National Aeronautics and
Space Administration

RELEASE DATE: 11-04-2020

EMAIL SERVICES

Prepared by:
Ron Colvin, Annabelle Durand, and Michael Powers

Table of Contents

Contents

Table of Contents 3

Purpose 5

Applicability 5

Authority 6

Applicable Documents, Other Resources 6

Measurement and Verification 7

Replacement 7

Requirements 7

Appendix A: Acronyms 11

Change History

Change Number	Date	Change Description
1.0	June 12, 2020	Initial release of NAII 2810.2

Purpose

The purpose of this NASA Advisory Implementing Instruction (NAII) 2810.2 is to establish a policy and set of requirements regarding email services in order to prevent information security breaches and better protect NASA users of email services.

The goal of the NASA user electronic messaging 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.

NAII 2810.2 replaces NASA Information Technology Requirement (NITR) 2800, *Email Services and Email Forwarding*, which went into effect on September 18, 2009, and expired on September 18, 2013.

NAII 2810.2 contains controls that are required in order to be compliant with the Department of Homeland Security (DHS) Binding Operational Directive (BOD) 18-01, *Enhance Email and Web Security*. The controls in this NAII ensure compliance by establishing a Domain-based Message Authentication, Reporting and Conformance (DMARC) policy, which rejects any email that does not come through an approved route. Any email sent from NASA's domain (i.e., ending in nasa.gov) will be subject to this policy. Any outbound NASA email not using an email service with a NASA Domain Name System (DNS) registration defined in a NASA Sender Policy Framework (SPF) or Domain Keys Identified Mail (DKIM) DNS entry will be subject to rejection by organizations respecting DMARC and the SPF.

Applicability

NAII 2810.2 is applicable to NASA Headquarters and all NASA centers, including component facilities as well as technical and service support centers. This NAII also applies to the NASA Jet Propulsion Laboratory, a federally funded research and development center (FFRDC), as well as other contractors.

The requirements in this document apply to all email services connecting to NASA Information Technology (IT) systems or NASA networks. NASA IT systems and networks include those that support NASA facilities, employees, contracts, grants, and cooperative agreements. Any email sent or received on behalf of, or in cooperation with, NASA is subject to these requirements.

Authority

Per NASA Policy Directive (NPD) 2800.1, *Managing Information Technology*, the NASA Chief Information Officer (CIO) has the responsibility, accountability, and authority to 1) manage the NASA IT infrastructure as an integrated end-to-end service to improve security, efficiency, and inter-center collaboration; 2) develop and/or enforce applicable Agency policies, procedures, standards, models, documents, and guidance that define the NASA IT environment; and 3) ensure the appropriate level confidentiality, integrity, and availability of information residing on, or processed by, NASA's automated information systems is achieved through the implementation and enforcement of risk- based policies, procedures, standards, guidelines, control techniques, and training mechanisms.

Applicable Documents, Other Resources

a. NASA Policy Directive (NPD) 2800.1, *Managing Information Technology*.

b. NASA Procedural Requirements (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. Binding Operational Directive 18-01, *Enhance Email and Web Security*

i. NASA-SPEC-2660 Version 1.0, *Email Infrastructure Security*

j. NASA-SPEC-2650 Version 3.0, *Transport Layer Security (TLS)*

k. NASA Email Service Requirements: https://sysadmin.nasa.gov/wiki/NASA-email-server-requirements.

l. Federal Information Processing Standard Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.

m. Federal Information Processing Standard Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*.

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

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

p. NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*.

q. NIST SP 800-45 Version 2, *Guidelines on Electronic Mail Security*.

r. NIST SP 800-53 Revision 4, *Recommended Security Controls for Federal Information Systems*.

s. NIST SP 800-81 Revision 2, *Secure Domain Name System (DNS) Deployment Guide*

t. NIST SP 800-177 Revision 1, *Trustworthy Email*.

u. Department of Homeland Security (DHS), Binding Operational Directive (BOD) 18-01, *Enhance Email and Web Security, October 6, 2017*.

v. National Archives Email Specific Guidance and Resources https://www.archives.gov/records-mgmt/email-management/email-guidance-and-resources.html

w. National Archives Universal Electronic Records Management (ERM) Requirements

x. NPR 1441.1E NASA Records Management Procedural Requirements

Measurement and Verification

None.

