

DRAFT

492-MOC-008

**Gamma-Ray Large Area
Space Telescope
(GLAST)
Project**

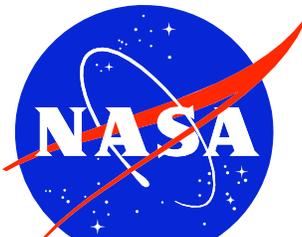
***Mission Operations Center
Security Plan***

492-MOC-008

Draft

Version 0.01

August 13, 2004



GODDARD SPACE FLIGHT CENTER
GREENBELT, MARYLAND

Administratively Controlled Information

This document contains sensitive information and shall be handled in a way that precludes its disclosure to the general public and limits its circulation. NASA entities must attach the NASA Form 1686, Administratively Controlled Information (ACI) form to the cover of this document.

Prepared by:

Jonathan DeGumbia Date
GLAST MOC Systems Engineer
Omitron Inc.

Approved by:

Dennis Small Date
GLAST MOC Lead
GSFC Code 584

Approved by:

Ken Lehtonen Date
GLAST Ground System and Operations Manager
GSFC Code 584

Approved by:

Howard Dew Date
GLAST Ground System Engineer
GSFC Code 586

Preface

This document provides a Security Plan for the GLAST Mission Operations Center (MOC) at Goddard Space Flight Center, Greenbelt, MD.

This document is under configuration control of the GLAST Ground System Configuration Control Board. Changes to this document will be issued by Document Change Notice (DCN) or, where applicable, by complete revision. All questions, recommended changes, or comments concerning this document should be addressed to:

Howard Dew

GLAST Security Manager

Code 586

GSFC Space Flight Center

Greenbelt, Maryland 20771

Change Information Page

List of Effective Pages			
Page Number		Issue	
Document History			
Document Number	Status/Issue	Publication Date	CCR Number
492-MOC-008	Initial Draft	8/13/2004	N/A

Table of Contents

1	SYSTEM IDENTIFICATION.....	1
1.1	RESPONSIBLE ORGANIZATION.....	1
1.2	SCOPE.....	1
1.3	SYSTEM NAME/TITLE.....	1
1.4	SYSTEM OPERATIONAL STATUS.....	1
1.5	GENERAL DESCRIPTION/PURPOSE OF SYSTEM.....	2
1.5.1	<i>GLAST MOC External Connections</i>	2
1.5.2	<i>MOC Network Architecture</i>	3
1.6	SYSTEM ENVIRONMENT AND SPECIAL CONSIDERATIONS.....	5
1.7	POINTS OF CONTACT.....	5
2	SENSITIVITY OF INFORMATION HANDLED.....	6
2.1	APPLICABLE LAWS/REGULATIONS AFFECTING THE SYSTEM.....	6
2.2	INFORMATION CATEGORY AND SENSITIVITY.....	6
2.2.1	<i>Mission Information (MSN)</i>	6
2.2.2	<i>Scientific, Engineering, and Research (SER) Information</i>	6
2.3	IMPACT OF LOSS OF SYSTEM OR DATA.....	7
2.4	SYSTEM VALUE.....	7
3	SYSTEM SECURITY MEASURES.....	8
3.1	INFORMATION SHARING.....	8
3.2	RISK ASSESSMENT AND ANALYSIS.....	9
3.3	TECHNICAL CONTROL MEASURES.....	9
3.3.1	<i>Physical Access</i>	9
3.3.2	<i>Environmental Protection</i>	10
3.3.3	<i>Software Controls</i>	10
3.3.4	<i>Network Access Controls</i>	10
3.3.5	<i>Public Access Controls</i>	11
3.4	ACCOUNT/APPLICATION ACCESS RULES.....	11
3.5	PERSONNEL SCREENING.....	13
3.6	SPECIALIZED TRAINING.....	13
3.7	CONTINGENCY PLANNING.....	13
3.8	INCIDENT RESPONSE.....	14
3.9	SYSTEM INTERCONNECTION.....	14
3.10	REVIEW OF SECURITY CONTROLS.....	15
3.11	AUTHORIZATION TO PROCESS.....	15
3.12	SECURITY DOCUMENTATION.....	15
	APPENDIX A RESPONSIBILITIES.....	17
A.1.1	GLAST SECURITY MANAGER.....	17
A.1.2	GLAST SECURITY OFFICER.....	17

A.1.3 GLAST COMMUNICATIONS ENGINEER17
A.1.4 SYSTEM USERS18
APPENDIX B ABBREVIATIONS AND ACRONYMS19

Table of Figures

[FIGURE 1 GLAST GROUND SYSTEM NETWORK ARCHITECTURE](#)..... 3
[FIGURE 2 GLAST MOC NETWORK ARCHITECTURE](#) 4

Table of Tables

[TABLE 1 SECURITY DOCUMENTATION](#)..... 6
[TABLE 2 INFORMATION SHARING](#)..... 8

1 System Identification

1.1 Responsible Organization

The organization responsible for monitoring and ensuring the compliance of the Gamma ray Large Area Space Telescope (GLAST) Project with National Aeronautics and Space Administration (NASA) security policy is the GLAST Project Office, Code 492, NASA, Goddard Space Flight Center (GSFC), Greenbelt, Maryland.

