CSO NASA Communications (NASCOM) Mission Network -

Internet Protocol Operational Network (IONet) Security Policy

Document #: NMO-POL-001-20100901
Version: 3.3, 07/30/2020
Effective Date: 07/30/2020
Expiration Date: 09/30/2020
Responsible Offices: Communications Services Office (CSO) NASA Communications (NASCOM) -
Mission Networks Division (MND), Code 770
Goddard Space Flight Center (GSFC), Greenbelt, MD

SIGNATORY AUTHORITY

This document is valid for three (3) years after the last date on the signatures below at which time the document content will be reviewed, updated if necessary, and revalidated by the Communications Services Office (CS) NASA Communications (NASCOM), Mission Networks Division (MND), Code 770 at Goddard Space Flight Center (GSFC).

Approved by:

Curt Suprock 9/13/2016

Curt Suprock, System Owner Date
Mission Networks Division (MND), Code 770, GSFC

Approved by:

8/31/16

Scott Douglas, CSO NASCOM Mission Operations Manager Date
Mission Networks Division (MND), Code 770, GSFC

Concurrence Given by:

8/31/16

Matt Kirichok, CSO NASCOM Mission Engineering Team Lead Date
Mission Networks Division (MND), Code 770, GSFC

Concurrence Given by:

Tea Taylor 8/31/16

Tea Taylor Date
CSO NASCOM Mission Network Information Systems Security Officer (ISSO)
Mission Networks Division (MND), Code 770, GSFC

Prepared by:

9/8/16

Clayonna Wheat Date
CSO NASCOM Mission Network Security Intern
Mission Networks Division (MND), Code 770, GSFC

Contents

Appendices

Note: Printed copies of this document are uncontrolled. Before using a printed copy to perform work, verify the version against the Code 770 electronic document library to ensure you are using the correct version.

SECTION 1: INTRODUCTION

1.1 Purpose

The *Communication Service Office (CSO) NASA Communications Mission Network (NASCOM) Internet Protocol Operational Network (IONet) Security Policy* sets forth the principles by which confidentiality, integrity and availability of CSO IONet mission networks are managed and maintained.

1.2 Applicability

The *NASCOM IONet Security Policy* is applicable to all NASA personnel, contractors, vendors, international partners, and other persons or entities that utilize or are responsible for the management and maintenance of the CSO NASCOM Mission Network's IONet. The most current version of the *IONet Security Policy* is available on the CSO website https://cso.nasa.gov/resources/policies.

Compliance with the *IONet Security Policy* is mandatory of all NASA and non-NASA projects, programs or organizations, and their personnel managing and/or using systems connected to the CSO NASCOM Mission Network's IONet.

Systems connected via one of the three IONet's are required to adhere to all applicable Federal and Agency Directives, Standard Operating Procedures, Procedural Requirements, and Memoranda.

In the event of a policy collision between this NASCOM Mission Network's IONet Security Policy and a higher-level NASA or Federal IT Security policy requirement, the most restrictive requirement shall be authoritative.

1.3 Authority

The CSO NASCOM Mission Network System Owner has the authority to develop, implement, and manage policies, processes, and procedures to protect the confidentiality, integrity and availability of the CSO mission network. Further, the CSO NASCOM Mission Network's System Owner has the responsibility and authority to ensure that interconnected systems are operating in such a manner that ensures the safety of other systems and the CSO mission networks.

1.4 References

The following are applicable to the operations and maintenance of the IONet, and as such has been identified as the primary governance for the *CSO NASCOM Mission Network's IONet Security Policy.*

1. FIPS 199 - Standards for Security Categorization of Federal Information and Information Systems
   http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
2. NITR 2810-24 NASA IT Device Vulnerability Management
   http://nodis.hq.nasa.gov/tech_guidance/N_ITR_2810_24_.pdf
3. NPR 1600.1A NASA Security Program Procedural Requirements
   http://nodis3.gsfc.nasa.gov/displayCA.cfm?Internal_ID=N_PR_1600_0001_&page_name=main
4. NPR 2810 Security of Information Technology
   http://nodis3.gsfc.nasa.gov/
5. SP-800-53 NIST Recommended Security Controls for Federal Information Systems
   http://csrc.nist.gov/publications/PubsSPs.html
6. SP 800-125 Guide to Security for Full Virtualization technologies
   http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf

1.5 IONet Security Policy Exemptions (IPE)

IONet Security Policy Exemptions (IPEs) are used to grant non-compliant systems a temporary interconnection to the IONet for a period not to exceed twelve (12) months. In addition to the *IONet Policy Exemption Form*, projects are required to provide a mitigation plan in order for the exemption to be considered. The CSO Mission

Network System Owner is the final approving authority for approving and granting exemptions to the IONet Security Policy.

