MEASUREMENT SYSTEM IDENTIFICATION

NASA TECHNICAL STANDARD

National Aeronautics and Space Administration

NASA-STD-2804
Fall 2017

Approved: February 9, 2018

Superseding NASA-STD-2804
Spring 2017

NASA-STD-2804 Fall 2017
MINIMUM INTEROPERABILITY SOFTWARE SUITE

DOCUMENT HISTORY LOG

Status	Document Revision	Approval Date	Description
Informal Draft	0.1	11/6/2017	Draft Release
Formal Draft	0.2	12/4/2017	Draft Release
Final Draft	0.3	2017-1-10	Draft Release
Baseline	1.0		Baseline Release

FOREWORD

This Standard is approved for use by NASA Headquarters and all NASA centers. It is intended to provide a common framework for consistent practices across NASA programs.

The material covered in this Standard is governed and approved by the NASA Chief Information Officer. Its purpose is to define the baseline software suite necessary to support interoperability and security both between NASA end user computing devices and within the NASA operating environment. The Standard establishes Client Reference Configurations, operating system standards, and compliance dates for computers running Microsoft Windows, macOS, Red Hat Enterprise Linux, and mobile operating systems. Adherence to this Standard ensures compliance with Federal requirements for desktop computers, laptops, and other end user devices.

Requests for information, corrections, or additions to this Standard should be directed to the John H. Glenn Research Center at Lewis Field (GRC), Enterprise Technology Assessments and Digital Standards (ETADS) Office, MS 142-5, Cleveland, OH, 44135 or to desktop-standards@lists.nasa.gov.

ROSCOE SHEEHY

Digitally signed by ROSCOE SHEEHY
Date: 2018.02.09 14:22:11 -06'00'

Roscoe Sheehy
End User Services Program Executive
ES&I

February 9, 2018

Approval Date

TABLE OF CONTENTS

LIST OF TABLES

1 SCOPE

1.1 Purpose

This Standard defines the baseline software suite necessary to support interoperability among NASA end user computing devices and within the NASA operating environment. The Standard establishes client reference configurations, operating system standards, and compliance dates for Agency physical and virtual system interoperability, including computers running Microsoft Windows, Apple macOS, Android, iOS, and Linux operating systems. Adherence to this Standard ensures compliance with Federal requirements for desktop computers, laptops, and other end user devices.

1.2 Applicability

This standard is applicable to Agency Consolidated End-User Services (ACES) systems and non-ACES end user systems at NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This standard applies to the Jet Propulsion Laboratory (JPL), a Federally Funded Research and Development Center (FFRDC), and other non-Agency facility contractors only to the extent specified or referenced in applicable contracts.

Center CIOs shall ensure that all NASA employees at their respective centers have access to an interoperable system that is equipped with a minimum software suite that meets the standards listed in Section 3.

NPR 2810.1A, Security of Information Technology, §1.2.1.10, clearly defines the role and responsibilities of information system owners (ISO) in maintaining Agency information systems. These responsibilities include:

- Acquiring, developing, integrating, operating, modifying, maintaining, and disposing of information systems.
- Ensuring system-level implementation of all Agency and Center requirements.
- Taking appropriate actions to identify and minimize or eliminate information system security deficiencies and weaknesses.

The Client Reference Configuration (CRC) establishes required functionality and required products necessary to meet minimum functionality. Future procurements intended to address this functionality are restricted to the products defined in the CRC. Licenses for products not included in the CRCs may not exist or may not be renewed. Products will be added, replaced, or removed as appropriate to address Agency interoperability requirements.

1.2.1 Assessments

Only software and hardware assessed by Enterprise Technology Assessments and Digital Standards (ETADS) for end user interoperability prior to enterprise implementation shall be included in NASA-STD-2804 and NASA-STD-2805, Minimum Hardware Configurations. The ETADS Assessment page features overviews of current and planned activities, and ETADS invites end user and security stakeholders to register for potential participation in current assessments, as well as propose potential enterprise tools for future assessment:

https://etads.nasa.gov/technology-assessments/

Applications that meet common Agency end user technology needs while providing enhanced usability, mitigating security risks, reducing support costs, and/or offering other tangible and scalable improvements may also be submitted to standards-comments@lists.nasa.gov for consideration in future revisions to these Standards.

When proposing assessments and additions, please keep in mind that the primary purposes of these Standards are to promote interoperability among all of NASA's computer systems and to provide a common baselines of functionality and security that future agency-wide applications can build upon. It is also important to note that this Standard applies to all interoperable end user systems throughout the Agency. Substantial costs may be involved in order to bring all agency systems into compliance with an additional feature, particularly if the addition involves hardware, and cost vs. benefits must be carefully considered.

Each participant in ETADS assessment testing must be an Agency technology professional and must provide his or her own testing machine.

1.3 Authority

The Agency Chief Information Officer (CIO) and Senior Agency Information Security Officer (SAISO) have authorized Enterprise Technology Assessments and Digital Standards (ETADS) within the ETADS Charter, §2, to create binding technical standards related to Agency interoperability and security topics.

The NASA Technical Standards Program (NTSP), sponsored by the Office of the NASA Chief Engineer, recognizes ETADS as a standards-developing organization within the Agency. NTSP provides access to all technical standards at:

https://standards.nasa.gov/

"Shall" statements in this document impose an obligation to act. "Shall not" statements generally prohibit an action. "Should" statements imply an obligation to act, but not a necessity.

2 Architectural Compliance Requirements

NPR 2800.1B, *Managing Information Technol*ogy, §4, provides for a NASA Enterprise Architecture (EA) and Information Resource Management (IRM) Strategic Plan. Several facets of this Standard support the current NASA EA and IRM Strategic Plan:

- The selection of standards for a broad and cost-effective infrastructure using commercial off-the-shelf and well-supported open source products to the greatest extent practical.
- Interoperability both within and when used remotely to NASA.
- Flexibility for future growth.
- Consistency with generally accepted consensus standards as much as feasible.
- Security for NASA systems and data.

In many cases, it is in NASA's best interest to specify commercial products as standard for an interoperable and secure implementation of a particular set of related and integrated functions. The products themselves often include additional functionality or proprietary extensions not specified by this Standard. While these products can be used to create higher-level interoperability solutions, these solutions may not be recognized as appropriate for interoperability or security within the context of the NASA interoperability environment and may be deprecated without warning by future revisions to this Standard. Users of this Standard are advised to apply appropriate caution when implementing proprietary or non-standard extensions, features, and functions that go beyond the explicitly stated functionality.

Per NPR 2800.1B, §6, this standard also assumes consistent technology infrastructure exists at the individual Center level to support and maintain listed products and configurations.

3 CLIENT REFERENCE CONFIGURATIONS

To address application, data, and infrastructure interoperability, as well as ensure compliance with Federally-mandated system configuration settings, the software functionality, applications, interface standards, configuration settings, versions, and deployment settings established by this Standard are represented as Client Reference Configurations (CRCs).

The CRCs define the common enterprise images that system owners shall deploy to all interoperable end user computing systems. All IT initiatives funded or endorsed by the NASA OCIO presume systems that conform to the CRCs. Application service providers and software developers should use the CRCs to assist with integration and acceptance testing. Each CRC and corresponding applications are considered approved on the date of CIO signing. Operating systems and CRCs are now detailed between default and legacy / sunsetting statuses:

- Default configurations should be considered for all new and refreshed end user computing systems. These default configurations should meet the need for most standard Agency end users and are intended to further modernize, standardize, and secure the Agency IT environment.
- Legacy / sunsetting configurations relate to operating systems that have been superseded by newer versions and / or are scheduled to lose functionality or vendor support within the Agency environment. Mission or corporate considerations, such as a lack of critical mission or enterprise application interoperability with a default operating system, may necessitate some users retaining a legacy configuration.

CRCs are included for each operating system, with the version numbers and required configurations that were current at the time of NASA-STD-2804 signing. Current available versions of listed applications must be used unless specifically stated otherwise. Interface standards are included to guide service providers and system integrators on specific application expectations. System administrators should deploy the latest version of a requested operating system, unless the customer explicitly requests another supported version of the operating system.

