NASA-STD-2804 Spring 2015
MINIMUM INTEROPERABILITY SOFTWARE SUITE

May 6, 2015

NASA TECHNICAL STANDARD

Document History Log

Status	Document Revision	Approval Date	Description
Informal Draft	0.1		Draft Release
Formal Draft	0.2		Draft Release
Final Draft	0.3		Final Draft Release
Baseline		May 6, 2015	Approved Version

Table of Contents

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 Information Technology Management Board. Its purpose is to define the baseline software suite necessary to support interoperability both between NASA end user computers and within the NASA operating environment. The Standard establishes Client Reference Configurations, Operating System Standards, and Compliance Dates for computers running Microsoft Windows, Apple OS X, and various Linux and UNIX 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), Emerging Technology and Desktop Standards Group (ETADS), MS 142-4, Cleveland, OH, 44135 or to desktop-standards@lists.nasa.gov.

/signature on file/

Larry N. Sweet
Chief Information Officer

1 SCOPE

1.1 Purpose

This Standard defines the baseline software suite necessary to support interoperability both between NASA end user computers and within the NASA operating environment. The Standard establishes Client Reference Configurations, Operating System Standards, and Compliance Dates for Agency interoperability systems, including computers running Microsoft Windows, Apple OS X, and various Linux and UNIX operating systems. Adherence to this Standard ensures compliance with Federal requirements for desktop computers, laptops, and other end user devices.

1.2 Applicability

Center CIOs will 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 below.

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

1.3 Waivers

This technical Standard is governed by the Enterprise Architecture Function as defined in Section 1.2.1.3 of NPR 2800.1B Managing Information Technology. Adherence to this Standard ensures compliance with the future state architecture as described in NPR 2830.1 NASA Enterprise Architecture Procedures.

The Emerging Technology and Desktop Standards group, in cooperation with the End User Services Service Executive and the Chief Enterprise Architect, will evaluate and process waivers to this Standard as appropriate. Waiver requests will include:

1. the reason the waiver is required
2. justification for the waiver
3. a proposed date by which compliance with the standard will be met

Waivers will be granted by the NASA CIO or at his/her discretion, responsibility will be delegated to the Center or Mission Directorate CIO.

2 ACRONYMS AND DEFINITIONS

2.1 Acronyms

ACES	Agency Consolidated End-User Services
ASCS	Agency Security Configuration Standards
ASUS	Agency Security Update Service
CA	Certificate Authority

CIO	Chief Information Officer
CIS	Center for Internet Security
CRC	Client Reference Configuration
CSS	Cascading Style Sheets
CUI	Controlled Unclassified Information
DAR	Data at Rest (encryption)
ESR	Extended Support Release
ETADS	Emerging Technology and Desktop Standards
FDCC	Federal Desktop Core Configurations
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FPKI	Federal Public Key Infrastructure
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICA	Independent Computing Architecture
ICAM	Identity Credential and Access Management
IDI	ICAM Device Integration
IE	Internet Explorer
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Standards Organization
ITAR	International Traffic in Arms Regulations
IMAP	Internet Message Access Protocol
LTS	Long-term Support
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
NOCA	NASA Operational Certificate Authority
NOMAD	NASA Operational Messaging and Directory Service
NSS	Network Security Services
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
PDF	Portable Document Format
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RFC	Request for Comments
RPC	Remote Procedure Call
SCAP	Security Content Automation Protocol
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SMTP	Simple Mail Transport Protocol
SSH	Secure Shell Protocol
SSL	Secure Sockets Layer
S/MIME	Secure/Multipurpose Internet Mail Extensions
TLS	Transport Layer Security
USGCB	United States Government Configuration Baseline
VPAT	Voluntary Product Accessibility Templates
W3C	World Wide Web Consortium
XHTML	eXtensible HyperText Markup Language
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

2.2 Definitions

2.2.1 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, OS X, Linux, UNIX) based on the established standards. Basic interoperability is also required with the Agency continuous monitoring/reporting tools in order to comply with Federal requirements.

2.2.2 End User Computing System

The term *End User Computing System* is used generically to refer to traditional desktop systems, as well as laptop computers, notebooks, slates, tablets, engineering workstations, and similar platforms that are utilized to provide basic interoperability.

2.2.3 Mobile Engineering Workstation

Mobile Engineering Workstation is used to describe high performance systems targeting the scientific, engineering and CAD community in a mobile form factor. Mobile Engineering Workstations are configured with high performance components and a wider array of ports than typical mainstream offerings. The resulting systems are portable yet typically heavier than their non-engineering peers. Mobile Engineering workstations align with the Mission category of systems and NASA-STD-2805 specifies three such configurations: The Apple Mobile Engineering Workstation, 15” Mobile Engineering Workstation and the 17” Mobile Engineering workstation.

2.2.4 Slate Computer

A slate is a touch oriented computing device whose design omits a permanently attached physical keyboard, to achieve a much lighter weight than other form factors. NASA-STD-2805 includes two slate HRCs: the Apple iPad Air 2, the Apple iPad Mini 3, and the Detachable 2-In-1 systems.

2.2.5 Tablet Computer

A tablet computer is defined as a computing device with a physically attached keyboard and a touch screen. Tablets are noteworthy for their light weight and generally smaller display sizes. Hardware innovations such as slates and ultra lightweight laptops with touch screens have encroached on, and minimized the prominence of, the PC Tablet within the market. These marketing pressures are relegating PC Tablets to the category of sunsetting technology.

2.2.5 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 3.4, Client Reference Configurations.

3 DETAILED REQUIREMENTS

3.1 Architectural Compliance Requirements

NASA has base-lined and approved the NASA Integrated Information Technology Architecture. The architecture is predicated on:

- 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 external to NASA
- Flexibility for future growth – Consistency with generally accepted consensus standards as much as feasible
- Security for NASA systems and data

Among these objectives, ensuring interoperability is one of NASA’s most critical issues related to information technology. In many cases, it is in NASA’s best interest to specify commercial products as standards for an interoperable 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 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 standard functionality.

3.2 Security 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 must therefore develop processes and solutions that minimize the time required to install updates and new versions of software. This NASA-STD-2804 document will list specific minimum versions of software required for compliance. Except as specifically indicated, all NASA IT service providers will install minor updates throughout the life-cycle maintenance for the systems, and prepare major new versions of software (including operating systems and browsers) in the shortest time possible, cognizant of required testing.

The Client Reference Configurations will specify software that will be 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.

3.3 Agency Security Configuration Standards

The NASA Office of the Chief Information Officer (OCIO) establishes Agency Federal Information Security Management Act (FISMA) compliance goals and reporting requirements for NASA systems, through the use of NASA System Configuration Baselines, managed by the Agency Security Configuration Standards (ASCS) Service. OCIO policy requires deployment of the NASA ASCS system configurations to all system (https://etads.nasa.gov/downloads/12-12-17-Configuration-Guidance-Memo.pdf).