The IONet Security Policy Exemption form is posted to the CSO website **https://cso.nasa.gov/resources/policies** and includes the necessary forms and instructions needed to submit an exemption request.

SECTION 2: IONet SYSTEM SECURITY

2.1 Technical Overview of the IONet

The IONet is a NASA-wide IP network managed by CSO Mission Operations. The IONet supports missions on a 24-hour basis with real-time operational data supporting attitude, command, orbit, ephemeris, telemetry, and state vectors. In addition, IONet supports non-real-time network data communications including data products from space experiments and quick-look image data.

The IONet is divided into three zones: Closed, Restricted, and Open. All three IONet zones handle data that is critical for mission operations and, in the case of the Closed IONet, human spaceflight.

All zones of the IONet perimeter are protected by firewalls. CSO Mission Operations maintains oversight and control of the firewalls to control access to or from outside entities.

The data processed, access allowed, systems connected, dataflows, and network communications on IONet are required to support NASA mission requirements directly. For security and network maintenance purposes, authorized individuals within NASA may monitor equipment, systems and network traffic at any time. Under no circumstances is a system connected to the IONet to be utilized for any activity that is illegal under local, state, federal or international law.

The detection of non-mission data flows, data processing, and network communications can and will lead to disconnection from the IONet.

2.2 Assessment Authorization

All systems connecting to NASCOM Mission Network's IONET shall require an Authorization to Operate (ATO) or Authorization to Test (ATT) prior to establishing a connection. All NASA systems are required to have an approved ATO or ATT and are required to document NASCOM as an interconnection within their System Security Plan (SSP). All systems external to NASA shall require an Interconnection Security Agreement.

2.3 IONet Services Elements

Service Name	Service Description
Communications Transport	Provides Mission Projects/Organizations with IP network connectivity.
Domain Name System (DNS)	Provides domain name resolution to facilitate communication through hostname addressing.
Mission Network Intrusion Detection Service (IDS)	Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.
Network Perimeter Firewalls	Provide perimeter protection for each IONet zone based on the security requirements for that zone.
Network Time Protocol (NTP)	Provides network time services to facilitate consistent timestamps.
Patch Management	Provides a means by which System Administrators may assess whether their hosts are properly patched. Requires a client-side software installation. Patchlink is the current Mission Patch Reporting Service Limited to no support; will be decommissioned and replaced with CDM tools
Vulnerability Scanning	Regularly scheduled scans of all systems connected to the IONet for the purpose of vulnerability identification and mitigation.
Anti-virus	**Malware prevention, removal, and signature updates for systems connected to the IONet.** Centralized Symantec antivirus service providing a/v clients and signatures
MSGRS – Mission Secure Gateway Request System	Centralized firewall request system; can be accessed by customers
Windows Server Update Services (WSUS)	Provides local repository of Microsoft patches which is assessable to customers
Mission Secure Shell Gateway Service (SSHGS)	Proxies, decrypts, and provides IDS unencrypted SSH dataflows
Network Web Proxy Service	Provides hosts access to external whitelisted websites

2.4 Controlled Unclassified Information (CUI) / Sensitive But Unclassified (SBU) Information

IONet sensitive information, such as vulnerability scan results, firewall rules, passwords, circuit IDs, and special use port numbers, must be handled as Controlled Unclassified Information (CUI). According to NPR 1600.1, CUI data may only be disclosed to someone who has a valid need to know. If in doubt, the user should ask their system administrator, Information System Security Officer or Information System Owner. The identity of all personnel to whom CUI data is revealed should be verified. CUI documents and media require a coversheet, NASA form 1686.