1.2 Scope

This document provides the security plan of the GLAST Mission Operations Center (MOC) contractor, Goldbelt Orca, for security compliance of the GLAST MOC with NASA security requirements, pursuant to deliverable requirements of the GLAST MOC contract **NAS5-xxxxxx**. This plan will be incorporated into an overall Security Plan, Risk Management Plan, and Contingency Plan for the GLAST mission, under development by the GLAST Project ground system team.

1.3 System Name/Title

This document details the security plan for the system known as the GLAST MOC. The GLAST MOC, for the purposes of this document, collectively includes all of the hardware, software applications, data, and data connections contained within the GLAST MOC facility as defined in section 1.6 of this document. This facility is the main command center for the GLAST observatory and will command and receive telemetry from GLAST through the Tracking Data Relay Satellite System (TDRSS) and the Universal Space Network (USN) ground stations from launch throughout mission life.

1.4 System Operational Status

The GLAST MOC is not currently operational. As of the date of this document, the hardware, software applications, data, and data connections, to be referenced collectively as MOC equipment, have not been installed within the operational environment in the GLAST MOC. The MOC equipment will begin to be populated in the GLAST MOC over several months leading up to the first Ground Readiness Test (GRT). The GLAST MOC will not be considered operational until the ground system freeze, currently scheduled for December 28, 2006, prior to launch on February 28, 2007.

The practices defined in this security plan will be applied from the time the first piece of MOC equipment is installed in the GLAST MOC until the end of the 5 year (10 year goal) mission.

1.5 General Description/Purpose of System

The purpose of the GLAST MOC is to provide the means to perform observatory commanding, telemetry and science data processing, and mission planning activities for the GLAST project.

The GLAST MOC equipment will have three external connections, one to the Restricted Internet Protocol Operational Network (IONet) segment of the NASA Integrated Services Network (NISN), one the Closed IONet segment of the NISN, and one to the GSFC Center Network Environment (CNE).

1.5.1 GLAST MOC External Connections

The GLAST MOC will be connected to the Restricted IONet segment of the NISN. This connection will be used to access the White Sands Complex (WSC) near Las Cruces, New Mexico and the USN Network Management Center (NMC) in Horsham, Pennsylvania to send and receive observatory command and telemetry as well as ground station directives and status messages.

The GLAST MOC will also be connected to the Closed IONet segment of the NISN. This connection is needed to establish a socket connection from the GLAST Front End Processor (GFEP) which is connected to the Closed IONet to the MOC network segment that is connected to the Restricted IONet. The GFEP is located at the WSC.

In addition, the GLAST MOC will be connected to the CNE. This connection will be used primarily to communicate mission planning and data products with the other ground system elements and interested personnel via the World Wide Web (WWW).

