MEASUREMENT SYSTEM
IDENTIFICATION

NASA TECHNICAL STANDARD

National Aeronautics and Space Administration

NASA-STD-2804
Spring 2016

Approved: 2016-05-31

Superseding NASA-STD-2804 Fall 2015

NASA-STD-2804 Spring 2016
MINIMUM INTEROPERABILITY SOFTWARE SUITE

DOCUMENT HISTORY LOG

Status	Document Revision	Approval Date	Description
Informal Draft	0.1	2016-03-15	Draft Release
Formal Draft	0.2	2016-05-05	Draft Release
Baseline	1.0	2016-05-31	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, Apple OS X, mobile operating systems, and various Linux 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.

/signature on file/   May 31, 2106

Renee P. Wynn   Approval Date

Chief Information Officer

LIST OF TABLES

1 SCOPE

1.1 Purpose

This Standard defines the baseline software suite necessary to support interoperability, 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 Agency interoperability systems, including computers running Microsoft Windows, Apple OS X, Android, iOS, and various Linux 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 Authority

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.

2 ARCHITECTURAL COMPLIANCE REQUIREMENTS

NASA maintains a baselined and approved 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 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

Among these objectives, ensuring interoperability is one of NASA's most critical issues related to information technology. This Standard, along with NASA-STD-2805, *Minimum Hardware Configurations*, defines the interoperable NASA-end-user system. 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 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 represented as Client Reference Configurations (CRC).

The Client Reference Configurations define the operational configuration upon which service providers shall 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.

CRCs 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 NASA Enterprise Technology Assessments and Digital Standards (ETADS) Office 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.

3.1 Client Reference Configuration for Windows 7

Windows 7 NASA Core Build						
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Dates**	**Approved on NASA Interoperable Systems**
Operating System	Windows 7 Enterprise or Ultimate x64 Edition		NASA Security Configuration Settings (ASCS)	SP1	7/1/18	8/9/11

Windows 7 NASA Core Build						
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Dates**	**Approved on NASA Interoperable Systems**
Applications, Plugins, and Tools						
Word Processing	Microsoft Word Professional	Office Open XML document format	NASA Security Configuration Settings (ASCS)	2013	Permitted for use. No new installs	1/29/14
				2016	New installs	5/31/16
Spreadsheet	Microsoft Excel Professional	Office Open XML document format	NASA Security Configuration Settings (ASCS)	2013	Permitted for use. No new installs	1/29/14
				2016	New installs	5/31/16
Presentation	Microsoft PowerPoint Professional	Office Open XML document format	NASA Security Configuration Settings (ASCS)	2013	Permitted for use. No new installs	1/29/14
				2016	New installs	5/31/16
Electronic Mail and Calendaring	Microsoft Outlook Professional	IMAP4, SMTP, IMAP over TLS, MAPI over HTTP, iCalendar (RFC 5545)	Configured for access to NOMAD; NASA Security Configuration Settings (ASCS)	2013	Permitted for use. No new installs	1/29/14
				2016	New installs	5/31/16
Secure Electronic Mail	Entrust ESP Outlook Plug-In	S/MIME	See section 7.3; NASA Security Configuration Settings (ASCS)	9.3		11/1/15
Instant Messaging and Web Conferencing	Microsoft Skype for Business	SIP	Enterprise OCS Settings; Configured for access to NOMAD; Pidgin-sipe OCS plugin; NASA Security Configuration Settings (ASCS)	2015		8/18/15
PDF Viewer and Electronic Forms	Adobe Acrobat Reader DC	PDF	NASA Security Configuration Settings (ASCS)	2015		5/31/16
Java	Oracle Java Run-time Environment (JRE)		NASA Security Configuration Settings (ASCS); AES256 Strong Crypto	Java 8	9/1/2017	3/31/15

	Windows 7 NASA Core Build					
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Dates**	**Approved on NASA Interoperable Systems**
Audio/video players	Adobe Flash Player	Flash SWF		21.x		5/31/16
Browsers						
Web Browser	Microsoft Internet Explorer	W3C and industry standards	NASA Security Configuration Settings (ASCS); See section 7	11.0.x		9/22/14
Web Browser	Mozilla Firefox Extended Support Release	W3C and industry standards	NFCE v2016.x or higher; See section 7; NASA Security Configuration Settings (ASCS); Auto-updates enabled	45.x		5/31/16
ICAM						
Smartcard Middleware	ActivClient	NIST SP 800-73 Part 4	See sections 8.1 and 8.5	7.x	DSI version 3.x	9/22/14
Content Encryption	Entrust ESP for Windows	S/MIME	See section 7.3	9.x		9/7/10
Trust Anchor Management	NASA Trust Anchor Management	X.509	See Section 7.3	2016.x		5/31/16
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)			2016.x		5/31/16
Security						
Firewall	Windows Firewall		NASA Security Configuration Settings (ASCS)			9/10/10
Anti-Virus and Anti-Malware	Symantec Endpoint Protection		Enterprise update server	12.1.x		8/1/12
Data at Rest Full Disk Encryption	Symantec PGP Whole Disk Encryption, Microsoft BitLocker		Configured to use key escrow	10.3.x (PGP)		8/1/12 (PGP) 5/31/16 (BL)
Patch Reporting	Dell KACE	KACE Proprietary	See section 9.3.1; Auto-updates enabled	6.x		9/22/14

