NASA Information Technology Requirement

NITR-2800-2

Effective Date: September 18, 2009
Expiration Date: September 18, 2013

Email Services and Email Forwarding

Responsible Office: OCIO/ Chief Information Officer

Table of Contents

Change History

Distribution

NODIS

Change History

NITR-2800-2, Email Services and Email Forwarding

Change Number	Date	Change Description

PREFACE

P.1 PURPOSE

The purpose of this NASA Information Technology Requirement (NITR) is to establish policy and requirements regarding email services and email forwarding to enhance security of NASA's information and prevent information security breaches.

P.2 APPLICABILITY

a. This NITR applies to unclassified information systems at NASA Headquarters and Centers, including Component Facilities and Technical and Service Support Centers. To the extent specified in their respective contracts or agreements, it applies to the NASA Jet Propulsion Laboratory, other contractors, grant recipients, or parties to agreements for information systems that they use or operate on behalf of the Agency or that support the operations and assets of the Agency.

b. The requirements of this document apply to all email services connecting to NASA Information Technology (IT) systems or NASA networks. NASA networks and systems include those that support NASA facilities, employees, contracts, grants and cooperative agreements.

P.3 AUTHORITY

Same as NPR 2800.1B

P.4 APPLICABLE DOCUMENTS

a. NPD 2800.1, Managing Information Technology.

b. NPR 2800.1, Managing Information Technology

c. NPR 2830.1, NASA Enterprise Architecture.

d. NPR 2810.1, Security of Information Technology.

e. NPR 1382.1, NASA Privacy Procedural Requirements.

f. NPR 1600.1, NASA Security Program Procedural Requirements.

g. NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology.

h. Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems.

i. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.

j. NIST 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.

k. NIST SP 800-53, Recommended Security Controls for Federal Information Systems.

l. NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems.

P.5 MEASUREMENT AND VERIFICATION

None

P.6 CANCELLATION

The next version of NPR 2800.2 cancels this NITR

Bobby L. German
Chief Information Officer (Acting)

9/24/09
Date

1.0 Email Services and Email Forwarding

1.1 Requirement

1.1.1 The goal of the NASA Operational Messaging and Directory (NOMAD) service is to increase Agency interoperability across NASA Centers, comply with Federal directives and regulations, and reduce Agency security vulnerabilities, messaging complexity, and support costs. NOMAD services provide email, calendaring, task management, contacts, instant messaging and common file sharing services for NASA. This includes the NOMAD responsibility for Simple Mail Transfer Protocol (SMTP) services for NASA and routing all SMTP traffic for each center thru the relays.

1.1.1.1 NOMAD is the only authorized user messaging service within the NASA domain. All user email traffic within the domain shall originate from and/or terminate to NOMAD within 60 days of the effective date of this NITR. All NASA-badged personnel, including civil servants, on-site contractors, on-site business partners, and on-site grantees shall utilize NOMAD services for all email and calendaring in performing their NASA duties, with the following exceptions:

a. This requirement will not be levied onto existing contracts for which the contractor is currently required to provide their own messaging solution; however, all new contracts will be required to use the NOMAD service.

b. This policy does not apply to external NASA partners from industry, academia, and other government agencies, that may have NASA badges because they visit NASA facilities but whose primary duty station is external to NASA.

c. Contractors are not prohibited from accessing their corporate messaging system for conducting contractor business (e.g. timecards, business notifications). Contracting Officer Technical Representatives (COTRs) and Project Managers (PMs) are to advise contractors on the degree to which contractors will use their corporate messaging system off-site for receiving NASA data via email.

1.1.1.2 Sensitive NASA data transmitted using the NOMAD system shall be encrypted using the Agency Entrust capability that is available in Microsoft Outlook and Entourage.

1.1.1.3 NASA Centers shall decommission all local user messaging systems within 12 months of completion of the Center's migration to NOMAD.

1.1.1.4 All user email originating from a NASA email server shall be identified with a NASA email address unless otherwise approved by the NASA Agency Postmaster. The "From" and "Reply To" addresses for NOMAD accounts may only be set to Government or Military email addresses.

1.1.2 No NASA email servers shall receive email sent or forwarded from a non-NASA email server unless approved by the NASA Agency Postmaster.

1.1.2.1 The information system certification and accreditation (C&A) requirements for NASA systems that send and forward email shall include:

a. Documentation of the email data exchange and the NASA Agency Postmaster approval in the System Security Plan (SSP).

b. Approval by the Authorizing Official (AO).

c. A Memorandum of Agreement/Understanding (MOA/U) and a System Interface Agreement (SIA) in accordance with NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* and NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems* for the email data exchange. (See paragraph 1.1.3.3 for exception for a NOMAD email exchange server.)

1.1.2.2 Example: A computer system that accepts incoming email from a non-NASA server, including for maintenance purposes, shall have approval by the NASA Agency Postmaster to receive incoming email, with the approval documented in the SSP. This includes, but is not limited to, a computer accepting connections on IP port 25.