The NASA ASCS system configuration baselines 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, vendor and third-party sources, and are also internally developed by NASA. These system configuration baselines, and their associated compliance monitoring measurement content, are managed by ASCS.

NASA system configuration baselines 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, listed here:

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

or consult the ASCS web site for additional information.

3.4 Client Reference Configurations

To address application, data, and infrastructure interoperability, and 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 definitive.

Client Reference Configurations (CRC) are included for each operating system, with the version numbers that were current at the time of this writing, and required configurations listed as appropriate. Current versions of applications must be used as made available by the application vendor unless specifically stated otherwise. Interface standards are included to guide service providers and system integrators.

The Client Reference Configurations define the operational configuration upon which service providers can define common enterprise images for all interoperable end user computing systems. All IT initiatives

funded or endorsed by the NASA OCIO presume systems that conform to the Client Reference Configurations. Application service providers and software developers should use the reference configurations to assist with integration and acceptance testing.

The NASA Emerging Technology and Desktop Standards group is working to ensure interoperability at the highest possible revision of products included in the Client Reference Configurations. Applications that meet these interface standards while providing improved end user experience, mitigating security risks, reducing support costs, or offering other tangible improvements may be submitted to standards-comments@lists.nasa.gov for consideration in future revisions to these Standards.

3.4.1 Client Reference Configuration for Windows 7

The software versions stated are the versions available at the time of this writing. Software can be installed at the time it is approved for use on NASA interoperable systems. Software must be available on NASA interoperable systems within three months of the approval date. The software must be maintained, and upgraded throughout the system lifecycle, unless specifically stated otherwise.

Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Dates**	**Approved on NASA Interoperable systems**
Operating System	Windows 7 Enterprise or Ultimate		NASA Baseline Security settings	SP1		8/9/2011
Operating System	Windows 7 Enterprise or Ultimate X64 Edition		NASA Baseline Security settings	SP1	Default install	8/9/2011
Firewall	Windows Firewall		NASA Baseline Security settings			9/10/2010
Smartcard Middleware	ActivClient	NIST SP 800-73 Part 3	See sections 3.7.1 and 3.7.5	7.x	DSI version 3.x	9/22/2014
Data at Rest Full Disk Encryption	Symantec PGP Whole Disk Encryption, or any FIPS 140-2 validated solution			10.2.x		8/1/2012
Content Encryption	Entrust	S/MIME	See section 3.6.5.3	9.x		9/7/2010
Trust Anchor Management	See Section 3.7	X.509	See Section 3.7	1.4.x		10/1/2013
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)			2015.x		3/31/2015
Anti-Virus	Symantec Endpoint Protection		Enterprise update server	12.1.x		8/1/2012

Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable systems
Anti-Malware	Symantec Endpoint Protection		Enterprise update server	12.1.x		8/1/2012
Patch Reporting	KBOX	KACE Proprietary	See section 3.6.4 Auto-updates enabled	6.x		9/22/2014
Web Browser	Mozilla Firefox Extended Support Release	W3C and industry standards	NFCE v2014.x or higher, see section 3.7 Auto-updates enabled	31.x		9/22/2014
Web Browser	Microsoft Internet Explorer	W3C and industry standards	NASA System Baseline Configuration settings. Also see section 3.7	11.0.x		9/22/2014
Web Browser	Google Chrome	W3C and industry standards	See section 3.7 Auto-updates enabled			10/1/2013
Office Automation	Microsoft Office (Professional Edition with Outlook)	Office Open XML document format		2013		1/29/2014
Word Processing	Microsoft Word	Office Open XML document format	Configure to use Office Open XML file format by default	2013		1/29/2014
Spreadsheet	Microsoft Excel	Office Open XML document format	Configure to use Office Open XML file format by default	2013		1/29/2014
Presentation	Microsoft PowerPoint	Office Open XML document format	Configure to use Office Open XML file format by default	2013		1/29/2014
Electronic Mail	Microsoft Outlook	IMAP4, SMTP, IMAP over SSL/TLS, MAPI over HTTPS	Configured for access to NOMAD	2013		1/29/2014
Secure Electronic Mail	Entrust Desktop Solution (ESP) Entrust ESP Outlook Plug-In	S/MIME	See section 3.6.5.3	9.x		9/7/2010
Calendaring	Microsoft Outlook as	iCalendar (RFC 5545)		2013		1/29/2014

Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable systems
	implemented by NOMAD					
Instant Messaging	Lync	SIP	Enterprise OCS Settings as implemented by NOMAD Pidgin-sipe OCS plugin	2013		10/1/2013
Instant Messaging	Pidgin	XMPP	NASA Jabber Service Pidgin-sipe OCS plugin	2.10.x		8/1/2012
PDF Viewer	Adobe Reader X	PDF		11.0.x		10/1/2013
Java	Java run-time environment		See section 3.7.2.2	Java 8	32-bit only	3/31/2015
Photo Editing	Microsoft Photo Gallery			Windows Essentials 2012		3/31/2015
Audio/video players	Adobe Flash Player	Flash SWF	Auto-updates enabled	16.x		3/31/2015
Audio/video players	Microsoft Windows Media Player	Windows Media Files	Default for all supported formats	12.x		8/1/2012
Audio/video players	Apple iTunes	Various Multimedia		12.x		9/22/2014
Electronic Forms	FileNet Desktop e-Forms	See Section 3.8	NASA Distribution Center	4.2		6/24/2008
Electronic Forms	Adobe Reader X	PDF	See section 3.7.2.2	11.0.x		10/1/2013
Video Conferencing	Lync			2013		10/1/2013
Voice over IP	Cisco Jabber	SIP/RTP	For softphone use only	10.x		3/31/2015

3.4.2 Client Reference Configuration for Windows 8.1

The software versions stated are the versions available at the time of this writing. Software can be installed at the time it is approved for use on NASA interoperable systems. Software must be available on NASA interoperable systems within three months of the approval date. The software must be maintained, and upgraded throughout the system lifecycle, unless specifically stated otherwise.

Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable systems
Operating System	Windows 8 Enterprise 64-bit		NASA Baseline Security settings	8.1		10/1/2013
Firewall	Windows Firewall		NASA Baseline Security settings			10/1/2013
Smartcard Middleware	ActivClient	NIST SP 800-73 Part 3	See sections 3.7.1 and 3.7.5	7.x	DSI version 3.x	4/1/2014
Data at Rest Full Disk Encryption	Symantec PGP Whole Disk Encryption, or any FIPS 140-2 validated solution			10.3.x		3/31/2015
Content Encryption	Entrust or any FIPS 140-2 validated solution	S/MIME	See section 3.6.5.3	9.x		2/1/2014
Trust Anchor Management	See Section 3.7	X.509	See Section 3.7	1.4.x		10/1/2013
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)			2015.x		3/31/2015
Anti-Virus	Symantec Endpoint Protection		Enterprise update server or unmanaged	12.1.x		10/1/2013
Anti-Malware	Symantec Endpoint Protection		Enterprise update server or unmanaged	12.1.x		10/1/2013
Patch Reporting	KBOX	KACE Proprietary	See section 3.6.4 Auto-updates enabled	6.x		9/22/2014
Web Browser	Mozilla Firefox Extended Support Release	W3C and industry standards	NFCE v2014.x or higher, see section 3.7 Recommend automatic updates enabled	31.x		9/22/2014
Web Browser	Microsoft Internet Explorer	W3C and industry standards	NASA System Baseline Configuration settings. Also see section 3.7	11.0.x		10/1/2013
Web Browser	Google Chrome	W3C and industry standards	See section 3.7 Autoupdate on			10/1/2013

Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable systems
Office Automation	Microsoft Office (Professional Edition with Outlook)	Office Open XML document format		2013		10/1/2013
Word Processing	Microsoft Word	Office Open XML document format	Configure to use Office Open XML file format by default	2013		10/1/2013
Spreadsheet	Microsoft Excel	Office Open XML document format	Configure to use Office Open XML file format by default	2013		10/1/2013
Presentation	Microsoft PowerPoint	Office Open XML document format	Configure to use Office Open XML file format by default	2013		10/1/2013
Electronic Mail	Microsoft Outlook	IMAP4, SMTP, IMAP over SSL/TLS, MAPI over HTTPS	Configured for access to NOMAD	2013		10/1/2013
Secure Email	Entrust Desktop Solution (ESP)Entrust ESP Outlook Plug-In	S/MIME	See section 3.6.5.3	9.x		2/1/2014
Calendaring	Microsoft Outlook as implemented by NOMAD	iCalendar (RFC 5545)		2013		10/1/2013
Instant Messaging	Lync	SIP	Enterprise OCS Settings as implemented by NOMAD Pidgin-sipe OCS plugin	2013		10/1/2013
PDF Viewer	Adobe Reader X	PDF		11.0.x		10/1/2013
Java	Java run-time environment		See section 3.7.2.2	Java 8	32-bit only	3/31/2015
Photo Editing	Microsoft Photo Gallery			Windows Essentials 2012		3/31/2015
Audio/video players	Adobe Flash Player	Flash SWF		16.x		3/31/2015

Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable systems
Audio/video players	Microsoft Windows Media Player	Windows Media Files	Default for all supported formats	12.x		10/1/2013
Audio/video players	Apple iTunes	Various Multimedia		12.x		9/22/2015
Electronic Forms	FileNet Desktop e-Forms	See Section 3.8	NASA Distribution Center	4.2		6/24/2008
Electronic Forms	Adobe Reader X	PDF	See section 3.7.2.2	11.0.x		10/1/2013
Video Conferencing	Lync			2013		10/1/2013
Voice over IP	Cisco Jabber	SIP/RTP	For softphone use only	10.x		3/31/2015

3.4.3 Client Reference Configuration for OS X 10.9

The software versions stated are the versions available at the time of this writing. Software can be installed at the time it is approved for use on NASA interoperable systems. Software must be available on NASA interoperable systems within three months of the approval date. The software must be maintained, and upgraded throughout the system lifecycle, unless specifically stated otherwise.

Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable systems
Operating System	OS X		NASA Guidance based on CIS benchmarks	10.9.x		3/142014
Firewall	Apple Firewall		Allow signed software Enable firewall logging			3/14/2014
Smartcard Middleware	ActivClient	NIST SP800-73 Part 3	See section 3.7.1	4.x		1/1/2014
Content Encryption	Entrust Secure Desktop for Mac (SDM)	S/MIME	See section 3.6.5.3	8.x		8/1/2012
Trust Anchor Management	See Section 3.7	X.509	See Section 3.7	1.4.x		3/14/2014

Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable systems
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)			2015.x		3/31/2015
Anti-Virus	Symantec Endpoint Protection			12.1.x	RU 4 or newer	3/14/2014
Anti-Malware	Symantec Endpoint Protection			12.1.x	RU 4 or newer	3/14/2014
Data at Rest Full Disk Encryption	Symantec PGP Whole Disk Encryption, or any FIPS 140-2 validated solution			10.3.x		3/14/2014
Patch Reporting	KBOX	KACE Proprietary	See section 3.6.4 Auto-updates enabled	5.x or 6.x		5/1/2014
Web Browser	Mozilla Firefox Extended Support Release	W3C and industry standards	NFCE v2014.x or higher, see section 3.7 Recommend automatic updates enabled	31.x		9/22/2014
Web Browser	Apple Safari	W3C and industry standards	See section 3.7	7.x		3/14/2014
Web Browser	Google Chrome	W3C and industry standards	See section 3.7			3/14/2014
Office Automation	Microsoft Office 2011 for Mac	Office Open XML document format		2011		3/14/2014
Word Processing	Microsoft Word 2011 for Mac	Office Open XML document format	Configure to use Office Open XML file format by default	14.4.x		3/14/2014
Spreadsheet	Microsoft Excel 2011 for Mac	Office Open XML document format	Configure to use Office Open XML file format by default	14.4.x		3/14/2014
Presentation	Microsoft PowerPoint 2011 for Mac	Office Open XML document format	Configure to use Office Open XML file format by default	14.4.x		3/412014

Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable systems
Electronic Mail	Microsoft Outlook 2011 for Mac	IMAP4, SMTP, IMAP over SSL/TLS, MAPI over HTTPS	Configured for access to NOMAD	14.4.x		3/14/2014
Electronic Mail	Apple Mail	IMAP4, SMTP, IMAP over SSL/TLS, MAPI over HTTPS	Configured for access to NOMAD. Use Outlook for S/MIME	7.3.x		3/14/2014
Secure Electronic Mail	Microsoft Outlook 2011 for Mac with Entrust Secure Desktop for Mac (SDM)	IMAP4, SMTP, IMAP over SSL/TLS, MAPI over HTTPS	Configured for access to NOMAD	14.3 8.x (SDM)		3/14/2014
Calendaring	Microsoft Outlook 2011 for Mac as implemented by NOMAD	iCalendar (RFC 5545)		14.3.x		3/14/2014
Calendaring	Apple Calendar	iCalendar (RFC 5545)		7.0.x		3/14/2014
Instant Messaging	Lync	SIP	Enterprise OCS Settings as implemented by NOMAD	2011		3/14/2014
Instant Messaging	Apple Messages	XMPP		Bundled		3/14/2014
PDF Viewer	Apple Preview	PDF		7.0.x		3/14/2014
PDF Viewer	Adobe Reader X	PDF		11.0.x	Default	3/14/2014
Photo Editing	Apple iPhoto			9.6.x		3/31/2015
Oracle Java	Java run-time environment		See section 3.7.2.	Java 8		3/31/2015
Audio/video players	Apple QuickTime Player	Various Multimedia	Default for QuickTime formats	10.3.x		3/14/2014
Audio/video players	Adobe Flash Player	Flash SWF		16.x		3/31/2015
Audio/video players	Apple iTunes	Various Multimedia	Default for all supported formats	12.0.x		3/31/2015

Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable systems
Electronic Forms	Adobe Reader X	See Section 3.8	See section 3.7.2.	11.0.x		3/14/2014
Video Conferencing	Lync			2011		3/14/2014
Voice over IP	Cisco Jabber	SIP/RTP	For softphone use only	10.x		3/31/2015

3.4.4 Client Reference Configuration for OS X 10.10

The software versions stated are the versions available at the time of this writing. Software can be installed at the time it is approved for use on NASA interoperable systems. Software must be available on NASA interoperable systems within three months of the approval date. The software must be maintained, and upgraded throughout the system lifecycle, unless specifically stated otherwise.

Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable systems
Operating System	OS X		NASA Guidance based on CIS benchmarks	10.10.x		3/31/2015
Firewall	Apple Firewall		Allow signed software Enable firewall logging			3/31/2015
Smartcard Middleware	ActivClient	NIST SP800-73 Part 3	See section 3.7.1	4.x		3/31/2015
Content Encryption	Entrust Secure Desktop for Mac (SDM)	S/MIME	See section 3.6.5.3	8.x		3/31/2015
Trust Anchor Management	See Section 3.7	X.509	See Section 3.7	1.4.x		3/31/2015
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)			2015.x		3/31/2015
Anti-Virus	Symantec Endpoint Protection			12.1.x	RU 4 or newer	3/31/2015
Anti-Malware	Symantec Endpoint Protection			12.1.x	RU 4 or newer	3/31/2015

Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable systems
Data at Rest Full Disk Encryption	Symantec PGP Whole Disk Encryption, or any FIPS 140-2 validated solution			10.3.x		3/31/2015
Patch Reporting	KBOX	KACE Proprietary	See section 3.6.4 Auto-updates enabled	6.x		3/31/2015
Web Browser	Mozilla Firefox Extended Support Release	W3C and industry standards	NFCE v2014.x or higher, see section 3.7 Recommend automatic updates enabled	31.x		3/31/2015
Web Browser	Apple Safari	W3C and industry standards	See section 3.7	8.x		3/31/2015
Web Browser	Google Chrome	W3C and industry standards	See section 3.7			3/31/2015
Office Automation	Microsoft Office 2011 for Mac	Office Open XML document format		2011		3/31/2015
Word Processing	Microsoft Word 2011 for Mac	Office Open XML document format	Configure to use Office Open XML file format by default	14.4.x		3/31/2015
Spreadsheet	Microsoft Excel 2011 for Mac	Office Open XML document format	Configure to use Office Open XML file format by default	14.4.x		3/14/2014
Presentation	Microsoft PowerPoint 2011 for Mac	Office Open XML document format	Configure to use Office Open XML file format by default	14.4.x		3/31/2015
Electronic Mail	Microsoft Outlook 2011 for Mac	IMAP4, SMTP, IMAP over SSL/TLS, MAPI over HTTPS	Configured for access to NOMAD	14.4.x		3/31/2015

Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable systems
Electronic Mail	Apple Mail	IMAP4, SMTP, IMAP over SSL/TLS, MAPI over HTTPS	Configured for access to NOMAD. Use Outlook for S/MIME	7.3.x		3/31/2015
Secure Electronic Mail	Microsoft Outlook 2011 for Mac with Entrust Secure Desktop for Mac (SDM)	IMAP4, SMTP, IMAP over SSL/TLS, MAPI over HTTPS	Configured for access to NOMAD	14.3 8.x (SDM)		3/31/2015
Calendaring	Microsoft Outlook 2011 for Mac as implemented by NOMAD	iCalendar (RFC 5545)		14.3.x		3/14/2014
Calendaring	Apple Calendar	iCalendar (RFC 5545)		8.0.x		3/31/2015
Instant Messaging	Lync	SIP	Enterprise OCS Settings as implemented by NOMAD	2011		3/31/2015
Instant Messaging	Apple Messages	XMPP		Bundled		3/31/2015
PDF Viewer	Apple Preview	PDF		8.0.x		3/31/2015
PDF Viewer	Adobe Reader X	PDF		11.0.x	Default	3/31/2015
Oracle Java	Java run-time environment		See section 3.7.2.	Java 8		3/31/2015
Photo Editing	Apple iPhoto			9.6.x		3/31/2015
Audio/video players	Apple QuickTime Player	Various Multimedia	Default for QuickTime formats	10.4.x		3/31/2015
Audio/video players	Adobe Flash Player	Flash SWF		16.x		3/31/2015
Audio/video players	Apple iTunes	Various Multimedia	Default for all supported formats	12.0.x		3/31/2015
Electronic Forms	Adobe Reader X	See Section 3.8	See section 3.7.2.	11.0.x		3/31/2015
Video Conferencing	Lync			2011		3/31/2015

Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable systems
Voice over IP	Cisco Jabber	SIP/RTP	For softphone use only	10.x		3/31/2015

3.4.5 Client Reference Configuration for Linux

The software versions stated are the versions available at the time of this writing. Software can be installed at the time it is approved for use on NASA interoperable systems. Software must be available on NASA interoperable systems within three months of the approval date. The software must be maintained, and upgraded throughout the system lifecycle, unless specifically stated otherwise. When the Linux operating system vendor provides bundled support for applications included in the CRC, the vendor-provided and supported versions should supersede those of the CRC. Using the Linux vendor update stream is recommended by the operating system vendors and simplifies system maintenance.

Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable systems
Operating System	Red Hat Enterprise Linux Desktop with Workstation option		NASA baseline	6.x		6/24/2008
Operating System	Red Hat Enterprise Linux Desktop with Workstation option		NASA baseline	7.x		9/22/2014
Operating System	Ubuntu LTS		NASA baseline	14.04.x		9/22/2014
Firewall	Bundled		Control inbound and outbound connections enabled by default	Bundled		6/24/2008
Smartcard Middleware	OpenSC	NIST SP800-73 Part 3	See section 3.7.1			9/1/2013
Secure Email	Thunderbird	S/MIME	Use exported NOCA certificates	31.x		8/1/2012
Trust Anchor Management	See Section 3.7	X.509	See Section 3.7	1.4.x		10/1/2013

Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable systems
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)			2015.x		3/31/2015
Anti-Virus	Symantec Antivirus for Linux			1.0.x		8/1/2012
Data at Rest Encryption	Symantec PGP Whole Disk Encryption		Configured to use central policy and key escrow service			8/1/2012
Patch Reporting	KBOX	KACE Proprietary	See section 3.6.4 Auto-updates enabled	5.x or 6.x		9/22/2014
Web Browser	Mozilla Firefox Extended Support Release	W3C and industry standards	NFCE v2014.x or higher, see section 3.7 Recommend automatic updates enabled	31.x		9/22/2014
Web Browser	Google Chrome	W3C and industry standards			Not required for RHEL since Google dropped support for RHEL.	8/1/2012
Office Automation	LibreOffice	OASIS Open Document Format for		4.1.x		3/1/2014
Word Processing	LibreOffice Writer	OASIS Open Document Format for	Configure to use Office Open XML file format by default	4.1.x		3/1/2014
Spreadsheet	LibreOffice Calc	OASIS Open Document Format for	Configure to use Office Open XML file format by default	4.1.x		3/1/2014
Presentation	LibreOffice Impress	OASIS Open Document Format for	Configure to use Office Open XML file format by default	4.1.x		3/1/2014
Electronic Mail	Mozilla Thunderbird	IMAP4, SMTP, IMAP over SSL/TLS	Configured for access to NOMAD. Use Thunderbird for S/MIME	31.x		8/1/2012

Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable systems
Electronic Mail	Evolution (RHEL)	IMAP4, SMTP, IMAP over SSL/TLS	Configured for access to NOMAD	12.0.x		8/1/2012
Calendaring	NOMAD Outlook Web Access	iCalendar (RFC 5545)	Web Browser	2.x		6/24/2008
Instant Messaging	Pidgin	XMPP	NASA Jabber Service Pidgin-sipe OCS plugin	2.9.x		6/24/2008
PDF Viewer	Adobe Reader			9.4.x		8/1/2012
Java	Java run-time environment		See section 3.7.2.	Java 7		8/1/2012
Audio/video players	MPlayer	Multimedia	Default for supported formats	1.0.x		6/24/2008
Audio/video players	Adobe Flash Player	Flash SWF		14.0.x		8/1/2012
Electronic Forms	Adobe Reader X	PDF	See section 3.7.2.	9.4.x		8/1/2012

3.4.6 Client Reference Configuration for Mobile Computing Systems

The versions stated are the versions available at the time of this writing. The current version available from the vendor shall be used unless specifically stated otherwise.

Client Reference Configuration for Mobile Computing Systems				
Functionality	**Application**	**Required Settings**	**Version**	**Effective Date**
Operating System	iOS	CIS Benchmarks with NASA Guidance	8.1 or later	March 31, 2015
Operating System	Android	CIS Benchmarks with NASA Guidance	4.0 or later*	September 4, 2012
Operating System	Blackberry	Configured to use Agency Blackberry Enterprise Server	7.1 or later	September 4, 2012

*Note Android OS version 4.3 has some interoperability issues.

3.5 Operating System Standards, Timelines, and Compliance Dates

3.5.1 Microsoft Windows

For all versions of the Windows operating system the Windows firewall must be enabled. All Windows systems must meet the NASA Baseline Security Configurations, which ensure compliance with United States Government Configuration Baseline (USGCB) requirements.

Windows Version	Guidance
Windows XP	Removal was required by October 1, 2013
Windows XP Professional x 64 Edition	Removal was required by October 1, 2013
Windows Vista	Removal was required by October 1, 2013
Windows 7	Default for all Windows systems
Windows 8	Update to Windows 8.1 or greater was required by February 1, 2014
Windows 8.1	Approved for use

3.5.1.1 Microsoft Windows 7

The only 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 all new and refreshed (upgraded) systems. The 32-bit version of Microsoft Windows 7 may be installed if necessary to support non-64 bit capable applications.

3.5.1.2 Microsoft Windows 8

Windows 8 must be updated to Windows 8.1. Windows 8.1 or greater is approved for use. Users selecting hardware with touch capability shall be given the choice to select Windows 8 as their operating system. No general migration or retrofit will be required of NASA service provider systems to Windows 8.x.

3.5.2 Apple OS X

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

OS X Version	Guidance
10.8 Mountain Lion	Removal was required by September 22, 2014
10.9 Mavericks	Approved for use on interoperable NASA systems March 14, 2014
10.10 Yosemite	Approved for use on interoperable NASA systems March 31, 2015 Default for all OS X systems

3.5.3 Linux

Special purpose Linux computers may not need to comply with all requirements in the reference standard. Such systems would include special-purpose computers such as name servers, compute servers, data acquisition systems, special software development workstations, or other components of the overall computing infrastructure. Several product standards are not available for any Linux or UNIX system. In order to comply with this Standard, interoperable end user computing systems must have some way to access these products. The Citrix Receiver client is recommended to connect Linux or UNIX systems to a Microsoft Windows application server.

The Red Hat Linux distributions that are supported for use on interoperable systems are Red Hat Enterprise Linux Desktop 6 with Workstation option, or Red Hat Enterprise Linux Desktop 7 with Workstation option on all new and refreshed systems.

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

The Ubuntu distribution that is supported for use on interoperable systems is Ubuntu 14.04 LTS (Long-term support).

http://www.ubuntu.com/

All new and refreshed Linux systems must run one of the supported Linux distributions. For Linux operating systems, vendor-provided and supported versions of applications shall be used. The version of application the vendor provides in their update stream supersedes those of the Client Reference Configuration.

3.5.4 UNIX

The following UNIX systems are supported in the NASA interoperable computing environment. Generally, both the current version and prior version of the operating system are acceptable. However, the older version of the operating system must continue to be supported by the vendor, and like all systems, must be kept current with security patches.

3.5.4.1 Oracle Solaris

Oracle Solaris is at version 11. Information about supported Solaris releases may be found at:

http://www.oracle.com/us/products/servers-storage/solaris/index.html

3.5.4.2 IBM AIX/POWER

AIX 7.1 is current. AIX versions are described at:

http://www-03.ibm.com/systems/power/software/aix/v71/

3.5.4.3 HP HP-UX/PA-RISC

HP-UX 11i v3 is current. The HP-UX 11i web page is at:

http://h71028.www7.hp.com/enterprise/w1/en/os/hpux11i-overview.html

3.6 Additional Client Reference Configuration Guidance

3.6.1 Office Automation Applications

The default document format for Microsoft Office and LibreOffice is the ISO Standard Office Open XML format.