Windows 7 NASA Core Build						
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Dates**	**Approved on NASA Interoperable Systems**
Incident Response	Mandiant Intelligent Response (MIR)		NASA Security Configuration Settings (ASCS)	3.x		5/31/16
Vulnerability Protection	Enhanced Mitigation Experience Toolkit (EMET)			5.5		9/30/16

Windows 7 NASA Optional Supported Software						
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Date**	**Approved on NASA Interoperable systems**
Operating System	Windows 7 Enterprise or Ultimate		NASA Security Configuration Settings (ASCS)	SP1	7/1/18	8/9/11
Web Browser	Google Chrome	W3C and industry standards	See section 7; NASA Security Configuration Settings (ASCS); Auto update on			10/1/13
Softphone Client	Cisco Jabber	SIP/RTP	For softphone use only	11.5.x		5/31/16
Note Taking	Microsoft OneNote Professional	Office Open XML document format	NASA Security Configuration Settings (ASCS)	2013	Permitted for use. No new installs	1/29/14
				2016	New installs	5/31/16
Database	Microsoft Access			2013	Permitted for use. No new installs	1/29/14
				2016	New installs	5/31/16
Desktop Publishing	Microsoft Publisher			2013	Permitted for use. No new installs	1/29/14
				2016	New installs	5/31/16
Audio/video players	Microsoft Silverlight	Various Multimedia		5.1.x	10/12/21	8/1/12

Windows 7 NASA Optional Supported Software						
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Date**	**Approved on NASA Interoperable systems**
Audio/video players	Microsoft Windows Media Player	Windows Media Files	Default for all supported formats	12.x		8/1/12
Multimedia player	Apple iTunes	Various Multimedia		12.x		9/22/14
Instant Messaging	Pidgin	XMPP	NASA Jabber Service; Pidgin-sipe OCS plugin	2.10.x		8/1/12
Virtualization	VMware Workstation			12.x		5/31/16
Project Management	Microsoft Project			2013		5/31/16
				2016		5/31/16
PDF Creator	Adobe Acrobat Pro			XI		5/31/16
Access to Centrally Served Windows Applications	Citrix Receiver for Windows			4.4.x		5/31/16

3.2 Client Reference Configuration for Windows 8

Windows 8 NASA Core Build						
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Dates**	**Approved on NASA Interoperable Systems**
Operating System	Windows 8 Enterprise X64 Edition		NASA Security Configuration Settings (ASCS)	8.1	7/1/17	10/1/13

Windows 8 NASA Core Build						
Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable Systems
Applications, Plugins, and Tools						
Word Processing	Microsoft Word Professional	Office Open XML document format	NASA Security Configuration Settings (ASCS)	2013	Permitted for use. No new installs	1/29/14
				2016	New installs	5/31/16
Spreadsheet	Microsoft Excel Professional	Office Open XML document format	NASA Security Configuration Settings (ASCS)	2013	Permitted for use. No new installs	1/29/14
				2016	New installs	5/31/16
Presentation	Microsoft PowerPoint Professional	Office Open XML document format	NASA Security Configuration Settings (ASCS)	2013	Permitted for use. No new installs	1/29/14
				2016	New installs	5/31/16
Electronic Mail and Calendaring	Microsoft Outlook Professional	IMAP4, SMTP, IMAP over TLS, MAPI over HTTP, iCalendar (RFC 5545)	Configured for access to NOMAD; NASA Security Configuration Settings (ASCS)	2013	Permitted for use. No new installs	10/1/13
				2016	New installs	5/31/16
Secure Electronic Mail	Entrust ESP Outlook Plug-In	S/MIME	NASA Security Configuration Settings (ASCS), See section 7.3	9.3		11/1/15
Instant Messaging and Web Conferencing	Microsoft Skype for Business	SIP	Enterprise OCS Settings; Configured for access to NOMAD; Pidgin-sipe OCS plugin; NASA Security Configuration Settings (ASCS)	2015		8/18/15
PDF Viewer and Electronic Forms	Adobe Acrobat Reader DC	PDF	NASA Security Configuration Settings (ASCS)	2015		5/31/16