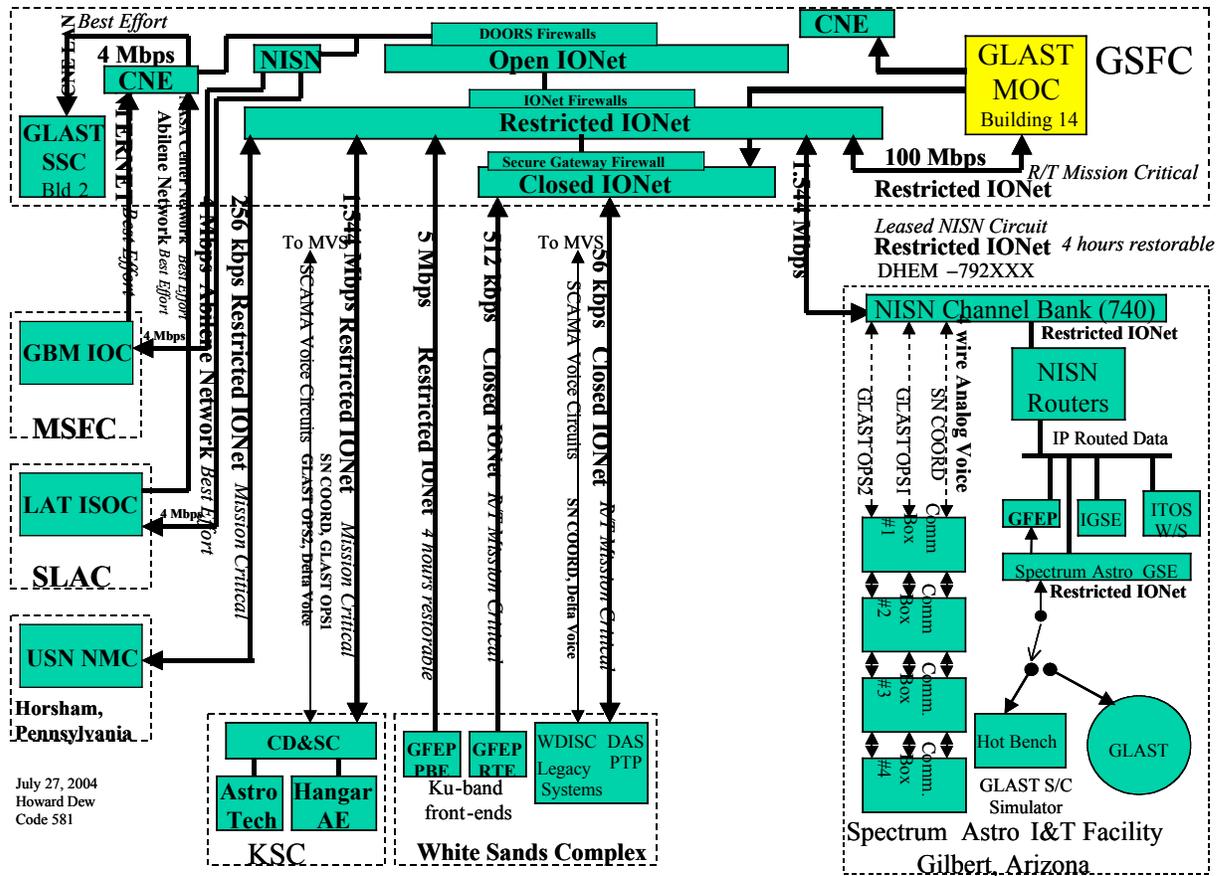


Figure 1 GLAST Ground System Network Architecture

1.5.2 MOC Network Architecture

The MOC network architecture consists of three independent segments. These are known as the MOC CNE Segment, the MOC Restricted IONet Segment, and the MOC Closed IONet Segment. There are no direct connections between any of these segments.