NASA-STD-2804 is published twice each year, and current recommended versions of applications may change in between edits and signings of this Standard. Managers for corporate

end user systems and enterprise management tools should consult application versions for supported operating systems and ensure ongoing maintenance:

https://etads.nasa.gov/operating-systems/

All operating systems and specific applications must adhere to Agency Security Configuration Standards (ASCS) configurations and be removed from systems by listed end of life dates:

https://etads.nasa.gov/ascs/

The Enterprise Service Desk (ESD) knowledge article "Base Services and General Services for ACES and Non-ACES Managed Systems" (KB0011257) clarifies applications and software in scope for Non-ACES enterprise licenses and support:

https://esd.nasa.gov/

3.1 Default Operating Systems for NASA End Users

Windows 10, macOS 10.12, and Red Hat Linux Enterprise (RHEL) 7 are the default operating systems for Agency end users.

3.1.1 Windows 10 Client Reference Configuration

Windows 10 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Operating System	Windows 10 Enterprise x64		NASA Security Configuration Settings (ASCS)	1703 Semi-Annual Channel	Remove by Oct. 9, 2018 (Microsoft end of support).
Applications, Plugins, and Tools					
Word Processing	Microsoft Word Professional	Office Open XML document format		2016	
Spreadsheet	Microsoft Excel Professional	Office Open XML document format		2016	
Presentation	Microsoft PowerPoint Professional	Office Open XML document format		2016	

Windows 10 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Electronic Mail and Calendaring	Microsoft Outlook Professional	NOMAD EWS over TLS; NOMAD GAL over TLS; S/MIME with PIV/Agency Smart Badge (ASB); MAPI over HTTP; iCalendar (RFC 5545)	NASA Security Configuration Settings (ASCS); configured to use NOMAD, NASA PIV/ASB, and GAL Directory service	2016	
Instant Messaging	Pidgin	XMPP	NASA Jabber Service; Pidgin-sipe OCS plug-in	2.10.x	
Instant Messaging and Web Conferencing	Microsoft Skype for Business	SIP	NASA Security Configuration Settings (ASCS); enterprise OCS Settings; configured for access to NOMAD; Pidgin-sipe OCS plugin	2016	
PDF Viewer and Electronic Forms	Adobe Acrobat Reader DC	Adobe PDF specification	Connection to cloud disabled	2017	Configured to open in Internet Explorer.
Java	Java run-time environment (JRE)		AES256 strong crypto	Java 8	
Browsers					
Web Browser	Microsoft Internet Explorer	W3C and industry standards	NASA Security Configuration Settings (ASCS)	11. x	
Web Browser	Microsoft Edge	W3C and industry standards	NASA Security Configuration Settings (ASCS); auto-updates enabled	Semi-Annual Channel	Bundled with OS. Limited interoperability. See section 6.2
Web Browser	Google Chrome	W3C and industry standards	NASA Security Configuration Settings (ASCS); auto-updates enabled	62.x	

Windows 10 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Web Browser	Mozilla Firefox Extended Support Release	W3C and industry standards	NASA Security Configuration Settings (ASCS); NFCE 2017.x or higher; see section 7.3; auto-updates enabled	52.x	Users may consider installing NASA Firefox Configuration Extension (NFCE) to streamline and simplify browser configuration of trusts and authentication. This extension will likely lose effectiveness with the release of 52.5 in spring 2018, or in a subsequent release. Spring 2018 vendor updates to this browser are likely to remove plug-ins that provide interoperability with Agency applications. See Section 6.3 for additional detail.
ICAM					
Smartcard Middleware	ActivClient	NIST SP 800-73 Part 4	OS PIV guidance; see sections 7.1 and 7.6	7.1.x	DSI version 4.1.x
Trust Anchor Management	NASA Trust Anchor Management	X.509	See section 7.3	2017.x	
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)	PKCS; W3C and industry standards		2017.x	
Security					
Firewall	Windows Firewall				
Anti-Virus and Anti-Malware	Symantec Endpoint Protection		Enterprise update server	14.x	

Windows 10 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Data at Rest Full Disk Encryption	Microsoft BitLocker		Configured to use key escrow		For key escrow enablement, non-ACES administrators will need to install the Symantec SEEM client on their computers. Once the installation is complete, the Windows 10 computer will encrypt the drive with BitLocker, prompt the user for a PIN and automatically send the recovery key to the SEEM server. If a BitLocker recovery key is required, the user only needs to contact the ESD helpdesk. BitLocker data at rest encryption is a base service provided by ACES. No costs are associated with obtaining this support.
Configuration Settings Management and Software Asset Management	IBM Endpoint Security (BigFix)		Auto-updates enabled	9.x	
Incident Monitoring and Response	FireEye HX		Auto-updates enabled	25.12	
Whitelisting	RES		Auto-updates enabled		

Windows 10 NASA Optional Supported Software					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Date**
Access to Centrally Served Windows Applications	Citrix Receiver for Windows			4.4.x	
Audio / Video Player	Adobe Flash Player	Flash SWF		27.x	
Audio / Video Player	Apple iTunes	Various multimedia		12.x	
Audio / Video Player	Microsoft Silverlight	Various multimedia		5.1.x	Remove by 10/12/2021.
Audio / Video Player	VLC	Various multimedia		2.2.8	Included to support legacy video codec playback capabilities. Compensates for Windows Media Player, which did not include legacy codecs like MPEG-2 in this Windows 10 release.
Content Encryption	Entrust ESP for Windows	S/MIME	See Section 7.4.	10.x	
Database	Microsoft Access			2016	
Desktop Publishing	Microsoft Publisher			2016	
File Archiver	7-Zip			18.01	
Note Taking	Microsoft OneNote Professional	Office Open XML document format	Connection to cloud disabled	2016	
PDF Creator	Adobe Acrobat Pro DC	Adobe PDF specification	Connection to cloud disabled; configured to open in Internet Explorer	2017	
Project Management	Microsoft Project			2016	See Section 5.1.1 for installation instructions.
SFTP	WinSCP		Auto-updates enabled	5.11.x	Also requires PuTTY-CAC and ActivClient for functionality.

Windows 10 NASA Optional Supported Software					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Date**
SSH	PuTTY-CAC		Auto-updates enabled	Current baseline	
Softphone Client	Cisco Jabber	SIP/RTP	For softphone use only	11.8.x	
Virtualization	WMWare Workstation			12.x	
Workflow	Microsoft Visio			2016	See section 5.1.1 for installation instructions.

3.1.2 macOS 10.12 Client Reference Configuration

macOS 10.12 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Operating System	macOS		NASA Security Configuration Settings (ASCS)	10.12.x	
Applications, Plugins, and Tools					
Word Processing	Microsoft Word 2016 for Mac	Office Open XML document format		Word 2016 15.x	
Spreadsheet	Microsoft Excel 2016 for Mac	Office Open XML document format		Excel 2016 15.x	
Presentation	Microsoft PowerPoint 2016 for Mac	Office Open XML document format		PowerPoint 2016 15.x	
Secure Electronic Mail and Calendaring	Microsoft Outlook 2016 for Mac	NOMAD EWS over TLS; NOMAD GAL over TLS; S/MIME with PIV/Agency Smart Badge (ASB)	NASA Security Configuration Settings (ASCS); configured to use NOMAD, NASA PIV/ASB, and GAL Directory service	Outlook 2016 15.x	Outlook is the only ICAM-supported email client for Mac; requires ActiveClient for Mac middleware, listed below in ICAM section of this CRC.