1.1.2.3 A MOA/U and a SIA shall not be required for SMTP email traffic to and from a NOMAD email exchange server.

1.1.3 A NOMAD mailbox shall not be automatically forwarded from a NASA email server to a non-NASA email server. An automatic forward may not be placed on a NOMAD mailbox to send to a personal or non-NASA business email account. The user may, however, selectively and manually forward individual email messages, which must not contain sensitive NASA information, for review at home or to a business partner's email system.

1.1.4 OneNASA addresses (e.g., username@nasa.gov) may only be forwarded to NOMAD mailboxes, legacy NASA Center-run email systems and to other Government or Military email addresses.

1.1.4.1 Forwarding of OneNASA addresses to accepted Contractor-run email systems may continue until the end of the current contract.

1.1.4.2 All other OneNASA addresses currently forwarded to non-Government and non-Military email addresses shall be removed within 60 days of the effective date of this NITR.

1.2 Responsibilities

1.2.1 Center CIOs shall:

a. Be responsible for ensuring compliance with this NITR and for ensuring that all non-compliant information systems and networks are brought to a compliant state by January 1, 2010, or are operating under an approved waiver.

b. Review and submit all waivers recommended for approval in accordance with NITR 2800-1, NASA Information Technology Waiver Requirements and Procedures.

c. Provide oversight for:

(1) The development and tracking of Center processes for compliance with this NITR.

(2) The preparation, tracking, and IT technical support for waiver requests

1.2.2 System owners shall ensure that:

a. The NASA Agency Postmaster has approved the acceptance of incoming email by their systems.

b. The incoming email requirement is documented in the SSP.

1.2.3 Authorizing Officials (AO) shall ensure that server based information systems that accept incoming email:

a. Are approved by the NASA Agency Postmaster to receive the email.

b. Have an approved and signed MOA/U and an SIA for this email data exchange.

1.2.4 Refer to NITR-2800-1 for waivers.

1.3 Waivers

Refer to NITR-2800-1.

Appendix A Definitions

Term	Definition
Authorizing Official	A senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. [FIPS 200 adapted]
Information System (Also referred to as IT System)	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.[44 U.S.C., Sec. 3502]
Information Technology (IT)	Any equipment or interconnected system(s) or subsystem(s) of equipment that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Agency. (FAR 2.101)
Internet Protocol	For the purposes of this policy, any collection of devices communicating over a wired or wireless network using the Internet Protocol (IP)
NASA Information	Any knowledge that can be communicated regardless of its physical form or characteristics, which is owned by, produced by, or produced for, or is under the control of NASA. (NPR 2810.1.)
Network	Information System implemented with a collection of interconnected nodes. (CNSS Instruction 4009)
OneNASA Account	An alias email account that ends in @nasa.gov
Plan of Action and Milestones (POA&M) - Programmatic	A Programmatic POA&M is used to document and track the security deficiencies and/or weaknesses in the security controls of an IT system, multiple IT systems, and/or organizational level policies, programs, and C&A implementation and the documentation and tracking of the mitigation of these deficiencies. These deficiencies are normally identified from audits/investigations by the OIG, Government Accounting Office (GAO) (congressional), or other authorized agency. A programmatic POA&M shall be managed and tracked at the Agency level and with mitigation reports provided to the agency/organization that identified the deficiency

Term	Definition
Plan of Action and Milestones (POA&M) - System	A System POA&M is used to document the security deficiencies and/or weaknesses in the security controls of an IT system and to track the mitigation of those deficiencies. These deficiencies are normally identified from the system security control assessments, security impact analyses, and continuous monitoring activities. A POA&M shall be prepared/established for every information system that has a deficiency
Security Control	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information. [FIPS 199]
Senior Agency Information Security Officer	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. [44 U.S.C., Sec. 3544] Synonymous with Chief Information Security Officer (CISO)
Simple Mail Transfer Protocol	An Internet standard for electronic mail (email) transmission across Internet Protocol (IP) networks
System	The combination of elements that function together to produce the capability required to meet a need. The elements include all hardware, software, equipment, facilities, personnel, processes, and procedures needed for this purpose.
System Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. [NIST SP 800-18]

Appendix B Acronyms

AO	Authorizing Official
ATO	Authorization To Operate
C&A	Certification and Accreditation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee for National System Security
DCID	Director of Central Intelligence Directives
FAR	Federal Acquisition Regulations
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAO	General Accounting Office
IP	Internet Protocol
ISO	Information System Owner
IT	Information Technology
ITSM	Information Technology Security Manager
MOA/U	Memorandum of Agreement/Memorandum of Understanding
NIST	National Institute of Standards and Technology
NOMAD	NASA Operational Messaging and Directory Services
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PDA	Personal Digital Assistant
POA&M	Plan of Action and Milestones
SAISO	Senior Agency Information Security Officer
SIA	System Interface Agreement
SMTP	Simple Mail Transfer Protocol
SSP	System Security Plan