2.5 Host and Device Registration

All systems/hosts that interconnect to the IONet shall be registered in the Agency's IP Management System DDI (DNS, DHCP and IPAM).

Unregistered hosts are not permitted and will be considered hostile rogue hosts and are subject to disconnection. System administrators are responsible for keeping the information about their host current with the CSO NASCOM Mission Network Information System Security Officer (ISSO).

The system information below is to be provided to the CSO mission network CSO NASCOM Mission Network ISSO prior to the activation of all new connections and must be available during the security audit. The information is as follows:

a. Mission project that this system supports
b. Host name that is unique within the Mission Network
c. System description/purpose
d. The name of the domain that the system resides on
e. Operating System
f. Device type (desktop, server, router, switch, etc.)
g. Location (i.e., NASA Center, state, street address)
h. Building/room number
i. System Security Plan (SSP) identification number
j. Security POC contact information
k. System Owner contact information
l. IONet Zone: Open, Closed, Restricted
m. IP address (will be assigned by the IONet Security Auditor)
n. Split Domain Name Service (DNS) visibility: internal/external
o. System Administrator(s) (responsible for the host) contact information
p. Organization Code responsible for system

2.6 Background Checks

All persons with access to IONet-connected resources require a National Agency Check with Inquiries (NACI) which requires background screening and fingerprinting. A NACI “in progress” is not sufficient.

Foreign nationals (including those with a green card) are either non-international or international partners. International partners may not under any circumstance have limited or elevated privileged access to IT resources on the IONet.

2.7 Connection Requests

IONet Security audits shall be conducted prior to connecting any IT resource to the IONet. Audits are conducted in parallel with the processing of the Communication Service Request (CRQ) process. Connection requests are made using *NASCOM-FOR-020-20100913 – Mission Operations NMO-NASCOM- Access Control Compliance for Information Systems on the IP Operational Network (IONet).*

System Owners are also required to provide a copy of their final Security Assessment Review (SAR) or approved Authorization To Operate (ATO) for CSO NASCOM Mission Network ISSO review prior to the enabling of any new interconnection to the IONet.

2.8 Permitted on the IONet

1. Use of current versions of SSHv2 is allowed within an IONet zone
2. Project firewalls are allowed on the Restricted and Open IONet zones.
3. FTP is allowed on the IONet and use of bbftp and sftp is allowed with an approved IONET Policy Exemption.
4. Use of virtual computing on the IONet is strictly limited to configurations consistent with Mission IONet guidelines and is required to be reviewed and authorized by the CSO NASCOM Mission Network ISSO. NIST SP 800-125 should be used as a reference for implementing a virtualized environment.

2.9 Prohibited on the IONet

1. Remote logins across zones are prohibited. Remote connection protocols such as rsh, rlogin, telnet, etc., are prohibited on all devices that support Secure Shell (SSH). The cryptologically insecure SSH v1 protocol is prohibited and shall be disabled if detected.

2. Dual-homed systems that are connected to two different networks are prohibited. A *dual- homed system* is a system that has multiple network interface cards and is connected to two networks at the same time. For example: Being connected to the local center administrative network and Closed IONet.
3. Hosts are not permitted to run dynamic routing protocols and/or IP forwarding.
4. Project e-mail servers are prohibited. NASCOM will provide email services if required.
5. Outbound X11 service display to an external network is prohibited.
6. Network Address Translation (NAT) is prohibited.
7. Project-managed Virtual Private Networks (VPNs) are prohibited.
8. Systems shall not allow user-initiated actions without authentication.
9. Chat, Internet Relay Chat (IRC), and Peer-to-Peer (P2P) messaging/file transfers are prohibited.
10. IONet-connected devices must not have wireless network interfaces, make use of wireless network communication technologies including, but not limited to GSM, GPRS, CDMA, Bluetooth, Wifi, and/or infrared.
11. Voice over IP (VoIP) is prohibited.
12. Dynamic Host Configuration Protocol (DHCP) is prohibited.
13. Out-of-band remote access, including but not limited to modems or Integrated Services Digital Network (ISDN) lines, is prohibited.
14. Hosts on the Closed IONet shall not be connected to or communicate with any network outside the Closed IONet, except through the Closed IONet firewall.
15. All externally sourced connections through the Closed IONet firewall are prohibited.
16. Project network firewalls are prohibited on the Closed IONet.
17. Sniffing, network monitoring, and/or network intrusion detection is prohibited.
18. IPv6 network communications including transition mechanisms including, but not limited to, teredo, 6in4, 6to4, and NAT64 are prohibited.
19. Cryptographically insecure protocols are prohibited including, but not limited to SSL v3.0 and TLS 1.0.