macOS 10.12 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Instant Messaging and Web Conferencing	Microsoft Skype for Business	SIP	Configured for access to NOMAD	6.x	
Instant Messaging	Apple Messages	XMPP		11.x	
PDF Viewer and Electronic Forms	Adobe Acrobat Reader DC	Adobe PDF specification	Connection to cloud disabled	2017	Open documents in Safari
Java	Oracle Java run-time environment (JRE)		AES256 Strong Crypto	Java 8	
Multimedia Player	Apple iTunes	Various Multimedia	Default for all supported formats	12.7.x	
Audio / Video Player	Apple QuickTime Player	Various Multimedia	Default for QuickTime formats	10.4.x	
Browsers					
Web Browser	Apple Safari	W3C and industry standards	NASA Security Configuration Settings (ASCS); auto-updates enabled	11.x	
Web Browser	Google Chrome	W3C and industry standards	NASA Security Configuration Settings (ASCS); auto-updates enabled	62.x	

macOS 10.12 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Web Browser	Mozilla Firefox Extended Support Release (ESR)	W3C and industry standards	NASA Security Configuration Settings (ASCS); NFCE 2017.x or higher; See section 7; auto-updates enabled	52.x	Users may consider installing NASA Firefox Configuration Extension (NFCE) to streamline and simplify browser configuration of trusts and authentication. This extension will likely lose effectiveness with and beyond Release 52.5 in spring 2018. Spring 2018 vendor updates to this browser are also likely to remove plug-ins that provide interoperability with Agency applications. See Section 6.3 for additional detail.

macOS 10.12 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
ICAM					
Authentication Client	Enterprise Connect			1.x	This is baseline software to enable PIV-M native pairing operation and compliance, but other acceptable, federally-compliant authentication solutions may exist and be applied at the discretion of the ISO and Authorizing Official. Centrify is also listed as an optional solution later in Section 3.1.2.
Smartcard Middleware	ActivClient for Mac	NIST SP 800-73 Part 4	OS PIV guidance; see sections 7.1 and 7.6	4.0.1.88	
Trust Anchor Management	NASA Trust Anchor Management	X.509	See section 7.3	2017.x	
Security					
Firewall	Apple Firewall		NASA Security Configuration Settings (ASCS); allow signed software; enable firewall logging		
Anti-Virus and Anti-Malware	Symantec Endpoint Protection for Mac		Enterprise update server	14.x	RU 6 or newer

macOS 10.12 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Data at Rest Full Disk Encryption	FileVault 2		Configured to use key escrow; see section 8.3	FileVault2 - bundled	For key escrow enablement, non-ACES administrators will need to install the Symantec SEEM client on their computers. Once the installation is complete, the Mac computer will encrypt the drive with FileVault, prompt the user for a PIN and automatically send the recovery key to the SEEM server. If a FileVault recovery key is required, the user only needs to contact the ESD helpdesk. FileVault data at rest encryption is a base service provided by ACES. No costs are associated with obtaining this support.
Configuration Settings Management and Software Asset Management	IBM Endpoint Security (BigFix)		Auto-updates enabled	9.x	

macOS 10.12 NASA Optional Supported Software					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Date**
Access to Centrally Served Windows Applications	Citrix Receiver for Mac			12.7	
Audio / Video Player	Adobe Flash Player	Flash SWF		27.x	
Audio / Video Player	Microsoft Silverlight	Various Multimedia		5.x	Remove by 10/12/2021.
Audio / Video Player	VLC			2.x	
Authentication Client	Centrify		4-Cert PIV Smartcard required	2016.1	Optional solution for PIV-M native pairing operation and compliance; for more information, visit https://aces.ndc.nasa.gov/subnav/os-mac.html. System owners should consult ASCS guidance and their individual security plan(s) to determine which option will meet Agency requirements for federal PIV-M authentication compliance for their systems.
Content Encryption	Entrust Secure Desktop for Mac (SDM)	S/MIME	Configured for access to NOMAD; see Section 7.4	Outlook 15.x; SDM 8.1.x build 5 or later	Does not support file and folder encryption using FIPS 201-2 smartcards.
Instant Messaging	Adium	XMPP	NASA Jabber service; Pidgin-sipe OCS plug-in	1.5.x	
Project Management	Open Proj			1.7.x	
Softphone Client	Cisco Jabber	SIP/RTP	For softphone use only	11.8.x	

macOS 10.12 NASA Optional Supported Software					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Date**
Virtualization	VMware Fusion			8.5.x	

3.1.3 RHEL 7 Client Reference Configuration

Use most recent versions of software available that are compatible with your system configuration. Software updates shall be applied to systems as they become available:

Red Hat Product Lifecycle (https://access.redhat.com/support/policy/updates/errata)

RHEL 7 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Operating System	Red Hat Linux Workstation		NASA Security Configuration Settings (ASCS)	≥7.4 Update source: Red Hat	RHEL systems shall shall be installed and maintained with FIPS mode enabled.
Applications, Plugins, and Tools					
Office Automation	LibreOffice	Oasis Open Document Format	Configured to use Office Open XML file format by default.		
Secure Electronic Mail	Mozilla Thunderbird	NOMAD EWS over TLS; NOMAD GAL over TLS; S/MIME with PIV/ASB.	Configured for access to NOMAD.		
Calendaring	Microsoft Outlook Web Access (NOMAD)	iCalendar (RFC 5545)			Accessible via web browser.
Instant Messaging	Pidgin	XMPP			Requires pidgin-sipe plugin for Skype for Business.
Web Conferencing			No support for Linux clients		
PDF Viewer	Evince Document Viewer	Adobe PDF specification			
Electronic Forms	No current standard solution. See Section 5.3.		No support for Linux clients		

RHEL 7 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Java	Java Run-time Environment (JRE) – java-1.8.0-opendjk	Java specifications	With Java Cryptography Extension (JCE); Unlimited Strength Jurisdiction Policy Files installed	Java 8	
Browsers					
Web Browser	Mozilla Firefox Extended Support Release (ESR)	W3C and industry standards	NASA Security Configuration Settings (ASCS); see Section 7.3; auto-updates enabled	52.x	Users may consider installing NASA Firefox Configuration Extension (NFCE) to streamline and simplify browser configuration of trusts and authentication. This extension will likely lose effectiveness with the release of 52.5 in spring 2018, or in a subsequent release. Spring 2018 vendor updates to this browser are likely to remove plug-ins that provide interoperability with Agency applications. See Section 6.3 for additional detail.
Web Browser	Google Chrome	W3C and industry standards	NASA Security Configuration Settings (ASCS); auto-updates enabled	62.x	
ICAM					
Smartcard Middleware	Open SC	NIST SP 800-73 Part 4	OS PIV guidance; see sections 7.1 and 7.6		
Trust Anchor Management	NASA Trust Anchor Management	X.509	See section 7.3	≥2017.x Update source: NASA ETADS	Lacks auto-update

RHEL 7 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)	PKCS; W3C and industry standards		≥2017.x Update source: NASA ETADS	Lacks extension auto-update (trust anchors are updated automatically)
Security					
Firewall	System-config-firewall		Enable control of inbound and outbound connections.		Used in conjunction with iptables.
Anti-Virus	Symantec Endpoint Protection		Enterprise update server	14.x	ClamAV may be a suitable alternative at the system owner's discretion.
Data at Rest Encryption	Linux Unified Key Setup (LUKS)		Configured to use key escrow when available.		
Configuration Settings Management and Software Asset Management	IBM Endpoint Security (BigFix)		Auto-updates enabled	≥9.x	
Whitelisting	RES		Auto-updates enabled		

RHEL 7 NASA Optional Supported Software					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Date**
Access to Centrally-Served Windows Applications	Windows Receiver			≥14.x of wfica32 .exe	
Anti-Virus	ClamAV				
Data at Rest Encryption	Symantec Drive Encryption for Linux		Configured to use key escrow when available.		

RHEL 7 NASA Optional Supported Software					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Date**
Electronic Mail	Evolution	IMAP4, SMTP, IMAP over TLS			
Java	Oracle Java Run-time Environment (JRE)	Java specifications	With Java Cryptography Extension (JCE); Unlimited Strength Jurisdiction Policy Files installed	Java 8 Update source: Oracle	

3.2 Legacy and Sunsetting Operating Systems for NASA End Users

Windows 7, macOS 10.11, and Red Hat Linux Enterprise (RHEL) 6 are operating systems that are approaching end-of-life for Agency end users.

3.2.1 Windows 7 Client Reference Configuration

Windows 7 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Operating System	Windows 7 Enterprise or Ultimate X64 Edition		NASA Security Configuration Settings (ASCS)	SP1	No new installs; removal required by 7/1/2018.
Applications, Plugins, and Tools					
Word Processing	Microsoft Word Professional	Office Open XML document format		2016	
Spreadsheet	Microsoft Excel Professional	Office Open XML document format		2016	
Presentation	Microsoft PowerPoint Professional	Office Open XML document format		2016	
Secure Electronic Mail and Calendaring	Microsoft Outlook Professional	NOMAD EWS over TLS; NOMAD GAL over TLS; S/MIME with PIV/Agency Smart Badge (ASB); iCalendar (RFC 5545)	NASA Security Configuration Settings (ASCS); configured to use NOMAD, NASA PIV/ASB, and GAL Directory service	2016	Requires Entrust ESP Outlook Plug-in.