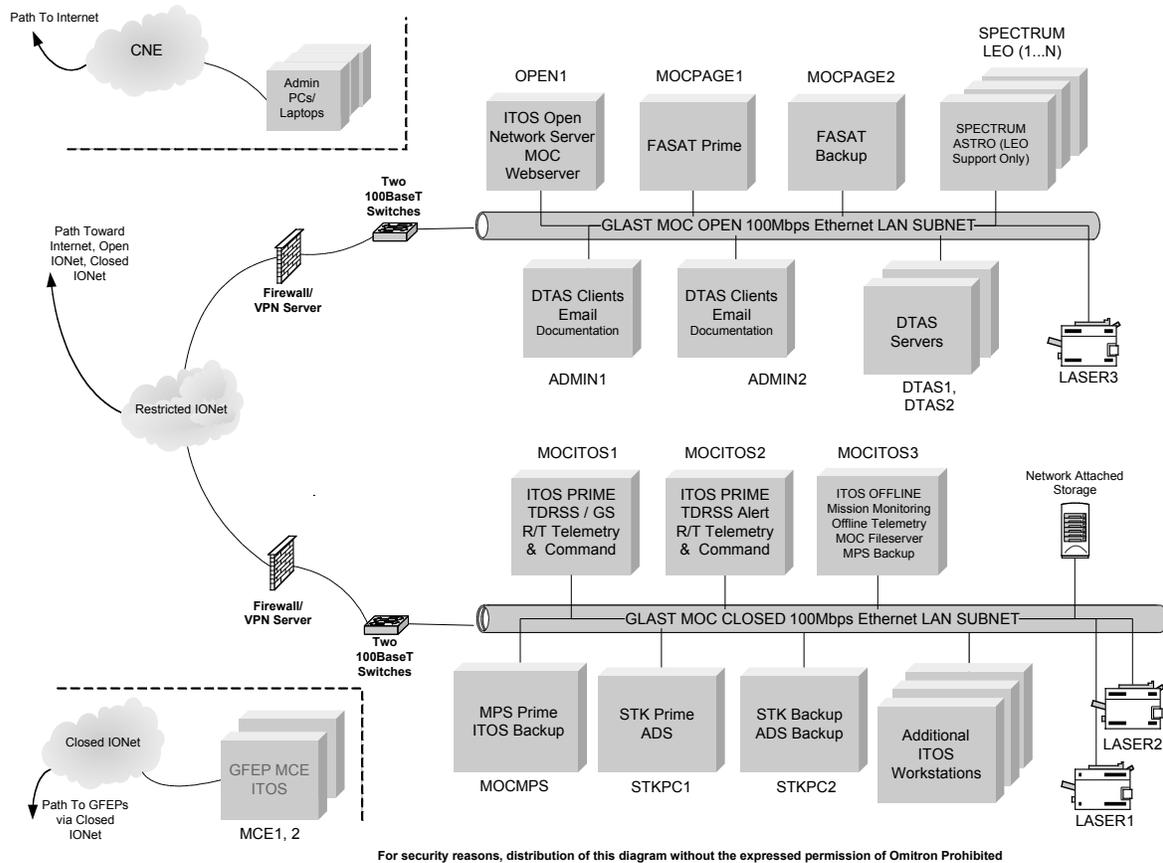


Figure 2 GLAST MOC Network Architecture

The primary purpose of the CNE segment is to allow non-operational WWW access for various computers in the GLAST MOC. This will allow temporary GLAST personnel to use their own laptops to access email other internet functions from within the MOC during Launch and Early Orbit (L&EO). Computers on the CNE segment will not have any direct connections to any other MOC network segment.

The MOC Restricted IONet Segment is where the primary GLAST MOC functions are performed. It is split into two independent Ethernet Local Area Network (LAN) subnets. The MOC Closed Subnet is to connect the MOC equipment necessary to send commands to the observatory; receive, process, and archive observatory science and housekeeping data; and provide mission planning functions. The Closed Subnet is connected to the Restricted IONet and protected by a firewall / Virtual Private Network (VPN) server. The MOC Open Subnet will be used to connect to the WWW. This connection will allow mission operations products and data to be communicated between the GLAST MOC and ground system elements and personnel. In addition, the Open Subnet will be a connection point for additional workstations that will be used to monitor observatory telemetry during L&EO. The Open Subnet is also connected to the Restricted IONet and protected by a firewall/VPN server. All information passed

between the Open and Closed subnets is routed through the Restricted IONet. There are no direct connections between the Restricted IONet Segment and any other MOC network segment.

The MOC Closed IONet Segment will be used establish the connection from the GFEP located at WSC to the MOC Closed Subnet. In addition, the MOC Closed IONet Segment will be used to remotely perform sustaining engineering tasks on the GFEP. There are no direct connections between the Closed IONet Segment and any other MOC network segment.

1.6 System Environment and Special Considerations

The GLAST MOC is located in rooms N285, N287, and N291 of Building 14 at GSFC in Greenbelt, Maryland for the life of the GLAST mission. In addition, rooms E295A, E295B, and E295C will be considered part of the GLAST MOC until the end of L&EO operations.

1.7 Points of Contact

The points of contact for security considerations are:

Howard Dew

GLAST Security Manager
Code 586
Goddard Space Flight Center
Greenbelt, Maryland 20771
301-614-5329

Dustin Aldridge

GLAST MOC Security Officer
Omitron, Inc.
7051 Muirkirk Meadows, Suite A
Beltsville, Maryland 20705
301-474-1700

Bernard Tomardy

GSFC Security Officer
Code 297
Goddard Space Flight Center
Greenbelt, Maryland 20771
301-286-8089

2 Sensitivity of Information Handled

2.1 Applicable Laws/Regulations Affecting the System

Due to its design, the GLAST MOC is subject to various special security restrictions and/or procedures. The following table identifies the key security design aspects of the GLAST MOC and the documentation that provides the details of the security restrictions and/or procedures.

Table 1 Security Documentation

Security Drivers	Applicable Documentation
GLAST MOC's connection to the Restricted IONet	290-004, IONet Access Protection Policy and Requirements Document
GLAST MOC's connection to the Closed IONet	290-004, IONet Access Protection Policy and Requirements Document
GLAST MOC's connection the CNE	???
GLAST MOC's use of the NASA Communications (Nascom) system	541-107, NASA Communications (Nascom) Access Protection Policy and Guidelines

Goldbelt Orca/Omitron is working with the appropriate governing authorities, as necessary, to ensure compliance with their security requirements.

2.2 Information Category and Sensitivity

Information received, stored, processed, and distributed by the GLAST MOC falls into the Mission (MSN) and Scientific, Engineering, and Research (SER) categories as defined by NASA Procedures and Guidelines (NPG) 2810.1.