Windows 8 NASA Core Build						
Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable Systems
Java	Java run-time environment (JRE)		NASA Security Configuration Settings (ASCS); AES256 Strong Crypto	Java 8	9/1/17	10/1/15
Audio/video players	Adobe Flash Player	Flash SWF		21.x		5/31/16
Browsers						
Web Browser	Microsoft Internet Explorer	W3C and industry standards	NASA Security Configuration Settings (ASCS); See section 7	11.0.x		10/1/13
Web Browser	Mozilla Firefox Extended Support Release	W3C and industry standards	NASA Security Configuration Settings (ASCS); NFCE v2016.1 or higher; See section 7; Auto-updates enabled	45.x		5/31/16
ICAM						
Smartcard Middleware	ActivClient	NIST SP 800-73 Part 4	See sections 8.1 and 8.5	7.x	DSI version 3.x	4/1/14
Content Encryption	Entrust ESP for Windows	S/MIME	See section 7.3	9.x		2/1/14
Trust Anchor Management	NASA Trust Anchor Management	X.509	See section 7	2016.x		5/31/16
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)			2016.x		5/31/16
Security						
Firewall	Windows Firewall		NASA Security Configuration Settings (ASCS)			10/1/13

15 of 49

Windows 8 NASA Core Build						
Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable Systems
Anti-Virus and Anti-Malware	Symantec Endpoint Protection		Enterprise update server	12.1.x		10/1/13
Data at Rest Full Disk Encryption	Symantec PGP Whole Disk Encryption, Microsoft BitLocker		Configured to use key escrow	10.3.x (PGP)		10/1/13
Patch Reporting	Dell KACE	KACE Proprietary	See section 9.3.1; Auto-updates enabled	6.x		9/22/14
Incident Response	Mandiant Intelligent Response		NASA Security Configuration Settings (ASCS)	3.x		5/31/16
Vulnerability Protection	Enhanced Mitigation Experience Toolkit (EMET)			5.5	9/30/16	5/31/16

Windows 8 NASA Optional Supported Software						
Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Date	Approved on NASA Interoperable systems
Web Browser	Google Chrome	W3C and industry standards	NASA Security Configuration Settings (ASCS); See section 7; Auto-update on			10/1/13
Softphone Client	Cisco Jabber	SIP/RTP	For soft phone use only	11.5.x		3/31/15
Note Taking	Microsoft OneNote Professional	Office Open XML document format	NASA Security Configuration Settings (ASCS)	2013	Permitted for use. No new installs	1/29/14
				2016	New installs	5/31/16
Database	Microsoft Access			2013	Permitted for use. No new installs	10/1/13
				2016	New installs	5/31/16

Windows 8 NASA Optional Supported Software						
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Date**	**Approved on NASA Interoperable systems**
Desktop Publishing	Microsoft Publisher			2013	Permitted for use. No new installs	10/1/13
				2016	New installs	5/31/16
Audio/video players	Microsoft Silverlight	Various Multimedia		5.1.x	10/12/21	10/1/13
Audio/video players	Microsoft Windows Media Player	Windows Media Files	Default for all supported formats	12.x		10/1/13
Multimedia player	Apple iTunes	Various Multimedia		12.x		9/22/15
Instant Messaging	Pidgin	XMPP	NASA Jabber Service; Pidgin-sipe OCS plugin	2.10.x		10/1/13
Virtualization	VMware Workstation			12.x		5/31/16
Project Management	Microsoft Project			2013		5/31/16
				2016		5/31/16
PDF Creator	Adobe Acrobat Pro			XI		5/31/16
Access to Centrally Served Windows Applications	Citrix Receiver for Windows			4.4.x		5/31/16

3.3   Client Reference Configuration for Windows 10

Windows 10 NASA Core Build						
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Dates**	**Approved on NASA Interoperable Systems**
Operating System	Windows10 Enterprise		NASA Security Configuration Settings (ASCS)	10.x		5/31/16
Applications, Plugins, and Tools						
Word Processing	Microsoft Word Professional	Office Open XML document format	NASA Security Configuration Settings (ASCS)	2016		5/31/16

Windows 10 NASA Core Build						
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Dates**	**Approved on NASA Interoperable Systems**
Spreadsheet	Microsoft Excel Professional	Office Open XML document format	NASA Security Configuration Settings (ASCS)	2016		5/31/16
Presentation	Microsoft PowerPoint Professional	Office Open XML document format	NASA Security Configuration Settings (ASCS)	2016		5/31/16
Electronic Mail and Calendaring	Microsoft Outlook Professional	IMAP4, SMTP, IMAP over TLS, MAPI over HTTP, iCalendar (RFC 5545)	NASA Security Configuration Settings (ASCS); Configured for access to NOMAD	2016		5/31/16
Secure Electronic Mail	Entrust ESP Outlook Plug-In	S/MIME	NASA Security Configuration Settings (ASCS); See section 7.3	9.3		5/31/16
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		5/31/16
PDF Viewer and Electronic Forms	Adobe Acrobat Reader DC	PDF	NASA Security Configuration Settings (ASCS)	2015		5/31/16
Java	Java run-time environment (JRE)		NASA Security Configuration Settings (ASCS); AES256 Strong Crypto	Java 8	9/1/17	5/31/16
Audio/video players	Adobe Flash Player	Flash SWF		21.x		5/31/16
Browsers						
Web Browser	Microsoft Internet Explorer	W3C and industry standards	NASA Security Configuration Settings (ASCS); See section 7	11.0.x		5/31/16