Windows 7 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Secure Electronic Mail	Entrust ESP Outlook Plug-In	S/MIME	NASA Security Configuration Settings (ASCS); see section 7.4	9.3	
Instant Messaging and Web Conferencing	Microsoft Skype for Business	SIP	NASA Security Configuration Settings (ASCS); enterprise OCS Settings; configured for access to NOMAD; Pidgin-sipe OCS plugin	2016	
PDF Viewer and Electronic Forms	Adobe Acrobat Reader DC	Adobe PDF specification	Connection to cloud disabled	2017	Configured to open in Internet Explorer
Java	Oracle Java Run-time Environment (JRE)		AES256 strong crypto	Java 8	
Browsers					
Web Browser	Microsoft Internet Explorer	W3C and industry standards	NASA Security Configuration Settings (ASCS); See Section 7	11.x	
Web Browser	Google Chrome	W3C and industry standards	NASA Security Configuration Settings (ASCS); see section 7; auto-update on	62.x	

Windows 7 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Web Browser	Mozilla Firefox Extended Support Release	W3C and industry standards	NASA Security Configuration Settings (ASCS); NFCE v2017.x or higher; see auto-updates enabled	52.x	Users may consider installing NASA Firefox Configuration Extension (NFCE) to streamline and simplify browser configuration of trusts and authentication. This extension will likely lose effectiveness with and beyond Release 52.5 in spring 2018. Spring 2018 vendor updates to this browser are also likely to remove plug-ins that provide interoperability with Agency applications. See Section 6.3 for additional detail.
ICAM					
Smartcard Middleware	ActivClient	NIST SP 800-73 Part 4	OS PIV guidance; see sections 7.1 and 7.6	7.x	DSI version 3.4.x
Content Encryption	Entrust ESP for Windows	S/MIME	See section 7.4	9.x	
Trust Anchor Management	NASA Trust Anchor Management	X.509	See section 7.3	2017.x	
Security					
Firewall	Windows Firewall				
Anti-Virus and Anti-Malware	Symantec Endpoint Protection		Enterprise update server	14.x	
Data at Rest Full Disk Encryption	Symantec PGP Whole Disk Encryption		Configured to use key escrow	10.3.x (PGP)	

Windows 7 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Configuration Settings Management and Software Asset Management	IBM Endpoint Security (BigFix)		Auto-updates enabled	9.x	
Incident Monitoring and Response	FireEye HX		Auto-updates enabled	25.12	
Whitelisting	RES		Auto-updates enabled		
Vulnerability Protection	Enhanced Mitigation Experience Toolkit (EMET)		NASA Security Configuration Settings (ASCS)	5.52	

Windows 7 NASA Optional Supported Software					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Date**
Access to Centrally-Served Windows Applications	Citrix Receiver for Windows			4.9.x	
Audio / Video Player	Adobe Flash Player	Flash SWF		27.x	
Audio / Video Player	Apple iTunes	Various multimedia		12.x	
Audio / Video Player	Microsoft Silverlight	Various multimedia		5.1.x	Remove by 10/12/2021.
Database	Microsoft Access			2016	
Desktop Publishing	Microsoft Publisher			2016	
Instant Messaging	Pidgin	XMPP	NASA Jabber Service; Pidgin-sipe OCS plugin	2.10.x	
Note Taking	Microsoft OneNote Professional	Office Open XML document format		2016	

Windows 7 NASA Optional Supported Software					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Date**
PDF Creator	Adobe Acrobat Pro DC	Adobe PDF specification	Connection to cloud disabled; configured to open in Internet Explorer	2017	
Project Management	Microsoft Project			2016	See section 5.1.1 for installation instructions.
Softphone Client	Cisco Jabber	SIP/RTP	For softphone use only	11.8.x	
Virtualization	VMware Workstation Pro			14.x	VMWare Tools must be installed.
Workflow	Microsoft Visio			2016	See section 5.1.1 for installation instructions.

3.2.2 RHEL 6 Client Reference Configuration

Use most recent versions of software available that are compatible with your system configuration. Software updates shall be applied to systems as they become available:

Red Hat Product Lifecycle (https://access.redhat.com/support/policy/updates/errata)

RHEL 6 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Operating System	Red Hat Linux Workstation		NASA Security Configuration Settings (ASCS)	≥6.9 Update source: Red Hat	No new installs; must be removed from NASA user systems by 11/30/20. RHEL 6.9 will be the final version of this operating system. Existing RHEL systems shall have FIPS mode enabled.

RHEL 6 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Applications, Plugins, and Tools					
Office Automation	LibreOffice	Oasis Open Document Format	Configured to use Office Open XML file format by default.		
Secure Electronic Mail	Mozilla Thunderbird	NOMAD EWS over TLS; NOMAD GAL over TLS; S/MIME with PIV/ASB.	Configured for access to NOMAD.		
Calendaring	Microsoft Outlook Web Access (NOMAD)	iCalendar (RFC 5545)			Accessible via web browser.
Instant Messaging	Pidgin	XMPP			Requires pidgin-sipe plugin for Skype for Business.
Web Conferencing			No support for Linux clients		
Electronic Forms	No current standard solution. See Section 5.3.		No support for Linux clients		
Java	Java Run-time Environment (JRE)	Java specifications	With Java Cryptography Extension (JCE); Unlimited Strength Jurisdiction Policy Files installed	Java 8	
Browsers					
Web Browser	Chromium-browser				Google Chrome is not available.

RHEL 6 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Web Browser	Mozilla Firefox Extended Support Release (ESR)	W3C and industry standards	NASA Security Configuration Settings (ASCS); see Section 7.3; auto-updates enabled	52.x	Users may consider installing NASA Firefox Configuration Extension (NFCE) to streamline and simplify browser configuration of trusts and authentication. This extension will likely lose effectiveness with the release of 52.5 in spring 2018, or in a subsequent release. Spring 2018 vendor updates to this browser are likely to remove plug-ins that provide interoperability with Agency applications. See Section 6.3 for additional detail.
ICAM					
Smartcard Middleware	Open SC	NIST SP 800-73 Part 4	OS PIV guidance; see sections 7.1 and 7.6		
Trust Anchor Management	NASA Trust Anchor Management	X.509	See section 7.3	≥2017.x Update source: NASA ETADS	Lacks auto-update
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)	PKCS; W3C and industry standards		≥2017.x Update source: NASA ETADS	Lacks extension auto-update (trust anchors are updated automatically)
Security					
Firewall	System-config-firewall		Enable control of inbound and outbound connections.		Used in conjunction with iptables.

RHEL 6 NASA Core Build					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Dates**
Anti-Virus	ClamAV		Enterprise update server		Other suitable anti-virus alternatives may exist based on system needs and configurations.
Data at Rest Encryption	Linux Unified Key Setup (LUKS)		Configured to use key escrow when available.		
Configuration Settings Management and Software Asset Management	IBM Endpoint Security (BigFix)		Auto-updates enabled	≥9.x	
Whitelisting	RES		Auto-updates enabled		

RHEL 6 NASA Optional Supported Software					
Function	**Application**	**Relevant Standards**	**Required Settings**	**Version**	**Comments & Required Removal Date**
Access to Centrally-Served Windows Applications	Windows Receiver			≥14.x of wfica32 .exe	
Electronic Mail	Evolution	IMAP4, SMTP, IMAP over TLS			
Java	Oracle Java Run-time Environment (JRE)	Java specifications	With Java Cryptography Extension (JCE); Unlimited Strength Jurisdiction Policy Files installed	Java 8 Update source: Oracle	
PDF Creator	Scribus	Adobe PDF specification			

3.3 Client Reference Configuration for Mobile Computing Systems

Client Reference Configuration for Mobile Computing Systems			
Functionality	**Application**	**Required Settings**	**Version**
Operating System	iOS	NASA Security Configuration Settings (ASCS)	11.x
Operating System	Android	NASA Security Configuration Settings (ASCS)	7.x
Mobile Device Management	MaaS360	NASA Security Configuration Settings (ASCS)	10.x

4 Operating Systems

4.1 Operating System Standards, Timelines, and Compliance Dates

ASCS investigates and identifies the applications and operating system versions that are unsupported by the vendor or signify an imminent threat due to unpatched vulnerabilities. The software life cycle status for supported software can be found on the ASCS website at:

https://etads.nasa.gov/ascs/software-life-cycle/

4.2 Microsoft Windows

The Windows firewall must be enabled for all versions of the Windows operating system. All Windows systems must meet the NASA Baseline Security Configurations, which ensure compliance with FISMA requirements.