2.2.1 Mission Information (MSN)

The GLAST MOC MSN includes the software applications and configuration data that allow the GLAST MOC to perform all of its functions as well as any health and safety information generated by the observatory and relayed to the GLAST MOC.

2.2.2 Scientific, Engineering, and Research (SER) Information

The GLAST MOC SER includes the science data generated by the Large Area Telescope (LAT) and Gamma-ray Burst Monitor (GBM) instruments and relayed to the GLAST

MOC. This information is not considered to be sensitive in nature; the data are free and available to everyone who is interested.

2.3 Impact of Loss of System or Data

The impact of the loss or corruption of GLAST MOC data varies with the type and amount of data involved. Impacts could range from no impact to a complete, but temporary, loss of the MOC's ability to perform its primary functions or a permanent loss of observatory data.

Equipment redundancy, data duplication, and off-site storage ensure insure that the probability of any permanent loss of GLAST MOC systems or data is extremely low.

2.4 System Value

The estimated cost for a system rebuild and replacement is **TBD**; it will be included in the GLAST Information Technology (IT) Risk Management Plan.

3 System Security Measures

3.1 Information Sharing

A subset of the GLAST MOC information will be shared with external GLAST ground system elements and interested personnel. The interfacing GLAST ground system elements are the GLAST Science Support Center (GSSC), the LAT Instrument Science Operations Center (LISOC), the GBM Instrument Operation Center, Kennedy Space Center (KSC), USN, and WSC. The shared information is limited to the data generated by the GLAST observatory and mission planning products generated by the MOC. These include both the MSN and SER.

Regardless of its sensitivity level, shared information will be made available only to external entities authorized to receive it. The following table provides a summary of the shared information and external entities that will be authorized to access it. A complete listing of all shared information may be found in the *GLAST MOC System Design Specification* document.

Table 2 Information Sharing

Information	GSSC	LISOC	GIOC	KSC	USN	WSC	Authorized Web Users
Level 0 Data	Y	Y	Y				Y
Realtime Housekeeping Telemetry			Y				
Burst Alert Telemetry	Y		Y				
Mission Planning Products	Y	Y	Y		Y	Y	Y
Observatory Commands				Y	Y	Y	
Ground System Directives					Y	Y	

Level 0 data is comprised of observatory generated engineering and science data that is relayed to the GLAST MOC and then processed into its level 0 form.

Realtime housekeeping telemetry is comprised of observatory generated engineering data that is relayed to the GLAST MOC.

Burst alert telemetry is comprised of observatory generated science data that is relayed to the GLAST MOC.

Mission planning products is comprised of various MOC generated products used for the purpose of mission planning.

Spacecraft commands are comprised, in part, of the bit patterns that are used command the GLAST observatory.

Ground system directives are comprised of the bit patterns that are used to control the functions of the ground systems.

3.2 Risk Assessment and Analysis

Risk assessment and analysis will be performed to determine the susceptibility of the GLAST MOC to a degradation of the integrity, availability, and confidentiality of hardware, software applications, data, and data connections contained within the GLAST MOC facility.

The complete risk assessment for the GLAST facilities, once completed, will be contained within the *GLAST IT Risk Management Plan*.

3.3 Technical Control Measures

Security controls are put in place to enforce the rules policies of the GLAST MOC. Controls may take the form of management activities as well as technical controls. This section describes the measures (in place or planned) that will meet the protection requirements of the system.

3.3.1 Physical Access

Physical access to the MOC facility is limited by electronic keycard devices. Only personnel with keycards will be allowed unescorted access into this facility. Access to the MOC will be monitored by GLAST MOC personnel and this facility will be manned 24 hours per day, 7 days per week during L&EO and 8 hours per day 5 days per week thereafter. GLAST personnel manning the MOC will challenge any individual entering the MOC if not recognized. GLAST keeps a list of personnel who have submitted and/or

passed a National Agency Check (NAC). This list will be used to determine access to any GLAST MOC equipment.

3.3.2 Environmental Protection

The GLAST MOC facility contains smoke detectors and has a dedicated Heating, Ventilation, and Air-conditioning (HVAC) system. Emergency lighting is provided and a sprinkler system is in place.

3.3.3 Software Controls

Procedural controls will require all software applications to be reviewed by the Security Officer and the System Administrator prior to being installed by the System Administrator. All Commercial-Off-The-Shelf (COTS) software will be licensed for use and all custom software will be tested and integrated before being made operational. All software security patches will be updated as mandated by the appropriate governing policies. The system administrator will maintain a spreadsheet of the version of all the applications, code, and operating systems utilized in this facility. This spreadsheet will be used to confirm the latest patches and security issues are kept up to date.