Microsoft Office 2013 is approved for use on all NASA interoperable systems as of January 29, 2014. Microsoft Windows systems are required to run the 32-bit version of Office 2013 Standard Edition (or better) regardless of processor architecture. The 64-bit version of Office 2013 may be deployed as a point solution, though interoperability problems will likely persist and be uncorrectable. The removal of Microsoft Office 2010 on interoperable Windows systems was required by June 29, 2014.

Microsoft Office 2011 for Mac (Standard Edition) was approved for use on all interoperable OS X systems as of December 1, 2010. A Mac version of Outlook replaces Entourage. Note: Office 2011 reinstates support for Visual Basic Applications.

LibreOffice 4 is approved for deployment on all interoperable Linux systems as of October 1, 2013. There continue to be data format interoperability and rendering issues between Microsoft Office and Libre Office.

3.6.2 Electronic Messaging

NASA has implemented an enterprise-wide electronic messaging service known as NOMAD. This 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.

Note that while NOMAD is based upon open standards and can support stand-alone email clients that adhere to the defined interface standards of the Client Reference Configurations, utilizing such clients limits end user interoperability, may not be supported by NOMAD, and may result in future inability to participate in the enterprise messaging environment.

Supported Messaging Clients

Windows	**Microsoft Outlook**
OS X	Microsoft Outlook and Apple Mail*
Linux	Mozilla Thunderbird (Ubuntu & RHEL), Evolution (RHEL)

Apple Mail supports the NOMAD calendar and scheduling environment but does have some integration issues. The choice of client on OS X depends upon the required functionality. In some cases, Microsoft Outlook is more appropriate (for instance, when delegation functionality is required). In other cases Apple Mail and iCal with Address Book are suitable.

*Issues exist with Apple Mail and S/MIME. At this time it is not recommended to send encrypted mail using Apple Mail.

Additional clients which conform to the interface standards may be used as point solutions where interoperability might otherwise not be available.

The selection of mail clients will continue to promote secure access to commercial and partner email services in support of extra-Agency (non-NOMAD) collaborative activities.

3.6.3 Web Browsers

Web browser vendors have changed the browser delivery model. The frequency new version release has changed from yearly or bi-annually to every 1-2 months. In some cases vendors are managing the release cycle by auto-updating their browser in the background without user intervention or knowledge.

To avoid inefficiencies and interoperability issues, NASA must adjust to the rapid pace of browser enhancements resulting in new versions from the browser vendors. It is recommended for browsers with a rapid release cycle that auto-updating be used.

Web authors, application providers, system integrators, etc., 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.

Since no single browser meets the needs of the Agency, multiple browsers are approved for use. Internet Explorer, Firefox ESR, and Chrome must be available on Agency interoperable Windows systems; Safari,

Firefox ESR, and Chrome must be available on Agency interoperable Macs, and Firefox ESR and Chrome on Linux systems.

For Internet Explorer, NASA will maintain support for the most recent production version and the version immediately preceding it. Firefox ESR will be configured to automatically update with point releases for security updates only. Chrome will 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. If the browser maintains its own trusted certificates store, independent of the operating system, the NASA Trust Anchor Management (NTAM) collection of trusted certificates should be applied. Additional ICAM Device Integration (IDI) configuration requirements for authentication may also be required. Please refer to the internal ETADS IDI pages for all related up-to-date browser configuration guidance:

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

For additional information see section 3.7 ICAM Device Integration.

3.6.3.1 Microsoft Internet Explorer

Internet Explorer is approved for use on interoperable Windows systems to align with the features and capabilities expected by the operating system vendor. The NASA System Configuration Baseline must be used for all versions of Microsoft Internet Explorer.

Timelines for Internet Explorer

Version	Guidance
Internet Explorer 7	Removal was required by October 1, 2013
Internet Explorer 8	Removal was required by October 1, 2013
Internet Explorer 9	Removal is required by March 31, 2015
Internet Explorer 10	Approved for use on May 15, 2014. No general deployment Removal is required by March 31, 2015
Internet Explorer 11	Approved for use.

3.6.3.2 Mozilla Firefox Extended Support Release (ESR)

Mozilla Firefox ESR is approved for use on all interoperable Windows and OS X systems for those applications that require a more stable browser environment. Mozilla Firefox (ESR) is offered by Mozilla to address the needs of large organizations that do not have the agility to remain current with the rapid release cycle of modern browsers. Mozilla maintains Firefox ESR for a one-year period, while providing point releases containing security updates. No new features are added to Firefox ESR within this time frame. The version of Mozilla Firefox ESR must be continuously maintained by Mozilla's automatic update process.

3.6.3.3 Apple Safari

OS X Version	Version of Safari Approved for Use

OS X 10.9 (Mavericks)	Safari 7.x
OS X 10.10 (Yosemite)	Safari 8.x

Safari is approved for use on all interoperable OS X to align with the features and capabilities expected by the operating system vendor.

3.6.3.4 Google Chrome

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

3.6.4 System Configuration Reporting and Patch Management

The Agency solution for patch management, compliance reporting and system configuration reporting is the Dell KACE product. For current information on the appropriate configuration and patch management client for your system(s), including specific version levels, please refer to the Agency Security Update Service (ASUS) web site at:

https://asus.nasa.gov/

Agency policy requires that a reporting client be installed on all systems for which clients are available.

3.6.5 Data Encryption

3.6.5.1 Data at Rest (DAR) Encryption

All Agency laptop systems, as well as desktop computers that store sensitive information, will implement a DAR encryption solution. Symantec PGP Desktop is the Agency solution for Data at Rest (DAR) encryption. Please contact your local DAR representative for center specific deployment details or visit https://aces.ndc.nasa.gov/subnav/dar.html for more information.

3.6.5.2 Alternative Data at Rest (DAR) Encryption Solutions

As discussed in the NASA I3P PROGRAM DECISION MEMORANDUM (PDM) the use of alternative DAR encryption solutions are acceptable if they meet the following criteria:

- The solution must be FIPS 140-2 validated
- Encryption Keys must be managed and secured pursuant to NIST SP 800-57 and NIST SP 800-53 Rev 3
- Encryption Keys must be centrally managed and escrowed to provide the ability for the Security Operations Center, law enforcement, the Inspector General, and incident responders to access and recover data when necessary.

The following alternative DAR encryption solutions currently meet the above criteria and are acceptable for use on Agency interoperable systems:

- FileVault 2 on OS X systems
- BitLocker on Windows systems

Other additional DAR solutions that meet the above criteria may be used.