Windows 10 NASA Core Build						
Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable Systems
Web Browser	Microsoft Edge		NASA Security Configuration Settings (ASCS)	14.x	Bundled with OS. Not interoperable. See section 6.1.2	5/31/16
Web Browser	Mozilla Firefox Extended Support Release	W3C and industry standards	NASA Security Configuration Settings (ASCS); NFCE v2016.1 or higher; See section 7; Auto-updates enabled	45.x		5/31/16
ICAM						
Smartcard Middleware	ActivClient	NIST SP 800-73 Part 4	See sections 8.1 and 8.5	7.x	DSI version 3.x	5/31/16
Content Encryption	Entrust ESP for Windows	S/MIME	See section 7.3	9.3		5/31/16
Trust Anchor Management	NASA Trust Anchor Management	X.509	See section 7	2016.x		5/31/16
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)			2016.x		5/31/16
Security						
Firewall	Windows Firewall		NASA Security Configuration Settings (ASCS)			5/31/16
Anti-Virus and Anti-Malware	Symantec Endpoint Protection		Enterprise update server	12.1.x		5/31/16
Data at Rest Full Disk Encryption	Microsoft BitLocker		Configured to use key escrow			5/31/16
Patch Reporting	Dell KACE	KACE Proprietary	See section 8.5; Auto-updates enabled	6.x		5/31/16
Incident Response	Mandiant Intelligent Response (MIR)		NASA Security Configuration Settings (ASCS)	3.x		5/31/16
Vulnerability Protection	Enhanced Mitigation Experience Toolkit (EMET)			5.5	9/30/16	5/31/16

Windows 10 NASA Optional Supported Software						
Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Date	Approved on NASA Interoperable systems
Web Browser	Google Chrome	W3C and industry standards	NASA Security Configuration Settings (ASCS); See section 7; Auto-update on			5/31/16
Softphone Client	Cisco Jabber	SIP/RTP	For soft phone use only	11.5.x		5/31/16
Note Taking	Microsoft OneNote Professional	Office Open XML document format	NASA Security Configuration Settings (ASCS)	2016		5/31/16
Database	Microsoft Access			2016		5/31/16
Desktop Publishing	Microsoft Publisher			2016		5/31/16
Audio/video players	Microsoft Silverlight	Various Multimedia		5.1.x	10/12/21	5/31/16
Audio/video players	Microsoft Windows Media Player	Windows Media Files	Default for all supported formats	12.x		5/31/16
Multimedia player	Apple iTunes	Various Multimedia		12.x		5/31/16
Instant Messaging	Pidgin	XMPP	NASA Jabber Service; Pidgin-sipe OCS plugin	2.10.x		5/31/16
Virtualization	VMware Workstation			12.x		5/31/16
Project Management	Microsoft Project			2013		5/31/16
				2016		5/31/16
PDF Creator	Adobe Acrobat Pro			XI		5/31/16
Access to Centrally Served Windows Applications	Citrix Receiver for Windows			4.4.x		5/31/16

3.4 Client Reference Configuration for OS X 10.10

OS X 10.10 NASA Core Build						
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Dates**	**Approved on NASA Interoperable Systems**
Operating System	OS X		NASA Security Configuration Settings (ASCS)	10.10.x	8/31/16	3/31/15
Applications, Plugins, and Tools						
Word Processing	Microsoft Word for Mac	Office Open XML document format	NASA Security Configuration Settings (ASCS)	Word 2011 14.5.x	Permitted for use. No new installs	11/1/15
				Word 2016 15.x	New installs	1/1/16
Spreadsheet	Microsoft Excel for Mac	Office Open XML document format	NASA Security Configuration Settings (ASCS)	Excel 2011 14.5.x	Permitted for use. No new installs	11/1/15
				Excel 2016 15.x	New installs	1/1/16
Presentation	Microsoft PowerPoint for Mac	Office Open XML document format	NASA Security Configuration Settings (ASCS)	PowerPoint 2011 14.5.x	Permitted for use. No new installs	11/1/15
				PowerPoint 2016 15.x	New installs	1/1/16
Electronic Mail and Calendaring	Microsoft Outlook for Mac	IMAP4, SMTP, IMAP over TLS, MAPI over HTTP	NASA Security Configuration Settings (ASCS); Configured for access to NOMAD	Outlook 2011 14.5.x	Permitted for use. No new installs	11/1/15
				Outlook 2016 15.x	New installs	1/1/16
Electronic Mail	Apple Mail	IMAP4, SMTP, IMAP over TLS, MAPI over HTTP	NASA Security Configuration Settings (ASCS); Configured for access to NOMAD; Use Outlook for S/MIME	7.3.x		3/31/15
Calendaring	Apple iCal	iCalendar (RFC 5545)		8.0.x		3/31/15
Secure Electronic Mail	Microsoft Outlook for Mac with Entrust Secure Desktop for Mac (SDM)	IMAP4, SMTP, IMAP over TLS, MAPI over HTTP	NASA Security Configuration Settings (ASCS); Configured for access to NOMAD	Outlook 2011 14.4.x or Outlook 2016 15.x ; SDM 8.1.x build 5 or later		3/31/15