All personnel using this facility will have signed the appropriate Rules of Behavior for IONet. All personnel using this facility will use the Applied Engineering and Technology Directorate (AETD) Rules of Behavior. Access to sensitive application will be restricted through the use of password protection.

All GLAST MOC applications and data will be duplicated and stored off-site.

3.3.4 Network Access Controls

Firewalls will restrict access from computers in the MOC facility to the IONets. Control of observatory commands and telemetry is maintained requiring IP sessions to be originated by known IP hosts outside of the GLAST MOC. All command and telemetry paths are restricted to between the MOC and either the WSC or the USN Ground Stations.

Only the facility Security Officer and facility System Administrator will have the privilege to view or modify the rule set of the firewalls contained in the GLAST MOC. Changes to the rule sets will be communicated to the GSFC Security Office within 7 calendar days of the change. The firewall system logs, which detail system activity, will be provided automatically by the firewall. Event logs will be reviewed routinely by the Security Officer to ensure that no actions have occurred that affected the security of the system.

3.3.5 Public Access Controls

3.3.5.1 Virtual Access Controls

General public access is limited to a Hyper-Text Transfer Protocol (HTTP) communications and trusted Transmission Control Protocol (TCP)/IP sockets. Connections to the web server are a result of pushed data to the server with no return data paths/sessions. All other outside access requires IP address verification of a trusted host and rules allowing access through the firewall. The MOC will use VPN in the MOC firewall for network discrimination.

3.3.5.2 Physical Access Controls

Visitors physically visiting the facility will be escorted at all times and will be identified with ESCORT REQUIRED name tags. They will be kept away from the computer equipment by the escort. During times of non-occupation by the operations personnel, visitors will be prevented from entering the facility by a keycard reader.

3.4 Account/Application Access Rules

The following procedures will be used for securing access to IONet Restricted and OPEN connected computer systems for all the GLAST facilities:

- a. Sessions with an IONet CLOSED host shall always be initiated by the closed host with pre-defined firewall rules through the IONet gateway firewall entered by the closed organization
- b. Passwords using a minimum of 8 characters including three of the four categories: upper case letters, lower case letters, special characters and numbers.
- c. Group passwords shall only be used for the GLAST MOC personnel for operations between shifts and not by instrument users or spacecraft monitors.
- d. Passwords shall be unique to each account.
- e. User Identifications (IDs) shall be verified annually.
- f. All unused accounts shall be removed as soon as possible following testing phases.
- g. A minimum number (5 or less) of personnel shall have access to root passwords, and in no case shall foreign nationals have root privilege or super user privilege.
- h. Passwords for privileged accounts will be changed automatically by the system administrator every 30 days.

- i. Passwords for non-privileged accounts will be changed automatically by the system administrator every 90 days.
- j. Accounts shall be disabled 30 days after the password change period and require re-certification of the User ID for re-establishment.
- k. Operating Systems shall be kept up to date for security patches and other access vulnerabilities.
- l. Hosts shall disable unused services and ports.
- m. The use of Remote Login (RLOGIN), Remote Shell (RSH), Telnet, and File Transfer Protocol (FTP) shall be prohibited in or out of the facility firewall.
- n. Only TCP/IP sockets to specific trusted host IP addresses shall be allowed through to specific IP addresses of hosts behind the facility firewall.
- o. All personal computer software media being brought into a facility shall be checked by the anti-virus programs first before being allowed to be inserted into a facility computer. The Security Officer shall either do this personally or have a designated person do this function for the facility.
- p. The Firewall deny-based rule set shall be maintained only by the facility Security Officer or backup Security Officer (when so designated).
- q. Changes to firewall rules shall be communicated to the GSFC Security Office within 7 calendar days following the change by the facility Security Officer or backup Security Officer (when so designated).
- r. Logs shall be maintained for the following hosts and activities: firewall, super user logins, root usage, access failures to systems, files, objects and resources.
- s. If a host has anti-virus software available to the operating system, it shall be updated at least weekly.
- t. No modems shall be used in any of the GLAST facilities.
- u. If a host is suspected of being compromised, the facility Security Officer shall notify the GSFC Inspector General and the GSFC Security Office of the suspected event as soon as possible.
- v. No hosts in the facility except for the facility firewall and backup facility firewall shall have more than 1 network interface card.
- w. At no time shall a computer be moved from a network to the IONet Restricted or OPEN network until scanned by the GSFC Security Office before connection.

