsible for scheduling and controlling the Space Network and residual portion of the Ground Network. NCC 98 means the NCC as it will exist when the Service Planning Segment Replacement (SPSR) and other related new elements become operational. The NCC 98 development project is the first step toward migrating the present proprietary NCC Data System (NCCDS) to an open system featuring a client/server architecture, substantial use of commercial-off-the-shelf products, and industry-standard communications protocols. Ancillary systems to support operations are being upgraded to assure compatibility with NCC 98

1.6 System Environment and Special Considerations

a. Architecture

NCC 98 is a major step in the transition from a mainframe-based architecture to a client-server architecture. The single most significant part of this transition is the replacement of the Service Planning Segment. NCC 98 will also provide a

completely new graphical user interface for the NCC operators, and a completely new Network and Systems Management element for the internal control of the NCC. However, NCC 98 will still include legacy elements such as the Communications and Control Segment and the Service Accounting Segment. Also, the Restricted Access Processor is being replaced by a firewall.

b. Functions

NCC 98 will provide functional improvements in several areas. Some of these are intended to simplify internal NCC operations. Major external functional improvements include providing greater scheduling flexibility for Space Network customers, and support of the next generation of TDRSs.

c. Interfaces

In conjunction with Nascom's IP transition, NCC 98 will utilize TCP/IP, UDP/IP, and FTP protocols for external communications. NCC 98 will also include a world-wide web (WWW) site for SN customer access to TDRS Unscheduled Time (TUT) information. However, NCC 98 will continue to support legacy Nascom 4800 bit block (bb) interfaces and will provide the option of full backwards compatibility for legacy customers.

d. Physical environment

The system resides in an environmentally controlled area. There are no special environmental concerns other than clean air, temperature and humidity.

1.7 Information Contacts

Lynn Myers, Code 451.5 301-286-6343

Reine Chimiak, Code 583 301-286-3469

SECTION 2—SENSITIVITY OF INFORMATION HANDLED

2.1 Applicable Laws and Regulations Affecting the System

There are no specific laws affecting the operation of the system.

2.2 General Description of Information Sensitivity

The NCC 98 handles planning and real-time data. Planning data includes schedules and schedule updates. Real-time data includes changes in configuration, acquisition data, and service performance reports.

2.2.1 Confidentiality

- a. Low—There is no information residing on the system or being transmitted by the system that requires protection from unauthorized disclosure.
- b. Exception: Information used by the system or its communicants to authenticate identity or detect modification (e.g., passwords and cryptographic variables) will have HIGH confidentiality requirements. Compromise of the confidentiality of this information could result in loss of data integrity and/or system availability.

2.2.2 Integrity

High—It is absolutely necessary that the data be accurate and protected from accidental or unauthorized modification. The system controls the scheduling and operational parameters of spaceborne and terrestrial communication data relay resources for multiple space missions. Corruption of the accuracy of NCC data at critical times could seriously jeopardize the success of those space missions.

2.2.3 Availability

- a. High - The system has to be available at all times. The design specification states that NCC 98 shall provide an availability of 0.9998 for the critical support functions, and 0.9990 for the non-critical functions. The system controls the scheduling and operational parameters of spaceborne and terrestrial communication data relay resources for multiple space missions. Unavailability of NCC functions at critical times could seriously jeopardize the success of those space missions.
- b. The design specification also requires a mean time between failures of at least 2500 hours for critical support functions and 1000 hours for non-critical support functions.

2.2.4 Statement of Impact

- a. Space Network services provide for telecommunications between customer spacecraft operations control centers and the customer spacecraft. The NCC schedules, reschedules, monitors, and provides fault isolation of these services.
- b. Loss of NCC capabilities in the short term causes inability to change or reconfigure scheduled and active services and loss of "quality" data concerning the scientific and housekeeping data.
- c. Loss of the NCC would impact real time changes to customer services.

SECTION 3—SYSTEM SECURITY MEASURES

3.1 Risk Assessment and Management

Information is currently being gathered to perform a risk assessment.