			OS X 10.10 NASA Core Build			
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Dates**	**Approved on NASA Interoperable Systems**
Instant Messaging and Web Conferencing	Microsoft Lync	SIP	NASA Security Configuration Settings (ASCS); Enterprise OCS Settings; Configured for access to NOMAD	14.0.x		3/14/14
Instant Messaging	Apple Messages	XMPP		Bundled		3/31/15
PDF Viewer and Electronic Forms	Adobe Acrobat Reader DC	PDF	NASA Security Configuration Settings (ASCS)	2015	Default	5/31/16
PDF Viewer	Apple Preview	PDF		8.1.x		5/31/16
Java	Oracle Java run-time environment (JRE)		NASA Security Configuration Settings (ASCS); AES256 Strong Crypto	Java 8	9/1/17	3/31/15
Audio/video players	Adobe Flash Player	Flash SWF		21.x		5/31/16
Multimedia player	Apple iTunes	Various Multimedia	Default for all supported formats	12.0.x		3/31/15
Audio/video players	Apple QuickTime Player	Various Multimedia	Default for QuickTime formats	10.4.x		3/31/15
Photo Editing	Apple Photos			1.3.x		5/31/16
Browsers						
Web Browser	Apple Safari	W3C and industry standards	NASA Security Configuration Settings (ASCS)	9.0.x		11/1/15
Web Browser	Mozilla Firefox Extended Support Release	W3C and industry standards	NASA Security Configuration Settings (ASCS); NFCE v2016.1 or higher; See section 7; Recommend automatic updates enabled	45.x		5/31/16
ICAM						
Smartcard Middleware	ActivClient for Mac	NIST SP800-73 Part 4	See section 7.1	4.0.1		1/1/16

OS X 10.10 NASA Core Build						
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Dates**	**Approved on NASA Interoperable Systems**
Content Encryption	Entrust Secure Desktop for Mac (SDM)	S/MIME	Configured for access to NOMAD; See section 7	Outlook 2011 14.4.x SDM 8.1.x build 5 or later		3/31/15
				Outlook 2016 15.x SDM 8.1.x build 5 or later		1/1/16
Trust Anchor Management	NASA Trust Anchor Management	X.509	See section 7	2016.x		5/31/16
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)			2016.x		5/31/16
Security						
Firewall	Apple Firewall		NASA Security Configuration Settings (ASCS); Allow signed software; Enable firewall logging			3/31/15
Anti-Virus and Anti-Malware	Symantec Endpoint Protection for Mac		Enterprise update server	12.1.x	RU 4 or newer	3/31/15
Data at Rest Full Disk Encryption	FileVault 2, Symantec PGP Whole Disk Encryption		Configured to use key escrow; See section 8.5.1	FilleVault2 – bundled	Symantec PGP removed by 8/31/16	3/31/15
Patch Reporting	Dell KACE	KACE Proprietary	See section 8.2.1; Auto-updates enabled	6.x		3/31/15

			OS X 10.10 NASA Optional Supported Software			
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Date**	**Approved on NASA Interoperable systems**
Web Browser	Google Chrome	W3C and industry standards	NASA Security Configuration Settings (ASCS); See section 7			3/31/15
Audio/video players	Microsoft Silverlight	Various Multimedia		5.x	10/12/21	11/1/15
Audio/video players	Flip4Mac WMV	Windows Media		3.3.x		5/31/16
Softphone Client	Cisco Jabber	SIP/RTP	For soft phone use only	10.5.x		5/31/16
Note Taking	Microsoft OneNote 2011 for Mac	Office Open XML document format	NASA Security Configuration Settings (ASCS)	14.5.x	Permitted for use. No new installs	11/1/15
Note Taking	Microsoft OneNote 2016 for Mac	Office Open XML document format	NASA Security Configuration Settings (ASCS)	15.x	New installs	1/1/16
Instant Messaging	Adium	XMPP	NASA Jabber Service; Pidgin-sipe OCS plugin	1.5.x		5/31/16
Virtualization	VMware Fusion			8.0.x		11/1/15
Project Management	OpenProj			1.4		5/31/16
PDF Creator	Adobe Acrobat Pro			XI		5/31/16
Access to Centrally Served Windows Applications	Citrix Receiver			12.1.x		5/31/16