- x. International LAN connections are considered to be untrusted networks.
- y. All computers in the facilities shall have logon banners informing the user that the computer is a government resource and that they consent to having keystrokes monitored.

3.5 Personnel Screening

The GLAST facilities shall require all individuals requiring access to IONet Restricted or Closed computers to have applied for a NAC and submit a completed fingerprint form. A list of foreign nationals shall be submitted to NASA headquarters to allow access to any GLAST facility. Foreign nationals shall never have root or super user privilege. All users of the IONet equipment in the facility shall sign the appropriate IONet Rules of Behavior forms as well as the AETD or equivalent Rules of Behavior for accessing government equipment form before accessing the computer equipment.

3.6 Specialized Training

Any person requiring access to an IONet Restricted or Closed connected computer resource must first read and sign the appropriate IONet Rules of Behavior and read and sign either the AETD Rules of Behavior or a template based upon the AETD Rules of Behavior. The individual shall also be trained on the proper procedures for identifying personnel who have access to GLAST facilities and for challenging any unidentified access. Training shall also be provided to each individual concerning the steps to take if a computer resource is suspected of being compromised. Security awareness training shall be re-administered annually by the Security Officer of the GLAST facility. All training certifications shall be kept on file by the Security Officer for auditing purposes.

3.7 Contingency Planning

The GLAST MOC will maintain duplication of all software applications and data. The duplicated information will be stored outside of the GLAST MOC facility at **TBD** location. Using this information the GLAST MOC will be able to recover from any loss or corruption of data.

The hardware design of the MOC is fully redundant, ensuring that the failure of any one piece of hardware will not compromise the integrity, availability, or confidentiality of any MSN or SER. MOC performance and specification requirements dictate maximum time allowed before restoring back-up capabilities following a hardware failure.

Further description of this contingency planning is contained within the GLAST Contingency Plan.

3.8 Incident Response

Users of the computer resources in the GLAST MOC facility shall understand and follow procedures received in training if a security incident (compromise) is suspected. They will first notify the Security Officer and if possible the System Administrator. The Security Officer and System Administrator will then verify that a security incident has indeed occurred. The Security Officer shall then notify the Security Manager, the GLAST MOC facility manager, the Mission Operations Manager, and the GSFC Security Office in that order. The computer shall be disconnected from the network but kept powered on with no attempt to reboot the operating system or to close the software application that is running. The Security Officer shall wait for a security inspection team to arrive on site to further analyze and dispose of the situation. The following personnel are the points of contact for the MOC facility:

Security Manager – Howard Dew 301-614-5329

Security Officer – Dustin Aldridge 301-474-1700 x 656

Facility Manager – TBD

System Administrator – TBD

3.9 System Interconnection

Figure 1 shows the GLAST MOC's connection to the Restricted IONet, CNE, and Closed IONet. These connections are necessary to provide the required communications between the GLAST MOC and other external GLAST ground system elements. The protocols of the connections will be established in accordance with the various rules and policies mandated by each external IT system. Section 2.1 identifies the applicable regulations.

For the Closed IONet segment, additional firewall protection is not necessary. The GLAST MOC will rely on the security provided by the Closed IONet. All workstations and applications on the Closed IONet segment will conform to the requirements detailed in the *IONet Access Protection Policy and Requirements Document*.

On the restricted IONet segment, both the Open and Closed Subnets have direct connections to the Restricted IONet. Each connection contains a firewall. The firewall on the Open Subnet is configured to allow only TCP/IP communications from known IP addresses and HTTP communications. The firewall on the Closed Subnet is configured to restrict communications to a single direction from the MOC Closed Subnet to the MOC Open Subnet. This protects the Closed Subnet, which is used to command and monitor the GLAST observatory, from the WWW. All necessary communications are "pushed" from the Closed Subnet to the Open Subnet. File transfers between the MOC Restricted Segment and all external GLAST ground system elements will be controlled using the

FASTCopy COTS application located on the Open Subnet. This product uses a Secure Socket Layer (SSL) for encryption and authentication. Communications between FASTCopy nodes are authenticated using proxy usernames and passwords. In addition, FASTCopy enforces functional privileges which can be set independently on node and user accounts. All workstations and applications on the Restricted IONet segment will conform to the requirements detailed in the *IONet Access Protection Policy and Requirements Document*.

For the CNE segment, additional firewall protection is not necessary. The GLAST MOC will rely on the security provided by the CNE. Because the CNE Segment is isolated from the other MOC network segments, no additional security measures are required.

3.10 Review of Security Controls

The security protection of the GLAST MOC will undergo initial scanning by the GSFC Security Office prior to connecting to the IONets. Afterward, annual or bi-annual scans and audits will be performed on the MOC computer resources by the GSFC Security Office to verify documentation, configuration and procedural adherence to security requirements.