Microsoft Windows Timeline	
Windows Version	**Guidance**
Windows 10 , 1703 Semi-Annual Channel (SAC)	Approved for use as default operating system.
Windows 7	Approved for use. No new installs after July 1, 2017. Removal required by July 1, 2018.

4.2.1 Microsoft Windows 7

The editions of Windows 7 approved for use are the Enterprise and Ultimate editions. The 64-bit version of Microsoft Windows 7 is the default version of Windows approved for use. The 32-bit version of Microsoft Windows 7 may be installed if necessary to support non-64 bit capable

applications that only run on the 32-bit version. All Windows 7 systems must be removed from the environment or upgraded to Windows 10 by July 1, 2018.

4.2.2 Windows 10

Windows 10 Enterprise, 1703 SAC, or an assessed and approved version of 1709 SAC (anticipated in the Spring 2018 NASA-STD-2804 document) shall be required on all Windows systems as of July 1, 2018.

The 64-bit version of Microsoft Windows 10 is the default version of Windows approved for use. The 32-bit version of Microsoft Windows 10 may be installed if necessary to support non-64 bit capable applications that only run on the 32-bit version.

4.3 macOS

For all versions of Apple operating systems, the Apple firewall must be enabled. All Apple systems must meet the NASA Baseline Security Configurations.

The Agency has identified deficiencies in macOS 10.13 that introduce significant interoperability concerns. Vendor fixes for some macOS 10.13 challenges and validation of the updates by ETADS will continue into March 2018. As a result, macOS 10.13 is not included in this Standard update. The operating system will continue to be assessed and may be included in an addendum to this Standard once interoperability concerns have been resolved.

macOS timeline	
OS Version	**Guidance**
10.12 Sierra	Approved for use on all systems as of March 10, 2017. Default for all macOS systems.
10.13 High Sierra	Shall not be deployed on any new or refreshed systems upon signing.

4.4 Linux

All new and refreshed Linux systems must run a supported Red Hat Enterprise Linux distribution. Vendor-provided and -supported versions of applications shall be used. The version of application the vendor provides in their update stream shall supersede any listed in the CRC.

4.4.1 Red Hat

The default Red Hat Linux distribution for use on interoperable systems is Red Hat Enterprise Linux Desktop 7 with Workstation option on all new and refreshed systems. More information is available at:

http://www.redhat.com/rhel/desktop

RHEL 6.9 with workstation option is approved for use, but shall not be deployed to new or refreshed user systems, and it must be removed from NASA user systems by November 30,

2020. System owners should make a reasonable effort to upgrade their systems to RHEL 7 in the interim.

4.5 Mobile

The minimum iOS version is 11.1, and the current Android version is 7.0 ("Nougat").

The mobile operating systems supported shall apply NASA baseline security settings. All Android and iOS operating systems are required to be maintained to current supported vendor operating system versions.

With the implementation of the Mobile Device Management (MDM) Project's Certificate Lifecycle Management (CLM) (Phase 2) in summer 2017 for ACES-managed mobile devices, the following additional requirements shall apply:

- ACES mobile users must enroll in MDM via Mobile Device Registration (MDT).
    - This requires the user have a PIV card. MDM delivers additional certificates to the device for email and WiFi authentication and email encryption capability.
- MaaS360 secure container shall support NASA Microsoft Exchange email, calendar, and contacts.
- Mobile device PIN and MaaS360 secure container PIN, shall be a minimum of eight characters.
- Centralized management via MaaS360 policies with specific support for remote wipe capability, certificate management, and secure container locking after predetermined number of bad passcode attempts must be enabled.
- A native network supplicant requirement for EAP-TLS authentication to support WiFi authentication shall be observed.
- NASA data shall not be stored or used outside of the MDM secure container.
- Devices shall not be modified to circumvent the manufacturer's operating system security features, e.g., "jailbreak" or "root".
- A registered ACES mobile device shall not be used as the sole repository for NASA data; this will assure data are not irretrievable if the device is erased or lost.
- NASA delivered apps, policies or configuration shall not be modified.
- Registered mobile devices which are lost, stolen or compromised must be immediately reported to NASA's Security Operations Center at 1-877-NASA-SEC (1-877-627-2732).

Future Expected Updates: The MDM Project, Application Lifecycle Management (ALM), Phase 3, anticipates enabling mobile enterprise management of commercial-off-the-shelf, government-off-the-shelf, and custom enterprise applications utilized by NASA's workforce and stakeholders by early 2018. Additionally, it is likely that only Apple (iOS) and Samsung (Android OS) mobile devices will be approved and supported in the Agency environment in the future. These manufacturers' native cryptography supports both Agency security standards and MDM requirements for third-party applications. Specific hardware details are included in NASA-STD-2805.

4.5.1 Mobile Hotspots

ACES provides wifi hotspot options for Agency cell phone users who are seeking to enable network sharing with other NASA laptops and tablets. Please consult the ACES service catalogue for options.

5 APPLICATIONS

5.1 Office Automation Applications

The default document format for Microsoft Office and LibreOffice is the International Standards Organization's Standard Office Open XML format.

5.1.1 Office 2016 for Windows

Microsoft Office Professional 2016 is approved for use and is the default office automation version on interoperable Windows systems. Microsoft recommends the 32-bit application package for maximum legacy interoperability, but the 64-bit package is available and supported.

Office 2016 is typically installed on Agency hardware by two methods:

- Microsoft Installer (MSI), for mass deployments, and used by ACES.
- .exe install files, or "click-to-run" files, typically used for O365 and retail software instances, and often used for non-ACES installs.

MSI and click-to-run versions of Microsoft Office 2016 installation files are currently incompatible. A system owner or user seeking to install Microsoft Project 2016 or Microsoft Visio 2016 must use the same installation method that was used to install the core Office 2016 for Windows application on the machine, i.e. install the MSI version of Project/Visio 2016 with MSI versions of Office 2016, and the click-to-run versions of Project/Visio 2016 with click-to-run versions of Office 2016.

5.1.2 Office 2016 for Mac

Office 2016 for Mac is approved for use and is the default office automation version on interoperable macOS systems.

5.1.3 LibreOffice

LibreOffice 5 is approved for deployment on all interoperable RHEL 7 systems. There continue to be data format interoperability and rendering issues between Microsoft Office and Libre Office.

5.1.4 Collaboration Solutions

Future Expected Updates: OCIO has approved Microsoft O365 for implementation, and the solution is expected to include enterprise email, calendaring, instant messaging, and online file storage via EUSO. Implementation timeframes are currently being finalized. Additional services, including next-generation conferencing and document management, continue to be explored by

the Agency Collaboration working group. NASA anticipates significant changes will be required to our software licensing approach, end user training and outreach, and communications.

5.2 Electronic Messaging

The Agency NOMAD service provides integrated email, calendaring, scheduling, contact management, instant messaging, and web conferencing. All interoperable end user computing systems are required to be configured to access the NOMAD services.

Microsoft Outlook is the only email and calendaring solution fully supported by ICAM.

5.3 Electronic Forms

The design and control of forms (Agency level / NASA forms, Center forms, and organization forms) is addressed in NPD 1420.1, *NASA Forms Management*. NASA uses an Agency-wide, Adobe-integrated solution that supports NASA business practices, embraces technology and innovation, and increases efficiency.