3.5   Client Reference Configuration for OS X 10.11

			OS X 10.11 NASA Core Build			
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Dates**	**Approved on NASA Interoperable Systems**
Operating System	OS X		NASA Security Configuration Settings (ASCS)	10.11.x		1/1/16

OS X 10.11 NASA Core Build						
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Dates**	**Approved on NASA Interoperable Systems**
Applications, Plugins, and Tools						
Word Processing	Microsoft Word 2016 for Mac	Office Open XML document format	NASA Security Configuration Settings (ASCS)	Word 2016 15.x		1/1/16
Spreadsheet	Microsoft Excel 2016 for Mac	Office Open XML document format	NASA Security Configuration Settings (ASCS)	Excel 2016 15.x		1/1/16
Presentation	Microsoft PowerPoint 2016 for Mac	Office Open XML document format	NASA Security Configuration Settings (ASCS)	PowerPoint 2016 15.x		1/1/16
Electronic Mail and Calendaring	Microsoft Outlook 2016 for Mac	IMAP4, SMTP, IMAP over TLS, MAPI over HTTP	NASA Security Configuration Settings (ASCS); Configured for access to NOMAD	Outlook 2016 15.x		1/1/16
Electronic Mail	Apple Mail	IMAP4, SMTP, IMAP over TLS, MAPI over HTTP	NASA Security Configuration Settings (ASCS); Configured for access to NOMAD; Use Outlook for S/MIME	9.0.x		1/1/16
Calendaring	Apple iCal	iCalendar (RFC 5545)	Configured for access to NOMAD	8.0.x		1/1/16
Secure Electronic Mail	Microsoft Outlook 2016 for Mac with Entrust Secure Desktop for Mac (SDM)	IMAP4, SMTP, IMAP over TLS, MAPI over HTTP	NASA Security Configuration Settings (ASCS); Configured for access to NOMAD; Version depends upon type of smartcard; See https://pki.nasa.gov	Outlook 15.x SDM 8.1.x build 5 or later		1/12/16
Instant Messaging and Web Conferencing	Microsoft Lync	SIP	NASA Security Configuration Settings (ASCS). Enterprise OCS Settings Configured for access to NOMAD	14.0.x		1/1/16
Instant Messaging	Apple Messages	XMPP		Bundled		1/1/16
PDF Viewer and Electronic Forms	Adobe Acrobat Reader DC	PDF	NASA Security Configuration Settings (ASCS)	2015	Default	5/31/16
PDF Viewer	Apple Preview	PDF		8.1.x		1/1/16

OS X 10.11 NASA Core Build						
Function	Application	Interface Standard	Required Settings	Version	Comments & Required Removal Dates	Approved on NASA Interoperable Systems
Java	Oracle Java run-time environment (JRE)		NASA Security Configuration Settings (ASCS); AES256 Strong Crypto	Java 8	9/1/17	1/1/16
Multimedia player	Apple iTunes	Various Multimedia	Default for all supported formats	12.3.x		1/1/16
Audio/video players	Apple QuickTime Player	Various Multimedia	Default for QuickTime formats	10.4.x		1/1/16
Audio/video players	Adobe Flash Player	Flash SWF		21.x		5/31/16
Photo Editing	Apple Photos			1.3.x		5/31/16
Browsers						
Web Browser	Apple Safari	W3C and industry standards	NASA Security Configuration Settings (ASCS)	9.0.x		1/1/16
Web Browser	Mozilla Firefox Extended Support Release	W3C and industry standards	NASA Security Configuration Settings (ASCS); NFCE v2016.1 or higher; See section 7; Recommend automatic updates enabled	45.x		5/31/16
ICAM						
Smartcard Middleware	ActivClient for Mac	NIST SP 800-73 Part 4	See section 7.1	4.0.1		1/1/16
Content Encryption	Entrust Secure Desktop for Mac (SDM)	S/MIME	Configured for access to NOMAD; See section 7	Outlook 15.x SDM 8.1.x build 5 or later		1/12/16
Trust Anchor Management	NASA Trust Anchor Management	X.509	See section 7	2016.x		5/31/16
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)			2016.x		5/31/16
Security						

OS X 10.11 NASA Core Build						
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Dates**	**Approved on NASA Interoperable Systems**
Firewall	Apple Firewall		NASA Security Configuration Settings (ASCS); Allow signed software; Enable firewall logging			1/1/16
Anti-Virus and Anti-Malware	Symantec Endpoint Protection for Mac		Enterprise update server	12.1.x	RU 4 or newer	1/1/16
Data at Rest Full Disk Encryption	FileVault 2		Configured to use key escrow; See section 8.5.1	FilleVault2-bundled		1/1/16
Patch Reporting	Dell KACE	KACE Proprietary	See section 8.2.1; Auto-updates enabled	6.x		1/1/16