3.6.5.3 Content Encryption and Secure Email

NASA ICAM PKI maintains a secure desktop solution for OS X 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 will be transitioning to FIPS 201-2 PIV Cards for use with S/MIME on Windows, OS X, 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 the standard Entrust solution cannot be used to exchange sensitive information, contact the NASA ICAM PKI Team for alternatives.

3.7 ICAM Device Integration (IDI) Configuration Requirements

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

3.7.1 Authentication Configuration Requirements

The ICAM Device Integration 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
- User authentication with PIV-derived x.509 soft-certificate credentials (in development)

ICAM Device Integration configuration requirements, which include settings for operating system, browser, and middleware can be found at:

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

3.7.2 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/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

3.7.3 NASA Trust Anchor Management (NTAM)
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 NASA Trust Anchor Management (NTAM) effort. More information on NTAM can be found on the ETADS website at

https://etads.nasa.gov/ntam

3.7.4 Additional Relying Party Requirements

All client applications that perform PKI operations have been required to support the SHA-2 family of algorithms since November 2010. Information on SHA-2, RSA, and encryption algorithm lifetimes can be found in NIST Special Publications 800-78-2 and 800-131.

3.7.5 Additional Smartcard Middleware Requirements

The DSI v3.x Smartcard Middleware package for Windows 7 and 8.1 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 DSI version 3.x of ActivClient 7.0.x is to be installed by service providers using client configuration settings now managed by domain policy. See https://etads.nasa.gov/idi/Windows for additional deployment requirements for service providers including the appropriate NCAD Security Groups required to apply the correct configuration policies.

For Windows 7 and 8.1 systems, the Smartcard Middleware package, DSI version 3.x is required to be on systems by July 2015. At that time, it is recommended that all previous versions of the DSI smartcard middleware client be removed from Windows 7. [Installing DSI 3.x will automatically remove previous DSI versions of ActivClient as part of the installation process.]

3.8 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, and available in NODIS. NASA has transitioned to an Agency-wide Adobe integrated solution that supports NASA business practices, embraces technology and innovation, and increases efficiency.

- The majority of NASA and Center forms that were previously designed in FileNet have been converted to the new Agency solution, Adobe LiveCycle, and this process is targeted to be complete by the end of FY15.
- The NASA Electronic Forms System (NEFS) portal 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 workstations require:
    - Adobe Reader
    - Standard NASA supported browser (configured to open PDF documents with Adobe Reader)

3.8.1 Changes

- Links from forms posted on the former ARC-hosted NEFS website and Center repositories have changed due to the form conversion process and NEFS portal transition to the NEACC. In most all cases, the form number and/or name has not changed. Users can quickly locate the new form using the NEFS portal's "Quick Search" feature.

- During the conversion/transition process and/or as a part of the FY14 Biennial Forms Review, many forms were assessed and may have been cancelled by the Form Owner. Users can use the NEF portal's "Advanced Search" capabilities to search for forms that have been "Cancelled".
- NASA no longer hosts forms for other agencies forms, such as OMB, GSA, OPM standard forms (SF), on the NEFS portal. Users can locate current versions of these forms on the appropriate Agency's forms repository.

3.8.2 Decommissioning of FileNet Forms Client Software

- FileNet forms software no longer runs on NASA's Mac workstations
- Although FileNet still currently runs on Windows workstations, interoperability issues may occur.
- End-users should be converting and/or saving their filled/completed FileNet (.ifm) forms to PDF
    - Instructions on doing so are available as ESD Knowledge Articles (KAs)
- When the FileNet software is decommissioned, end-users will not be able to open stored IFM forms. Priority should be given to program/project records that have longer records retention periods, per NPR 1441.1, NASA Records Retention Schedules. End users should contact their Center Records Managers and/or if applicable, designated Records Liaison Officers.

3.9 Section 508 Compliance Requirements

Software products procured after June 21, 2001 must be in conformance with Section 508 of the Rehabilitation Act. Complete 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 are reminded to use the recommended tools for evaluation.

3.9.1 Section 508 Tools Table

Section 508 Tools

Function	Windows	OS X	Linux
Screen Reading Software	JAWS 16.x or higher VoiceOverWindow Eyes 9.x or higher NVDA 2015.1 or higher (IE or Firefox) ChromeVox (Chrome)	VoiceOver (Safari, Firefox, Chrome)	ORCA (Gnoome package)
Screen Magnification Software	Zoom Text 10.1 or higher	Zoom Text Mac 1.1 or higher	Ubuntu magnifier Gnome shell magnifier xzoom
Speech Recognition Software	Dragon Naturally Speaking version 12	Dragon Dictate 3 or higher	Dragon Naturally Speaking version 12 (on Ubuntu 12.04 using PlayOnLinux) Google2Ubuntu
Desktop Web Browser Tool	SortSite 5.7 or higher WebAim's Wave Toolbar 1.1.8 or higher (Firefox, Chrome add-on) Vision Australia's Web Accessibility Toolbar for IE - 2011	sortSite 5.7 or higher WebAim's Wave Toolbar 1.1.8 or higher (Firefox)	Mozilla SeaMonkey
PDF Documents	Adobe Acrobat 8.x or higher Adobe Acrobat XI Pro NetCentric Technologies CommonLook Plug-in for Acrobat	Adobe Acrobat 8.x or higher	

Function	Windows	OS X	Linux
Text-to-Speech	Natural Reader 13 or higher (IE, Firefox) Kurzwell 3000 13 or higher (Firefox) Read&Write Gold 11.5 or higher (IE, Chrome, Firefox)	Read&Write Gold 6 or higher (Safari, Chrome, Firefox)	

3.10 FIPS 140-2 Compliance Requirements

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

NASA application developers and service providers are reminded that whenever cryptographic-based security systems are used to protect sensitive information in computer systems, the cryptographic modules utilized must be FIPS 140-2 compliant as validated by NIST. A current list of validated products can be found at:

http://csrc.nist.gov/cryptval/

3.11 Wireless Requirements

The current minimum wireless hardware and software configuration that will be used by NASA to support interoperability is defined in NASA-STD-2850.1. For information on the ongoing conditions that wireless infrastructure devices must satisfy to connect to the NASA network see NASA-STD-2850.1 which when posted will be available at:

http://standards.nasa.gov/

3.12 Internet Protocol version 6 (IPv6) Requirements

Internet Protocol version 6 (IPv6) is a new version of the Internet Protocol, designed as the successor to Internet Protocol version 4 (IPv4). IPv6 is described in Internet standard document RFC 2460 et al.

Most modern day operating systems are IPv6 capable. On Windows systems from Windows Vista onward Microsoft has enabled IPv6 by default. Apple has delivered IPv6 capable systems since OS X 10.2. Both Red Hat Enterprise Linux and Ubuntu Linux are IPv6 capable. Modern cellular LTE networks are natively IPv6.