The NASA Electronic Forms System (NEFS) portal, which serves as the central repository for all Agency-level/NASA forms and Center-level forms, is available at:

https://nef.nasa.gov/

To access and fill form templates designed via the Adobe LiveCycle forms solution, end-user systems currently require the following applications on the Windows 7 / 10 or macOS 10.12 operating systems:

- Adobe Reader DC
- Standard NASA supported browser (configured to open Adobe Reader DC PDF documents)
    - Windows 7 /10: Internet Explorer (use with Edge browser is not recommended)
    - macOS 10.12: Safari

Plug-ins or other external software are often incompatible with or breaks features of NASA forms, such as signing, as does using or manipulating them within applications like Mac Preview or third-party .pdf editors. NASA forms are records and are intended to be used as-is with standard supporting software.

4-cert FIPS 201-2 smartcards are compatible with digital signature.

Linux operating systems and the Google Chrome and Mozilla Firefox browsers currently do not natively support Adobe Reader DC functionality.

5.4 SATERN

SATERN is currently being replatformed to a Software-as-a-Service (Saas) solution. NSSC has confirmed that this cloud-based, FedRAMP-approved solution will work with the standard operating systems and browsers included in Section 3 of this document. This functionality is

expected in spring 2018. There is no support for Linux clients until this transition, per SATERN Client Platforms Version 2.0 (May 2016).

5.5 Virtualization

Virtualization technology allows multiple operating systems to be run on a single physical computer. If a virtualization product is needed for interoperability, the current version of VMware for the respective operating system shall be used. The software listed in the Section 3 Client Reference Configuration for the virtualized operating system must be installed and configured as required by the system security plan.

5.6 Optional Software for Mobile Computing Devices

Optional software for mobile devices that provides useful functionality is available at:

https://apps.nasa.gov/applist

6 WEB BROWSERS

No single browser meets the needs of the Agency. Google Chrome must be available on all new or refreshed Windows, macOS and RHEL 7 interoperable end user systems. Internet Explorer and Edge (for Windows 10 only) shall be made available on Agency interoperable Windows systems; Safari shall be made available on Agency interoperable Macs; and Firefox ESR shall be made available on Linux systems.

To avoid inefficiencies and interoperability issues, NASA must adjust to the rapid pace of browser enhancements resulting in new versions from the browser vendors. For Internet Explorer and Edge, NASA shall maintain support for the most recent production version. Firefox ESR shall be configured to automatically update with point releases for security updates only. Chrome shall automatically update in the background as designed by Google.

Browsers should be configured with the Agency approved NASA Client Trust Reference (NCTR) list of trusted sites anchors. For additional information, see Section 7, “ICAM Device Integration”. Please refer to the internal ETADS IDI pages for all related up-to-date browser configuration guidance:

http://etads.nasa.gov/idi/nctr/

Web authors, application providers, and system integrators must ensure that their web sites are validated against W3C Markup Validation Service and discontinue the use of checking client browsers for specific versions before granting access.

NASA Security Configuration Specifications shall be used for all approved browsers:

https://etads.nasa.gov/ascs/security-configuration-specifications/

Web application developers should note that browser vendors have dropped support, or are dropping support, for Adobe Flash and NPAPI, impacting plugins for Silverlight, Java applets, Facebook Video and other similar applications. Chrome no longer supports NPAPI, and Mozilla intends to fully remove support for most NPAPI plugins in Firefox ESR in 2018.

6.1 Microsoft Internet Explorer

Internet Explorer is approved for use on interoperable Windows systems.

6.2 Microsoft Edge

Microsoft Edge is bundled with Windows 10, but it is not recommended as the primary browser on those systems due to potential interoperability issues with older Web-based Agency applications.

6.3 Mozilla Firefox Extended Support Release

Mozilla Firefox ESR's NPAPI support will end in 2018, reducing its value differentiation within the Agency browser set. It continues to be the most difficult browser to integrate with ICAM services and smartcard-based authentication requirements.

With the release of Firefox 57 / Firefox ESR 52.5 or subsequent releases of the browser, Firefox configuration is moving to WebExtensions exclusively and no longer will load other extension types. NASA Firefox Configuration Extension (NFCE) may no longer function, and it will cease to be supported beyond Firefox ESR 52.5. NFCE remains listed as an optional software enhancement for the Firefox browser. Manual instructions for configuration will be added to the Firefox application page on the ETADS website before NFCE support is dropped:

https://etads.nasa.gov/application/mozilla-firefox-extended-support-release-esr-52-x/

6.4 Apple Safari

Safari is approved for use on all interoperable macOS systems.

6.5 Google Chrome

Google Chrome is approved for use on all interoperable Windows, macOS, and Linux systems, and is intended as the browser to provide the most up-to-date browser features. The version of Google Chrome shall be continuously maintained by Google's automatic update process.

7 ICAM Device Integration Configuration Requirements

The Identity, Credential and Access Management (ICAM) infrastructure services provide security controls for a significant portion of the core NASA operating environment. The following requirements have been identified for proper interoperability with ICAM services.

7.1 Authentication Configuration Requirements

The ICAM Device Integration (IDI) team develops software and configuration requirements for authentication with NASA standard operating systems. These configurations support such functions as:

- Smartcard-based authentication with the NASA PIV badge and other Federally compliant smartcards, including non-NASA PIV, CAC, and PIV-I credentials.
- NASA Launchpad Simplified Logon.
- Single-Sign-On with other Active Directory integrated applications such as:
    - Exchange
    - SharePoint
    - Project Server

All NASA personal computing devices running a full Windows, Mac or Linux operating system shall have a built-in PIV smartcard reader or the ability to integrate a smartcard reader. ICAM Device Integration configuration requirements, which include settings for operating system, browser, and middleware, can be found at:

http://etads.nasa.gov/idi/

ETADS has engineered a solution using Apple's Enterprise Connect software that will authenticate users on their Macs without the need for third-party software. This solution is being engineered and validated through NPR 7120.7 review within the OCIO PIV-M program, and it has implementation dependencies on the Mac Operating System Management (MOSM) 7120.7 project, which is scheduled for delivery in spring 2018.

Centrify was assessed and identified as an optional smartcard authentication solution for macOS 10.12, and it remains listed as Optional Supported Software within the Client Reference Configurations in Section 3.1.2. More information on the ACES Centrify service is available at:

https://aces.ndc.nasa.gov/subnav/os-mac.html

Future Expected Update: NASA is exploring user authentication with PIV-derived X.509 soft-certificate credentials for use on managed mobile devices.

Future Expected Update: The Agency will continue to issue a new solution, called the NASA Smartcard, for long-term guests and employees who are ineligible for PIV.

Smartcard authentication assessment updates and findings will be found at:

https://etads.nasa.gov/technology-assessments

7.2 NASA Client Trust Reference

The NASA Client Trust Reference (NCTR) repository for Trusted Sites can be found on the ETADS web site at:

https://etads.nasa.gov/idi/nctr/

Trusted Sites are listed and or referenced in the NCTR when they are approved for deployment on NASA end user systems as required to enable Agency level business functions for groups of personnel appreciably larger than those at any single NASA Center.

7.3 NASA Trust Anchor Management

Operating systems, as well as some third party applications — such as Mozilla Firefox, Mozilla Thunderbird, Adobe products, and Java — contain trusted certificate stores. The certificate stores are already preloaded and updated periodically by the product vendors with trusted certificates that are required for standard business functionality.

In addition to these vendor-supplied certificates, some of these certificate stores require additional certificates for interoperability with Agency and Agency affiliate services. This collection of additional certificates is managed through the enterprise NASA Trust Anchor Management (NTAM) effort. Reference National Institute of Standards and Technology (NIST) SP 800-52 Revision 1 for client configuration requirements for management of trust anchors. More information on NTAM can be found on the ETADS website at:

https://etads.nasa.gov/idi/trust-anchor-management/

7.4 Content Encryption and Secure Email

Content encryption and secure email is delivered for most NASA users via 4-cert smartcards. For users who need additional encryption, NASA ICAM PKI maintains secure desktop solutions for macOS and Windows based on Entrust. The Client Reference Configurations include the appropriate Entrust client version for use in encrypting desktop files and folders and an Outlook plug-in for sending signed, encrypted messages. NASA ICAM issues FIPS 201-2 PIV smartcards for use with S/MIME on Windows, macOS, and Linux. For the latest required Entrust build, email client S/MIME configuration, and other transitional FIPS 201-2 information, please refer to the NASA ICAM PKI site at:

https://icam.nasa.gov/pki/

For situations in which a standard Entrust solution cannot be used to exchange sensitive information, you may contact the NASA ICAM PKI Team for alternatives.