2.10 Interconnection Security Agreements (ISA)

An Interconnection Security Agreement (ISA) shall be required between NASCOM Mission Network   and non-NASA Agencies, their Organizations and all associated Projects where an interconnection with the IONet is specifically required for NASA Mission Project requirements.

The ISA constitutes an agreement for the purpose of ensuring that Agencies, their Organizations and all associated Projects, as identified in the ISA, utilizing the interconnection and associated services understands and abides by the *IONet Security Policy.*

2.11 Security Plans

All systems connected to the IONet and leveraging CSO Mission Network /IONet IP Addresses shall be associated with a NASA System Security Plan that has been through the NASA Authorization and Accreditation (A&A) process and been granted Authorization to Process (ATP). This ensures that the necessary Federal and NASA IT Security technical controls are appropriately implemented.

2.12 Physical Security

Hosts connected to the IONet shall be behind locked doors, preferably, with at least a key card. If locks are used, there shall be a list of personnel with keys, and managed through a central key distribution process.

2.13 Domain Name System (DNS)

DNS Services for systems connected to the IONet shall be provided by the NASA' DDI System.

2.14 Disabling of non-Mission Network Services

Hosts connected to the IONet shall disable all network services not required for mission operations.

2.15 Password Management

Password management for all systems connected to the IONet shall be enforced in accordance with *NPR 2810, Security of Information Technology*.

2.16 Encryption

The following applies to the use of encryption on the IONet:

1. Encrypted communications across the IONet, with the exceptions of SSH and HTTPS, shall only be permitted with prior approval by the IONet CSO NASCOM Mission Network ISSO.
2. Encrypted communications shall not traverse the Closed IONet network perimeter.
3. Encrypted connections to IONet-connected resources that cross an IONet firewall shall be identified by individual IP addresses. Requests for access from wildcard or subnet sources will be denied.
4. Encrypted tunnels shall be configured to prohibit split tunneling. That is, when connected via an encrypted tunnel to a device connected to the IONet, the client host must not be connected to other networks simultaneously.
5. Hosts shall be configured to limit access to the most restrictive set of allowed connections.
6. IONet hosts providing encrypted communication services shall be configured to log all events to a physically separate IONet host.

2.17 SSH Communications

All externally-sourced internally-bound and internally-sourced externally-bound (internet) SSH communications are required to be proxied through CSO mission network proxy.

2.18 Web Proxy Communications

All internally-sourced externally-bound web communications are required to be proxied through CSO mission network proxy.

2.19 Firewalls and Externally-sourced Communications

Data flows with hosts external to the CSO mission network /IONet shall be initiated/sourced from hosts connected internally to the CSO mission network /IONet networks. Mission perimeter firewalls shall be configured to disallow all externally-sourced communications. Exceptions to this are permitted only with CSO NASCOM Mission Network ISSO approval via MSGRS.

All perimeter-crossing network communications shall be explicitly identified by source and destination and are required to directly support a Mission data delivery requirement. All requests for *-inbound or *-outbound connections should go through the IONet DMZ.

2.20 Ping

Hosts connected to the IONet must be “pingable” throughout the life of the host on the IONet. The ability to ping all hosts aids troubleshooting and the ability to conduct network scans. Projects must configure their networks and hosts to allow Inbound “ICMP type 8 echo request” to all hosts connected to the IONet and Outbound “ICMP type 0 echo reply” from all hosts connected to the IONet. If necessary, ping rules must be added to the project-managed and host-based firewalls to allow this.