3.2 Applicable Guidance

- NASA Handbook 2410.9A, NASA Automated Information Security Handbook, June 1993
- Goddard Space Flight Center Handbook, GHB 1600.1A, Security Manual, Nov 1990

3.3 Security Control Measures for Major Applications

In Place Planned N/A

3.3.1 Management Controls

- | | |
|--|---|
| a. Assignment of Security Responsibility | X |
| Keiji Tasaki/Code 450, Data Processing Installation Information Technology Security Officer for Code 450 | |
| b. Personnel Screening—All personnel are required to have National Agency Checks prior to being granted access privileges to the Network Control Center. | X |

3.3.2 Development/Implementation Controls

- | | | |
|----|--|---|
| a. | Security Specifications—Specifications assuring the confidentiality, integrity and availability were derived from NHB 2410.9A and GHB 12600.1A and are throughout the system requirements documentation, (530-SRD-NCCDS/1998), but are not separately identified as security requirements. | X |
| b. | Design Review and Testing—A detailed system test plan has been developed. Security related items affecting the reliability or integrity of the information residing on or being transmitted by the system are considered an integral part of the overall system and are included in any testing. In addition, specific security related items are included as part of the acceptance testing | X |
| c. | Certification—The NCC is a NASA Sensitivity Level-3 system. All Level-3 systems require recertification at least yearly and after any major modification. Certification is scheduled to be completed prior to the system becoming operational. | X |

3.3.3 Operational Controls

a.	Physical and Environmental Protection—Permanent employees are issued badges and proximity cards for access. Physical access for others is controlled by signing in (registering) with the guard, issuance of a specific badge for the NCC, and issuance of a proximity badge. The badges have to be turned into the guard upon departure. All unauthorized personnel have to be escorted at all times.	X		
b.	Production, I/O Controls—			X
c.	Emergency, Backup and Contingency Planning—The system has two backup capabilities. The NCC personnel practice the backup procedure every week to the primary backup and at least every six weeks to the secondary backup. The system also has a diesel powered backup generator.	X	X	
d.	Audit and Variance Detection—Each subsystem logs all incoming and outgoing messages. Alerts are provided to the operators for time-critical and security-related messages. Weekly service accounting reports are generated and compiled into monthly reports.	X	X	
e.	Application Software Maintenance Controls—The controls used to monitor the installation of and updates to application software and to assure a historical record is maintained of application system changes are documented in the “Network Control Center 1998 Configuration Management Plan,” 530-CMP-NCC 98.	X		
f.	Documentation— Network Control Center Standard Operations Procedures, volumes 1 and 2, June 1997.	X	X	

3.3.4 Security Awareness And Training

a.	Security Awareness and Training Measures—			X
----	---	--	--	---

3.3.5 Technical Controls

- | | | | |
|----|---|---|---|
| a. | Identification and Authentication—“Operator” physically within the NCC refers to any individual who may access the NCC 98. It never refers to any individual or system external to the NCC. NCC 98 will restrict individual operator access to system resources and functional capabilities. The system shall provide for automated logout of operators who have been inactive for an administratively selectable time period. | X | X |
| b. | Authorization/Access Control & Privileges—NCC 98 will utilize a firewall to enforce the external communications connectivity and audit policy requirements. A detailed description of the firewall rules can be found in the NCC 98 Delivery Letter, Appendix A. | | X |
| c. | Data Integrity/Validation Controls— | | |
| | 1. Password-like secret authenticators together with error detection. | X | |
| | 2. Encryption codes will be used to protect against data alteration and source impersonation for communications with the White Sands Complex and the Special Projects and Missions customer. No other customer has indicated willingness to use encryption. The NCC will not provide encryption for these customers. In addition, the NCC will not use encryption within the environment enclosed by the firewalls and dedicated small conversion devices (SCDs). These devices provide sufficient protection and the added cost of internal encryption would not be justified. | X | X |
| d. | Audit Trails and Journaling—The NCC shall have the capability to selectively record the passage or attempted passage into or out of NCC of low-level datagram or message block protocol data units (PDUs). The NCC shall have the capability to selectively record the actions of operators. | X | X |

3.3.6 Complementary Controls Provided By Support Systems

X

Abbreviations and Acronyms

ATSC	AlliedSignal Technical Services Corporation
bb	bit block
CMP	configuration management plan
CNMOS	Consolidated Network and Mission Operations Support
FTP	file transfer protocol
GHB	Goddard handbook
GSFC	Goddard Space Flight Center
I/O	input/output
IP	internet protocol
NASA	National Aeronautics and Space Administration
NCC	Network Control Center
NCCDS	Network Control Center Data System
NHB	NASA Handbook
PDU	protocol data unit
SPSR	Service Planning Segment Replacement
SRD	system requirements document
STDN	Spaceflight Tracking and Data Network
TBS	to be supplied
TCP/IP	transmission control protocol/internet protocol
TDRS	Tracking and Data Relay Satellite
TDRSS	Tracking and Data Relay Satellite System
TUT	TDRS unscheduled time
UDP/IP	user datagram protocol/internet protocol
WWW	world-wide web