IPv6 configuration settings should remain in the operating system manufacturer default settings where IPv6 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 the NIST USGv6 Profile and Testing Program at:

http://www.nist.gov/itl/antd/usgv6.cfm

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

3.13 Energy Management

In order to comply with Executive Order 13423, printers, and end user computing systems must be configured to use energy-saving settings.

3.13.1 Computers

Requirements:

- Displays must be set to sleep after 15 minutes of idle time
- Systems must go to sleep 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.

Servers and other special-purpose systems are exempted from this requirement.

3.13.2 Printers

All clients must be configured for duplex printing by default.

3.14 Virtualization

Virtualization technology allows multiple operating systems to be run on a single physical computer. If a virtualization product is required for interoperability the recommended solution (VMWare) must be used. See Table of Optional Software. The current version of VMWare must be installed for as required by the host operating system. The software listed in the Agency Required Software table in section 4.2 must be installed on the virtualized system, and configured as required by the system security plan.

3.15 Password Management

As part of the Federal and Agency Identity Credential and Access Management (ICAM) programs, NASA is implementing strong authentication for access to NASA IT systems and applications per the guidance of HSPD-12 and OMB M-11-11 using federally issued PIV smartcards, including PIV-I smartcards provided by authorized issuers. Part of the strategy includes requiring system and application authentication to utilize the central authentication sources, namely the NASA Consolidated Active Directory environment and the NASA Access Launchpad for web application authentication, and to deprecate the use of single factor authentication credentials, namely username and password. While significant progress has been made, smartcard enablement is still being developed in a number of cases. Further, it is recognized that users require access to a wide array of both Federal and non-Federal IT systems, most outside of NASA’s control, which employ password-based authentication mechanisms.

NIST SP 800-63 does not permit local storage of password credentials as such action would reveal the authentication secret to a party (application) other than the claimant (the user) or the verifier operated by the Credential Service Provider (the Federal IT system being accessed). 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. For access to non-Federally controlled IT systems, a password management tool is permissible if it has an implementation that is compliant with NPR 2810.1A requirements.

4 ADDITIONAL SOFTWARE TABLES

4.1 Optional Software

The following table contains optional useful functionality that is not required for interoperability. These software applications and utilities can be made available to end users upon request or distributed with standard enterprise images to support interoperability. Where practical, it is recommended that these tools be used rather than similar tools that address the same function. This table often identifies software that may be eventually be included in the Client Reference Configurations.

4.1.1 Table of Optional Software

The current version available from the vendor shall be used unless specifically stated otherwise.

Function	Windows	OS X	Linux
ssh client	XWin32 or PuTTY-CAC (for PIV)	bundled	bundled or OpenSSH (for PIV)
sftp client	FileZilla	Cyberduck	bundled or OpenSSH
Advance file archive extractor/creator	WinZip 12	bundled	bundled
Remote access to Windows systems	MS Remote Desktop Connection	MS Remote Desktop Connection / rdesktop (for PIV)	bundled
X window system server	XWin32	Apple X11	bundled
Postscript previewer	Win 7 Ghostscript, Win 8 bundled	bundled	bundled
PDF creator	Adobe Acrobat, Pro	Adobe Acrobat, Pro	Scribus
Project Management	MS Project	OpenProj	OpenProj
Virtualization	VMWare Workstation	VMWare Fusion	VMWare Workstation
Twitter	TweetDeck	bundled	Pidgin
Password Management	1Password	Password Manager Pro	Password Manager Pro
Voice-over-Internet Protocol	Skype	Skype	Skype
WebDAV	Firefox S3 Organizer	Firefox S3 Organizer	Firefox S3 Organizer
Active Directory Kerberos PKINIT Integration (PIV)	NA / Native Support Available	Centrify Suite or ADmit Mac PKI	Centrify Suite (RHEL Only)
Viewing of Visio drawings	Microsoft Visio 2013 Viewer	Free Visio View (Lucidchart) Add-on for Firefox	Free Visio View (Lucidchart) Add-on for Firefox
Access to centrally served Windows applications	Citrix Receiver 12.1.x	Citrix Receiver 12.1.x	Citrix Receiver 12.1.x
Audio/video players	Apple QuickTime Player for Windows	Flip4Mac WMV	
Audio/video players	Microsoft Silverlight 5.x	Microsoft Silverlight 5.x	

4.1.2 Optional Software for Mobile Computing Systems

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

https://apps.nasa.gov/applist

4.2 Agency Required Software

The following table summarizes software that must be installed on all Agency end user computing systems, regardless of their interoperability requirements. This software is included in the Client Reference Configuration.

Agency Required Software

Function	Windows	OS X	Linux	Unix
FISMA compliance	NASA System Configuration Baselines	NASA System Configuration Baselines	CIS Benchmarks	CIS Benchmarks
Patch reporting	KACE KBOX - See section 3.6.4 Auto-updates enabled	KACE KBOX- See section 3.6.4 Auto-updates enabled	KACE KBOX- See section 3.6.4 Auto-updates enabled	KACE KBOX- See section 3.6.4 Auto-updates enabled
Anti-Virus	Symantec Endpoint Protection	Symantec Endpoint Protection	Symantec	Symantec
PIV Middleware	ActivClient	PIV.tokend	RHEL: Coolkey Ubuntu: Open SC	OpenSC

5 REVIEW AND REPORTING REQUIREMENTS

5.1 Interoperability Maintenance Reporting

Upon request, Center CIOs will provide the NASA CIO with a summary report, outlining the status of minimum interoperability access for each NASA employee.

5.2 Interoperability Reporting

Each Center CIO will utilize the Agency selected processes and tools, both manual and automated, to report on an annual basis to the NASA CIO the hardware and software configuration of all systems at their respective Centers. The report will contain sufficient information to ascertain if each system supports NASA employees or is Government-furnished equipment to a contractor, whether the equipment is required to be interoperable, and a description of the hardware architecture/environment. The report will specify the number of NASA employees that do not have access to interoperable systems.

5.3 Basic Interoperability Standards Maintenance

This Standard, and its companion, NASA-STD-2805 Minimum Hardware Configurations, are maintained on behalf of the NASA CIO by the Emerging Technology and Desktop Standards group. Together, these Standards define the software, hardware, and configurations necessary to ensure basic interoperability within the NASA information technology computing infrastructure. 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. Details on how to be alerted of changes to the Standards and/or comment on proposed updates can be found at http://etads.nasa.gov/. This site also maintains interim guidance, position papers, software and hardware reviews, recommendations and other documentation intended to promote standardized basic interoperability.

6 DURATION

6.1 Duration

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

7 SUPPORTING DOCUMENTS

7.1 Supporting Documents

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

http://etads.nasa.gov/dcs