2.21 Well Known Port Usage

IONet-connected hosts providing server services shall adhere to the port number assignments as defined by IANA http://www.iana.org/assignments/port-numbers for IP network services. Moving a known service defined by IANA to other port numbers is prohibited.

2.22 Software Maintenance

Hosts connected to the IONet shall be maintained with current software revisions and vendor provided patches in accordance in accordance with local configuration management processes.

2.23 Patch Management

To fulfill NITR 2810-24 and patch management reporting requirements, IONet (Open, Close, Restricted) IT devices shall have the NASA patch management/reporting software agent installed. In the case where automatic reporting via the NASA agent is not feasible patch status reporting will be done manually. It is the System Owner's responsibility to ensure that systems under their cognizant are identified and documented in a System Security Plan (SSP) and that these systems are patched as required in NITR 2810-24.

2.24 Vulnerability Assessments and Scanning

The following applies to Mission vulnerability scans which include quarterly, audit, and new system connection scans (which can include new systems connecting to the network as well as configuration changes to existing systems that change a systems security baseline):

1. Mission vulnerability scanning shall be performed in support of Agency requirements as defined within ITS-HBK-2810-04-01 https://nodis-dms.gsfc.nasa.gov/NASA_Wide/restricted_directives/OCIO_Docs/ITS-HBK_2810_04_01.pdf to identify, eliminate, and/or mitigate vulnerabilities.
2. The Mission Operations Security Team (MOST) shall be the only personnel authorized to perform Mission vulnerability scans.
3. The MOST shall maintain records of identified vulnerabilities. Projects are required to eliminate, mitigate, or request a vulnerability exemption for identified vulnerabilities. Failure to address the same vulnerability in three consecutive quarters can result in disconnection.
4. A CSO NASCOM Mission Network Secure Gateway Request System (MSGRS) request must be submitted to permit scanning from MOST systems. Note: Customer is responsible for submitting MSGRS request if NASCOM manages the firewall.
5. Host based firewalls shall be disabled during audit and system connection scans.

2.25 Audits

Audits of the IONet zones are required by Federal and CSO mission network policy for purpose of evaluating, assessing, and documenting system interconnections and risks associated with existing, modified, or new connections to the IONet.

MOST auditors review system documentation and system connectivity for the purpose of identifying risks to the IONet through interconnected systems or hosts. Auditors recommend the acceptability of project interconnections to the CSO mission network CSO NASCOM Mission Network ISSO. Audits shall be conducted for, but not limited to, any of the following reasons:

1. New connections of an entire project/system to the IONet
2. A network device in a connected project/system was compromised
3. A new project/or a project system that was last audited 3 years ago
4. A CSO mission network CSO NASCOM Mission Network ISSO requested audit
5. A major change to the project
6. An *IONet Security Policy Exemption* submission

System Owners are also required to provide a copy of their final Security Assessment Review (SAR) or approved Authorization To Operate (ATO) for CSO NASCOM Mission Network ISSO review during the course of an audit.

2.26 Anti-Virus

The following applies to antivirus:

1. Systems utilizing operating systems compatible with antivirus software shall implement, activate, and maintain antivirus software on the system at all times.
2. Systems shall utilize the centralized CSO mission operations provided Antivirus System and are prohibited from communicating with other centralized antivirus systems.

2.27 Windows Server Update Services (WSUS)

The following applies to WSUS:

1. Systems shall utilize the centralized CSO mission operations WSUS System when these capabilities are operational.
2. Systems are prohibited from communicating with any other WSUS systems.

2.28 Incident Reporting

IT Security incidents involving or impacting hosts connected to the CSO mission network /IONet shall be reported to CSO Mission Security via the Goddard Communications Control Communications Manager (COMMGR) at 301-286-6141. GCC and/or MOST will report to NASA's SOC. The MOST will provide assistance isolating, remediating, reporting, and recovering from Information Security incidents.