Replacement

NAII 2810.2 replaces NITR 2800.2, *Email Services and Email Forwarding*.

Requirements

1. The NASA Senior Agency Information Security Officer (SAISO) shall designate a NASA Agency Postmaster to:
   a. perform oversight and approval activities specified in this document;
   b. serve as a point of contact for program and project managers, system owners, contracting officers, and other decision makers regarding requirements for email systems and services; and
   c. ensure the NASA Applicable Document List (ADL) is updated to include reference to NAII 2810.2.
2. All NASA-badged personnel (including all civil servants as well as other personnel who have been granted a NASA internal email account) shall utilize an authorized NASA user electronic mail/messaging service for all email and calendaring to perform their NASA duties, with the following exceptions:

   a. This policy does not apply to external NASA partners from industry, academia, and other government agencies who may have NASA badges because they visit NASA facilities but whose primary duty station is external to NASA.
   b. Contractors may access their corporate messaging system for conducting contractor business (e.g. timecards, business notifications). Contracting officer representatives and project managers shall advise contractors on the degree to which contractors will use their corporate messaging system for receiving NASA data via email.
   c. NASA-badged personnel who do not utilize email and calendaring services in the course of their duties and do not have such services provisioned to them by NASA are exempt from this requirement.

3. Contractors or vendors that send email on behalf of NASA and/or to NASA users as part of their contracted or task service offering shall comply with the following requirements (to be included in their contract language):
   a. All NASA, partner, or contracted systems sending email on behalf of NASA and/or to NASA users shall undergo and comply with the requirements of Agency assessment, approval, and continuous monitoring processes consistent with NPR 2810.1.
   b. The NASA Cybersecurity & Privacy Division (CSPD) Security Assessment Team performing assessments on a system that will send email on behalf of NASA and/or to NASA users shall include the NASA Agency Postmaster or technical subject matter expert(s) designated by the Agency Postmaster. The Agency Postmaster may impose email-specific assessment and approval requirements on the target system as deemed necessary and appropriate - to include approvals specified in this NAII.
   c. Contracted services that send email on behalf of NASA and/or to NASA users shall comply with requirements imposed by NASA policy and Federal controls (including DHS BOD 18-01 and Federal Information Security Management Act (FISMA) controls), and document compliance according to the requirements in the System Security Plan (SSP).
   d. Any email sent by a contracted system or service on behalf of NASA and/or to NASA users as part of processes or functions specified in the contract shall use a nasa.gov domain; an external or non-NASA domain shall never be used.
4. System Owners must ensure that all logically internal NASA applications that send Internet email shall use either @nasa.gov or @mail.nasa.gov as the return address. However, automation use cases that cannot use @nasa.gov or @mail.nasa.gov must be approved by the Agency Postmaster in advance.
   a. Logically external applications and services, including @jpl.nasa.gov, shall use Agency approved domains that are provisioned in NASA DNS. Please contact the Agency Postmaster for more details.