OS X 10.11 NASA Optional Supported Software						
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Date**	**Approved on NASA Interoperable systems**
Web Browser	Google Chrome	W3C and industry standards	NASA Security Configuration Settings (ASCS); See section 7			1/1/16
Audio/video players	Microsoft Silverlight	Various Multimedia		5.x	10/12/21	1/1/16
Audio/video players	Flip4Mac WMV	Windows Media		3.3.x		5/31/16
Softphone Client	Cisco Jabber	SIP/RTP	For soft phone use only	10.5.x		5/31/16
Note Taking	Microsoft OneNote 2016 for Mac	Office Open XML document format	NASA Security Configuration Settings (ASCS)	15.x		1/1/16
Instant Messaging	Adium	XMPP	NASA Jabber Service; Pidgin-sipe OCS plugin	1.5.x		5/31/16
Virtualization	VMware Fusion			8.0.x		1/1/16
Project Management	OpenProj			1.4		5/31/16

OS X 10.11 NASA Optional Supported Software						
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Date**	**Approved on NASA Interoperable systems**
PDF Creator	Adobe Acrobat Pro			XI		5/31/16
Access to Centrally Served Windows Applications	Citrix Receiver			12.1.x		5/31/16

3.6 Client Reference Configuration for Linux

Linux NASA Core Build						
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 Security Configuration Settings (ASCS)	6.0 or later		6/24/08
Operating System	Ubuntu LTS		NASA Security Configuration Settings (ASCS)	14.04.x		9/22/14
Applications, Plugins, and Tools						
Office Automation	LibreOffice	OASIS Open Document Format	NASA Security Configuration Settings (ASCS); Configure to use Office Open XML file format by default	5.x		5/31/16
Electronic Mail	Evolution	IMAP4, SMTP, IMAP over TLS, MAPI over HTTP	NASA Security Configuration Settings (ASCS); Configured for access to NOMAD	12.0.x	RHEL	8/1/12
Electronic Mail **Secure Electronic Mail**	Mozilla Thunderbird	IMAP4, SMTP, IMAP over TLS, MAPI over HTTP S/MIME	NASA Security Configuration Settings (ASCS); Configured for access to NOMAD	38.x	Ubuntu	11/1/15
Calendaring	Microsoft Outlook Web Access (NOMAD)	iCalendar (RFC 5545)	Web Browser	2.x		6/24/08

Linux NASA Core Build						
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Dates**	**Approved on NASA Interoperable Systems**
Instant Messaging	Pidgin	XMPP		2.10.x		6/24/08
PDF Viewer and Electronic Forms	Adobe Acrobat Reader DC	PDF	NASA Security Configuration Settings (ASCS)	2015		2015
Java run-time environment (JRE)	Oracle Java		NASA Security Configuration Settings (ASCS); AES256 Strong Crypto	Java 8	9/1/17	3/31/15
Audio/video players	MPlayer	Multimedia	Default for supported formats	1.0.x		6/24/08
Audio/video players	Adobe Flash Player	Flash SWF		11.2.x		3/31/15
Browsers						
Web Browser	Mozilla Firefox Extended Support Release	W3C and industry standards	NASA Security Configuration Settings (ASCS); NFCE v2016.1 or higher; See section 7; Automatic updates enabled	45.x		5/31/16
ICAM						
Smartcard Middleware	OpenSC	NIST SP800-73 Part 4	See section 7.1			9/1/13
Trust Anchor Management	NASA Trust Anchor Management	X.509	See section 7	2016.x		5/31/16
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)			2016.x		5/31/16
Security						
Firewall	Firewall		NASA Security Configuration Settings (ASCS); Control inbound and outbound connections enabled	Bundled		6/24/08
Anti-Virus	Symantec Antivirus for Linux			1.0.x		8/1/12

Linux NASA Core Build						
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Dates**	**Approved on NASA Interoperable Systems**
Data at Rest Encryption	Symantec PGP Whole Disk Encryption, Linux Unified Key Setup (LUKS)		Configured to use enterprise key escrow service			8/1/12
Patch Reporting	Dell KACE	KACE Proprietary	See section 8.2.1; Auto-updates enabled	6.x		9/22/14

Linux NASA Optional Supported Software						
Function	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Comments & Required Removal Date**	**Approved on NASA Interoperable systems**
Web Browser	Google Chrome	W3C and industry standards	NASA Security Configuration Settings (ASCS)		Not available for RHEL	8/1/12
Project Management	OpenProj			1.4		5/31/16
PDF Creator	Scribus			1.4		5/31/16
Access to Centrally Served Windows Applications	Citrix Receiver			13.3		5/31/16

3.7 Client Reference Configuration for Mobile Computing Systems

Client Reference Configuration for Mobile Computing Systems				
Functionality	**Application**	**Required Settings**	**Version**	**Effective Date**
Operating System	iOS	CIS Benchmarks with NASA Guidance	9.2 or later	5/31/16
Operating System	Android	CIS Benchmarks with NASA Guidance	5.0 or later	5/31/16

4 OPERATING SYSTEMS

4.1 Operating System Standards, Timelines, and Compliance Dates

ASCS provides information of the software life cycle for supported operating systems and applications. 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

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 FISMA requirements.