SECTION 3: ADMINISTRATION

3.1 Control Information

Originating Group:	Mission Operations Security Team (MOST)	**Date:** 02/2013
Author(s):	CSO Mission Network Information Systems Security Officer (ISSO); Mission Operations Security Team (MOST)	**Date:** 02/2013
Reviewer(s):	CSSD/Code 760 Division Chief, Engineering and Security Services/Code 762 Branch Head; CSO Mission Network Information Systems Security Officer (ISSO); CSO Mission Operations Manager; Deputy CSO Mission Network ISSO	**Date:** 03/2013
Approved by:	CSSD/Code 760 Division Chief, Engineering and Security Services/Code 762 Branch Head; CSO Mission Network Information Systems Security Officer (ISSO); CSO Mission Operations Manager; Deputy CSO Mission Network ISSO	**Date:** 03/05/2013
Distributed to:	CSSD/Code 760 personnel as applicable	**Date:** 03/05/2013
Posting completed by:	Code 760 NCMT	**Date:** 03/05/2013

3.2 Change History Log

Revision	Effective Date	Description of Changes
Baseline (v. 1.0)	07/19/2011	Initial Release
v2.0	03/05/2013	All references to NISN removed and replaced with CSO and/or CSO mission network as applicable; all mission operations security forms information updated as applicable; signature page updated to reflect current policy/document/content ownership.
v3.0	09/13/2016	All content reviewed for revision.
v3.1	09/05/2019	Effective Date modified from 09/13/2016 to 09/05/2019; Document Expiration Date modified from 09/12/2019 to 02/29/2020 per the direction of the CP NASCOM Mission Network Information System Security Officer (ISSO) (T. Taylor).
v3.2	03/01/2020	Effective Date modified from 09/12/2019 to 02/29/2020; Document Expiration Date modified from 03/01/2020 to 05/31/2020 per the direction of the CP NASCOM Mission Network Information System Security Officer (ISSO) (T. Taylor).
v3.3	07/30/2020	Effective Date modified from 02/29/2020 to 07/30/2020; Document Expiration Date modified from 05/31/2020 to 09/30/2020 per the direction of the CP NASCOM Mission Network Information System Security Officer (ISSO) (T. Taylor).

3.3 Document Change Control Mechanism

This document is under the administrative control of the MND, Code 770 at GSFC. This policy is enacted and maintained under the following guidelines:

1. This document becomes effective on the date of the last signature of the approval authorities.
2. This document shall be reviewed, as required, by the signatory authorities to determine the need for its continuation, modification, or termination.
3. Any modification to this document (post-approval) shall be executed in writing and signed by the officials executing this policy or a delegated authority. Any modification which creates an additional commitment of NASA resources must be signed by the original NASA signatory authority or successor, or a higher level NASA official possessing original or delegated authority to make such a commitment.

4. Upon declaration of a national emergency or general mobilization, this document shall remain in effect but may be subject to immediate review.

Appendix A: Acronyms and Abbreviations

A&A	Authorization and Accreditation
ATP	Authorization To Process
C&A	Certification and Accreditation
COMMGR	Communications Manager
CSO	Communication Service Office
CSSD	Communications and System Security Division
CRQ	Communications Change Request
DHCP	Dynamic Host Control Protocol
DNS	Domain Name System
FIPS	Federal Information Processing Standard
FOR	Form
FTP	File Transfer Protocol
GSFC	Goddard Space Flight Center
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IONet	Internet Protocol Operational Network
IP	Internet Protocol
IRC	Internet Relay Chat
ISA	Interconnection Security Agreement
ISDN	Integrated Services Digital Network
ISSO	Information System Security Officer
IT	Information Technology
MND	Mission Networks Division
MOA	Memorandum Of Agreement
MOST	Mission Operations Security Team
NAC-I	National Agency Check Inquiries
NASA	National Aeronautics and Space Administration
NAT	Network Address Translation
NCMT	Network Configuration Management Team
NFS	Network File System
NIST	National Institute of Standards and Technology
NITR	NASA Interim Technical Requirement
NPR	NASA Procedural Requirement
NSR	Network Service Request
NTP	Network Time Protocol
P2P	Peer-to-Peer
POA&M	Plan Of Action and Mitigation
POL	Policy
SBU	Sensitive But Unclassified
SP	Special Publication
SSH	Secure Shell (Secure Socket Shell)
SSP	System Security Plan
VM	Virtual Machine
VoIP	Voice over IP
VPN	Virtual Private Network
WSUS	Windows Server Update Services