Future Expected Update: Smartcards issued since August 2017 have additional storage for a longer encryption key history. Systems using these smartcards will require the latest middleware and post-issuance update software for proper functionality. This pending software can be found via the smartcard middleware link referenced in section 7.6.

7.5 Additional Relying Party Requirements

All client applications that perform PKI operations shall support the SHA-2 family of algorithms. Information on SHA-2, RSA, and encryption algorithm lifetimes can be found in NIST Special Publications 800-78 Revision 4.

7.6 Additional Smartcard Middleware Requirements

The DSI (Desktop Smartcard Integration) Smartcard Middleware package for Windows systems provides full functionality for smartcard use in the NASA environment. This includes the ability to update smartcard certificates without having to go to a centers' badging facility, integration for smartcard use with the Firefox browser, and support for FIPS 201-2 compliant smartcards. The most current version of DSI shall be installed by service providers via client reference configuration guidance in Section 3.

For additional deployment requirements for service providers, including the appropriate NASA Consolidated Active Directory (NCAD) Security Groups required to apply the correct configuration policies, see:

https://etads.nasa.gov/idi/smartcard-middleware/

7.7 Password Management

Among other strong authentication tools, like the NCAD environment and NASA Access Launchpad for web application authentication, and deprecating the use of single-factor authentication credentials, like username and password, the Agency adheres to specific password complexity requirements:

ITS-HBK 2810.17-01, Section 9, Control IA-05.

NIST SP 800-63 does not permit Agency system storage of password credentials. Under no circumstances shall a smartcard holder's PIV smartcard PIN, or other Federal IT system credentials (including NASA issued RSA token PINs, NCAD account password, Access Launchpad password, and DAR passcode), be managed within a consumer retail or other password management tool.

8 SECURITY REQUIREMENTS FOR NASA SYSTEMS

The ongoing utility and security of the NASA IT environment is directly dependent on a continuous stream of software and hardware updates. All NASA IT service providers shall enforce processes and solutions that minimize the time required to install updates and new versions of software. NASA-STD-2804 lists specific minimum versions of software required for compliance. Unless specifically indicated, NASA IT service providers and system administrators shall install minor updates throughout systems' lifecycles and prepare major, tested new versions of software (including operating systems and browsers) in the shortest time possible.

The CRCs specify software required to participate in the continuous stream of automatic software vendor updates in real time. NASA IT service providers should take note of this intent, and implement their system support and application update processes (or alternative environments) to support an appropriately secure and modernized NASA IT environment.

8.1 Agency Security Configuration Standards

The NASA OCIO establishes Agency Federal Information Security Modernization Act (FISMA) compliance goals and reporting requirements for NASA systems, through the use of NASA security configuration specifications, managed by the Agency Security Configuration Standards (ASCS) service. OCIO policy requires deployment of the NASA ASCS system configurations to all systems:

https://etads.nasa.gov/ascs-memo

The NASA ASCS security configuration specifications are developed from various sources, including the National Institute of Standards and Technology (NIST) Security Content Automation Program (SCAP) checklists, Center for Internet Security (CIS) Benchmarks, Department of Defense (DoD) Security Technical Implementation Guides (STIGs), vendor and third-party sources; and are also internally developed by NASA. NASA's security configuration specifications, and their associated compliance monitoring measurement content, are managed by ASCS.

NASA security configuration specifications for each operating system and applicable software listed in this Standard can be obtained at:

http://etads.nasa.gov/ascs/

Centers wishing informed local consultation should contact their ASCS point of contact:

https://etads.nasa.gov/ascs/contacts/

Future Expected Update: ETADS is assessing Symantec Endpoint Protection 14 as a broader security toolset that may have value for the Agency beyond anti-virus capabilities.

8.2 Continuous Diagnostics and Mitigation

The Continuous Diagnostics and Mitigation (CDM) program is a dynamic approach to fortifying the cybersecurity of government networks and systems. CDM provides capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

For more information on the CDM program schedule, please visit:

http://cdm.nasa.gov

8.2.1 Configuration Settings Management and Software Asset Management

As a component of the Federal Government's CDM Program, NASA has transitioned from Dell KACE to IBM BigFixto meet configuration and asset management reporting requirements.

8.2.2 Whitelisting

As a component of the Federal Government's CDM Program, NASA is installing the RES agent on all workstations. This agent provides the ability to block any executable from running that is not on the Agency's pending whitelist of approved software.

8.3 Data Encryption

All Agency systems shall implement a data at rest (DAR) encryption solution. Please refer to the CRCs in Section 3 for specific operating system solutions.

DAR encryption solutions shall meet the following criteria:

- Cryptographic modules and other solution components must be FIPS 140-2 validated.
- Encryption keys must be managed and secured pursuant to NIST SP 800-57 Part 1 Rev 4 and NIST SP 800-53 Rev 4.
- Encryption keys must be centrally managed and escrowed to provide the ability for the Security Operations Center, law enforcement, the NASA Inspector General, and incident responders to access and recover data when necessary.

8.4 FIPS 140-2 Compliance Requirements

NASA shall adhere to the guidelines and recommendations of the National Institute of Standards and Technology (NIST) as required by FISMA, particularly as they apply to computer security and encryption technology for hardware and software. More specifically, NASA shall comply with Federal Information Processing Standards (FIPS) 140-1 and 140-2 as validated encryption modules become available.

NASA application developers and service providers are reminded that cryptographic-based security systems being used to protect sensitive information in computer systems must be FIPS 140-2 validated. A current list of validated products can be found at:

https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules

RHEL systems should be installed with FIPS mode enabled.

9 NETWORK

9.1 Internet Protocol version 6 Requirements

Internet Protocol version 6 (IPv6) is a newer version of the Internet Protocol, designed as the successor to Internet Protocol version 4 (IPv4).

All vendor laptops and desktops procured and distributed to NASA civil servants and contractors shall have IPv6 operating capabilities, confirmed by a Supplier's Declaration of Conformity. Vendor products should support Dynamic Host Configuration Protocol version 6 (DHCPv6). IPv6 configuration settings should remain in the operating system manufacturer default settings where IPv6 is enabled, unless systems are required to be transitioned to a modified Agency IPv6 enabled configuration. Detailed information on Federal requirements for IPv6 can be found at:

https://policy.cio.gov/web-policy/ipv6/

Interoperable Agency systems should continue to provide IPv4 in addition to IPv6 network capability until further notice.

9.2 Network Access Control

9.2.1 Enterprise External Border Protection

The Enterprise External Border Protection Project (EBPro) is responsible for deploying a set of solutions designed to improve the security posture of NASA's corporate networks and IT infrastructure. Cisco's Adaptive Security Appliance (ASA) is a component of that solution. The ASA supports the Agency VPN solution, and requires installation of the Cisco AnyConnect Secure Mobility Client for end-users to connect to the NASA network from remote locations.

9.2.2 Agency Virtual Private Network

As part of the EBPro Project, the Agency is providing the Cisco AnyConnect Secure Mobility Client as the standard Virtual Private Network (VPN) client. The timeframe for deployment is October 2017 through July 2018.

9.2.3 Network Access Control Client

The Enterprise Internal Border Network Access Control (EIB-NAC) project is developing a solution for network access control based on IEEE 801.1X and 802.3 network standards. The project has configured the network infrastructure for network access control and will require Windows, Mac and Linux devices to be configured for the network access solution for device access to the NASA internal network. The design requires that a Network Access Control (NAC) Client is installed on all NASA BigFix-enabled systems. The client manages certificate issuance for the device and configures the network interfaces to use device certificates for network authentication

Future Expected Update: Once the EIB-NAC project provides an ORR-approved NAC Client, the initial version for each platform will be required to be installed on all in-scope devices. The required settings will be provided with the NAC implementation handbook.