5. System Owners must ensure that all Internet email to NASA shall be subject to NASA enterprise controlled anti-malware, anti-phishing, and spam tool review prior to allowing human or automated access. Tool configurations shall be based on the content receiver; different clients or email processing agents will likely need different protection.
6. The Postmaster will ensure that all NASA user email originating from an internal 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 NASA users' electronic mail/messaging service accounts may be set to authorized Government or Military email addresses with approval.
7. The Cybersecurity Standards and Engineering Team will ensure that only NASA authorized email servers will be able to relay NASA email to non-NASA email servers. Inbound and outbound port 25 traffic will be controlled with default deny rules at logical NASA perimeters (Trusted Internet Connections (TIC)) to allow email traffic only to authorized servers. All NASA email servers that accept email from non-NASA sources are expected to migrate to Internet Accessible zones as part of future network architecture improvements.
8. The Cybersecurity Standards and Engineering Team will ensure that all NASA email servers that allow email client access must be restricted to logically internal accessor through the use of a NASA VPN.
9. The System Owner shall ensure that the information system assessment and authorization requirements for NASA systems that send and forward email within NASA address space or for a NASA DNS domain shall include:
    a. documentation of the email data exchange and the NASA Agency Postmaster approval in the SSP and
    b. approval by the Authorizing Official (AO) in the form of an approved and signed Authorization to Operate.
10. System Owners of NASA email service providers must block or deny automatic forwards from a NASA email server to a non-NASA email server or account. Required SPF and DMARC rules for trustworthy email compromise consistent email delivery when using server-side forwarding rules. Automatic forwards risk the exposure of NASA information, and, therefore, NASA email service providers must monitor automatic forwarding from email clients.
    a. Selective and manual forwarding of individual email messages, which do not contain sensitive NASA information (i.e., privacy data or other controlled unclassified information), for review at home or to a business partner's email system is permissible.
11. The System Owner will ensure that all email services managed by NASA or in cooperation with NASA will meet the NASA retention requirements defined in NPR 1441.1E.
    a. SSP owners for email service providers must be responsible for section 2.10 of NPR 1441.1E.

   b. Providers of email services shall ensure familiarity with, and have processes in place, for compliance with section 5.4 of NPR 1441.1E

12. The Communications Program will ensure that all DNS management will be performed and controlled by the NASA OCIO.
    a. This requirement also pertains to all records for email services, including SPF, MX, and DMARC.
13. The Cybersecurity Standards and Engineering Team will ensure that all NASA procured email services, including logically internal and logically external will be subject to the Cybersecurity and Infrastructure Security Agency (CISA) National Cybersecurity Protection System, an intrusion prevention capability that includes email filtering; this is an element of the Einstein 3 Accelerated (E3A) system. Email services sending between trusted and untrusted NASA logical perimeters will pass through E3A.
14. The Postmaster will ensure that all NASA email services that are compliant with this policy will be considered “internal” delivery to NASA users. Emails originating from infrastructure that is external to Microsoft Office 365 or NASA Operational Messaging and Directory (NOMAD) will not be marked as “external” in subject fields if the email originated from a compliant authorized server. Any email service that is not compliant and delivering to the Enterprise email service will be marked “external.”
15. The System Owner shall ensure that prior to NASA authorization all email services need to be compliant with the requirements defined by the Cybersecurity Standards and Engineering Team (CSET), including configuration specifications for operating systems on any computers that are enumerated in the SSP of the offered email services. CSET configurations also include the following applicable specifications:
    a. NASA-SPEC-2650 Version 3.0, *Transport Layer Security (TLS)*
    b. NASA-SPEC-2660 Version 1.0, *Email Infrastructure Security*

Appendix A: Acronyms

ADL	Applicable Document List
AO	Authorizing Official
BOD	Binding Operational Directive
CIO	Chief Information Officer
CSET	Cybersecurity Standards and Engineering Team
CSPD	Cybersecurity & Privacy Division
DHS	Department of Homeland Security
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
E3A	Einstein 3 Accelerated, DHS system that detects and prevents intrusions
FISMA	Federal Information Security Management Act
IT	Information Technology
MX record	Mail Exchanger record**.** A Mail Exchanger record specifies the mail server responsible for accepting email messages on behalf of a domain name, it is a resource record in the Domain Name System (DNS)
NAII	NASA Advisory Implementing Instruction
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NITR	NASA Information Technology Requirement
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
SAISO	Senior Agency Information Security Officer
SP	Special Publication
SPF	Sender Policy Framework
SSP	System Security Plan, a document that identifies the functions and features of a system, including all its hardware and the software installed on the system
TIC	Trusted Internet Connections
TLS	Transport Layer Security