3.11 Authorization To Process

The Authorization to Process letter for the GLAST MOC facility will be reviewed and signed by the GLAST Project Manager, Kevin Grady, Code 492, once all security documentation and waivers have been submitted and accepted by the GSFC Security Office.

3.12 Security Documentation

The following documentation is required for the GLAST connections to the IONet:

- a. Security Plan
- b. Risk Management Plan
- c. Completed checklist to IONet Security Team for each facility
- d. Signed waivers for checklist non-compliance
- e. National Agency Checks for all personnel accessing computers attached to IONet.
- f. Authorization to Process signed by the Project manager.

In addition NASA Headquarters or the Federal Government requires the following:

- a. Contingency Plan
- b. Logon banner on all NASA-owned or NASA-funded IT systems
- c. Annual Computer Security Awareness Training
- d. Statement of Responsibility signed by users.
- e. List of foreign nationals sent to NASA Headquarters

Appendix A Responsibilities

The following paragraphs detail the responsibilities of key personnel in implementing this GLAST Security Plan.

A.1.1 GLAST Security Manager

The GLAST Security Manager has overall responsibility for the security of all systems within the GLAST MOC:

- Appoints the GLAST Security Officer
- Directs the Communications Engineer for creation of documentation and training
- Establishes and maintains procedures for the effective implementation of physical, personnel, and information technology security within the IOnet
- Plans and budgets for security related items in order to carry out procedures and controls
- Makes sure that the security of the GLAST facilities are within the bounds of established government and agency requirements
- Directs the support contractor(s) in security operations at the GLAST facilities

A.1.2 GLAST Security Officer

The GLAST Security Officer has overall responsibility for the implementation and continued conformance of security of all systems within the GLAST MOC:

- Approves all GLAST security plans and any subsequent changes
- Reports network security incidents as required by law
- Establishes overall GLAST security policy and guidelines for his/her facility
- Conducts periodic security audits
- Reports all security incidents to the Security Manager

A.1.3 GLAST Communications Engineer

The GLAST Communications Engineer has overall responsibility for the documentation and security training of all personnel using the GLAST MOC:

- Prepares and implements IOnet risk management plan, contingency plan, and security plan, and all subsequent changes
- Establishes effective security training and awareness programs
- Coordinates security policy and activities with the GLAST Security Manager and GLAST Security Officer
- Coordinates and works with the Security Officers to prepare and implement security procedures and controls

A.1.4 System Users

GLAST MOC system users must complete the following checklist before accessing any GLAST MOC system.

- a. Submit a formal request for a User ID
- b. Follow all developed security procedures
- c. Follow the Rules of Behavior for IOnet Open and AETD
- d. Report all security incidents to the facility Security Officer
- e. Attend Computer Security Awareness Training
- f. Take responsibility for protecting the data
- g. Sign a statement of responsibility indicating understanding of the requirements for using and safeguarding the information to which each are granted access

Appendix B Abbreviations and Acronyms

AETD	Applied Engineering and Technology Directorate
CNE	Center Network Environment
COTS	Commercial-Off-The-Shelf
FTP	File Transfer Protocol
GBM	Gamma-ray Burst Monitor
GFEP	GLAST Front End Processor
GIOC	GBM Instrument Operation Center
GLAST	Gamma-ray Large Area Space Telescope
GRT	Ground Readiness Test
GSFC	Goddard Space Flight Center
GSSC	GLAST Science Support Center
HTTP	Hyper-Text Transfer Protocol
HVAC	Heating, Ventilation, and Air-conditioning
ID	Identification
IP	Internet Protocol
IT	Information Technology
IONet	Internet Protocol Operational Network
KSC	Kennedy Space Center
L&EO	Launch and Early Orbit
LAN	Local Area Network
LAT	Large Area Telescope
LISOC	LAT Instrument Science Operation Center

MOC	Mission Operations Center
MSN	Mission Information
NAC	National Agency Check
NASA	National Aeronautics and Space Administration
Nascom	NASA Communications
NISN	NASA Integrated Services Network
NMC	Network Management Center
NPG	NASA Procedures and Guidelines
SER	Scientific, Engineering, and Research Information
SSL	Secure Socket Layer
RLOGIN	Remote Login
RSH	Remote Shell
TBD	To Be Determined
TCP	transmission control protocol
TDRSS	Tracking Data Relay Satellite System
USN	Universal Space Network
VPN	Virtual Private Network
WAN	wide area network
WSC	White Sands Complex
WWW	World Wide Web