ETADS anticipates this application, once delivered, will include the following CRC specification information:

Function=Network Access Control (NAC)
Application= Network Access Control Client
Interface Standard=IEEE 802.1X, 802.3
Required Settings=NAC Handbook (TDB)
Version=TBD

10 COMPLIANCE REQUIREMENTS

10.1 Section 508 Compliance Requirements

Software products procured after June 21, 2001, must be in conformance with Section 508 of the Rehabilitation Act.

In January 2017, the United States Access Board published a final rule updating accessibility requirements for information and communication technology (ICT) covered by Section 508 of the Rehabilitation Act and Section 255 of the Communications Act.

Requirements apply to hardware that transmits information or has a user interface. Examples include computers, information kiosks, and multi-function copy machines. These provisions address closed functionality, biometrics, privacy, operable parts, data connections, display screens, status indicators, color coding, audible signals, two-way voice communication, closed captioning, and audio description.

Software requirements apply to computerized code that directs the use and operation of ICT and instructs ICT to perform a given task or function, including applications and mobile apps, operating systems, and processes that transform or operate on information and data. These provisions cover the interoperability with assistive technology, applications, and authoring tools.

Among other changes, the final rule emphasizes:

- restructuring provisions by functionality instead of product type due to the increasingly multi-functional capabilities of ICT
- requiring that operating systems provide certain accessibility features
- clarifying that software and operating systems must interoperate with assistive technology (such as screen magnification software and refreshable braille displays)

Existing ICT, including content, that meets the original 508 Standards does not have to be upgraded to meet the refreshed standards unless it is altered. This “safe harbor” clause (E202.2) applies to any component or portion of ICT that complies with the existing 508 Standards and is not altered. Any component or portion of existing, compliant ICT that is altered after the compliance date (January 18, 2018) must conform to the updated 508 Standards.

This content was adapted from the United States Access Board Web site. For more final rule details, please visit:

https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/overview-of-the-final-rule

Complete NASA information and guidance on addressing Section 508 requirements is available at:

http://www.nasa.gov/accessibility/section508/sec508_overview.html

When developing and testing software, users should consider the tools in section 10.1.1, or more recent versions of these tools, for evaluation. These tools have been suggested for use by Agency users.

10.1.1 Section 508 Tools

Section 508 Tools			
Function	**Windows**	**Mac**	**Red Hat Linux**
Screen Reading Software	• JAWS 18.x • NVDA 2017.1 (IE or Firefox) • ChromeVox (Chrome and Chrome OS)	• VoiceOver (Safari, Firefox, Chrome)	• ORCA (Gnome package)
Screen Magnification Software	• ZoomText Magnifier / Reader 11.2 • ZoomText Fusion 10.1	• ZoomText Mac 1.2	• Gnome shell magnifier • xzoom
Speech Recognition Software	• Dragon Naturally Speaking version 14	• Dragon Dictate for Mac v4 (Safari) or Dragon for Mac v5	
HTML Accessibility Validators	• SortSite 5.7 • WebAim's WAVE Toolbar (Chrome extension 1.0.0) • Total Validator Pro 11.4.x (IE, Chrome, Firefox) • Vision Australia's Web Accessibility Toolbar	• SortSite 5.26 • Total Validator Pro 11.4.x • WebAim's WAVE Toolbar (Chrome extension 1.0.0)	• Total Validator Pro 11.4.x • Mozilla SeaMonkey

Section 508 Tools			
Function	**Windows**	**Mac**	**Red Hat Linux**
	(WAT) add-on for IE: 2012		
PDF Documents	• Adobe Acrobat Reader DC or Adobe Acrobat Pro DC • CommonLook Plug-in for Acrobat • CommonLook PDF Validator	• Adobe Acrobat Reader DC or Adobe Acrobat Pro DC	
Text-to-Speech	• Natural Reader 14 (IE, Firefox) • Kurzweil 3000 14 (Firefox) • Read&Write Gold vs 11.5 (IE, Chrome, Firefox)	• Read&Write Gold for Mac 6 (Safari, Chrome, Firefox)	

10.2 Energy Management Requirements

In order to comply with Executive Order 13693, *Planning for Federal Sustainability in the Next Decade*, printers and end user computing systems must be configured to use energy-saving settings.

10.2.1 Computers

Requirements:

- Displays must be set to sleep after 15 minutes of idle time.
- Systems shall go to sleep or hibernate after 60 minutes of idle time.
- Wake-on-LAN functionality must be enabled on all NASA interoperable end user computer systems whose hardware and software support this functionality.
- Generally, the level of sleep should be as effective as possible at saving power, given the constraints of the environment. To reduce power consumption to a minimum, the S4 power savings mode (suspend to disk) should be used.

10.2.2 Printers

All clients must be configured for duplex printing by default.

11 Basic Interoperability Standards Maintenance

This Standard will be reviewed and updated on an as-required basis, not to exceed 12-month intervals. Participation in the revision process is open to all NASA employees. Users who would like to be alerted of changes to this Standard and opportunities to review future standards in development may be added to the regular communications list at standards-comments@lists.nasa.gov.

12 Duration

This Standard will remain in effect until canceled or modified by the NASA CIO.

13 Supporting Documents

Supporting documents and additional information related to this standard may be found at:

https://etads.nasa.gov/standards/

14 Comments

NASA-STD-2804 includes information from teams and projects across the Agency. If outdated information from your team or project is referenced in the Standard, please review and provide updated information to your Center's Chief Information Officer.

15 Acronyms And Definitions

15.1 Acronyms and Abbreviations

ASA	Adaptive Security Appliance
ASCS	Agency Security Configuration Standards
ASUS	Agency Security Update Service
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CIS	Center for Internet Security
CRC	Client Reference Configuration
CSO	Communications Service Office
DAR	Data at Rest (encryption)
DHS	Department of Homeland Security
DCHPv	Dynamic Host Configuration Protocol version

DoD	Department of Defense
DSI	Desktop Smartcard Integration
EBPro	External Border Protection Project
EMET	Enhanced Experience Mitigation Toolkit
ESR	Extended Support Release
ETADS	Enterprise Technology Assessments and Digital Standards
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
GFE	Government Furnished Equipment
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICAM	Identity Credential and Access Management
IDI	ICAM Device Integration
IE	Internet Explorer
IPv	Internet Protocol version
IPv6	Internet Protocol version 6
ISO	International Standards Organization
ITAR	International Traffic in Arms Regulations
IMAP	Internet Message Access Protocol
LTS	Long-term Support
LUKS	Linux Unified Key Setup
MAPI	Messaging Application Programming Interface
MIME	Multipurpose Internet Mail Extension

NCTR	NASA Client Trust Reference
NEFS	NASA Electronic Forms System
NFCE	NASA Firefox Configuration Extension
NIST	National Institute of Standards and Technology
NOMAD	NASA Operational Messaging and Directory Service
NSc	NASA Smartcard
NTAM	NASA Trust Anchor Management
OASIS	Organization for the Advancement of Structured Information Standards
OCIO	Office of the Chief Information Officer
OCS	Microsoft Office Communications Server
ODV	Organizationally Defined Value
PDF	Portable Document Format
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RFC	Request for Comments
SCAP	Security Content Automation Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SMTP	Simple Mail Transport Protocol
STIG	Security Technical Implementation Guide
S/MIME	Secure/Multipurpose Internet Mail Extensions
TLS	Transport Layer Security
VPN	Virtual Private Network
W3C	World Wide Web Consortium

XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

15.2 Definitions

Term	**Definition**
Basic Interoperability	Interoperability is the ability to obtain consistent and deterministic results within a specific platform (operating system software, minimum hardware, required and optional software) as well as between platforms (Microsoft, macOS, Linux) based on the established standards. Basic interoperability is also required with the Agency continuous monitoring/reporting tools in order to comply with Federal requirements.
End User Computing System	The term “End User Computing System” is used generically to refer to traditional desktop systems, as well as laptop computers, mobile devices, engineering workstations, and similar platforms that are utilized to provide basic interoperability.
Support for Basic Interoperability	Systems supporting basic interoperability are defined as Agency systems used to exchange information electronically by end users that require any of the functionality listed in Section 3, Client Reference Configurations.