Microsoft Windows Timeline	
Windows Version	**Guidance**
Windows 7	Approved for use. No new installs after July 1, 2017 Removal required by July 1, 2018
Windows 8.1	Approved for use. Upgrade to Windows 10 Enterprise as soon as possible, no later than July 1, 2017.
Windows 10 Enterprise	Approved for use on May 31, 2016. Required on all new or refreshed systems by July 1, 2017 Required on all Windows systems by July 1, 2018 * Note: There are interoperability issues with Agency applications using Windows 10. See the Windows 10 assessment website for up to date information. https://etads.nasa.gov/research/windows10-enterprise-assessment/

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   Microsoft Windows 8

Windows 8.1 or greater is approved for use. No general migration or retrofit is required of NASA service provider systems to Windows 8.x. It is recommended that all Windows 8.1 systems are be updated to Windows 10 as soon as possible, and they must be updated to Windows 10 by July 1, 2017.

4.2.3   Windows 10

Windows 10 Enterprise is approved for use May 31, 2016. The Enterprise version of Windows 10 incorporates security features that the Agency plans to utilize. Windows 10 is available through the Enterprise License Management Team (ELMT) managed agreement. Information on ordering from the Enterprise License Agreement (ELA) can be found at:

https://www.nssc.nasa.gov/elmt

Windows 10 will be required on all new or refreshed systems by July 1, 2017, and on all systems by July 1, 2018.

To ensure adoption of Windows 10, Microsoft has changed the support structure for the Windows operating system. Windows 7 and Windows 8.1 are no longer available for purchase; and after October 31, 2016, OEM's will no longer be allowed to ship hardware with Windows 7 or 8.1 installed. Enterprises with volume licensing agreements have the rights to downgrade Windows 10 systems to Windows 7. After July 17, 2018 any system running Windows 7 with a Skylake Intel processor will no longer be supported by Microsoft. Systems with a Kaby Lake Intel processor will only run Windows 10 or later.

The ETADS Windows 10 Enterprise Interoperability Assessment identified some Agency applications that have interoperability issues. The owners of the identified applications are working with the associated software vendors for resolutions. The assessment and findings, as well as up-to-date information on application interoperability, can be found at:

https://etads.nasa.gov/research/windows10-enterprise-assessment/

4.3   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 10.11 (El Capitan) was approved for use January 1, 2016. Version 10.11 is the default operating system for all OS X systems. OS X 10.10 shall be removed from all systems by August 31, 2016.

Apple OS X Timeline	
OS X Version	**Guidance**
10.10 Yosemite	Approved for use on interoperable NASA systems March 31, 2015. Removal required by August 31, 2016. After May 31, 2016 10.10 shall not be deployed on any new or refreshed systems.
10.11 El Capitan	Approved for use on interoperable NASA systems January 1, 2016. Default for all OS X systems
10.12	Release expected in September 2016.

4.4   Linux

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.

4.4.1 Red Hat

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

4.4.2 Ubuntu

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

http://www.ubuntu.com/

Note: Ubuntu may become unsupported in the NASA environment if it is found that it cannot meet Agency PIV authentication requirements.

4.5 Mobile

The mobile operating systems supported will apply NASA Baseline Security Settings. For iOS devices, version 9.2 or later is required. For Android devices, version 5.0 or later is required.

Future Expected Updates: The Mobile Device Management (MDM) Project will require the following additional requirements:

- MaaS360 secure container support for Microsoft Exchange
- 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

5 APPLICATIONS

5.1 Office Automation Applications

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

5.1.1 Office 2013

Microsoft Office 2013 Standard Edition or better was approved for use on NASA interoperable systems January 29, 2014. Microsoft Office 2013 is approved for use on existing Windows systems. Microsoft Office 2013 is not approved for installation on new Windows systems. New Windows systems shall install Microsoft Office 2016.

If running Office 2013, 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 Microsoft recommends the 32-bit version for most users.

5.1.2 Office 2016 for Windows

Microsoft Office Professional 2016 is approved for use on interoperable Windows systems and is the default office automation version for new Windows systems, as well as Windows 10 systems.

5.1.3 Office 2011 for Mac

Microsoft Office 2011 for Mac (Standard Edition) was approved for use on interoperable OS X systems as of December 1, 2010. Office 2011 for Mac must be removed from all systems by August 31, 2016.

5.1.4 Office 2016 for Mac

Microsoft Office 2016 for Mac was approved for use on interoperable OS X systems as of January 1, 2016. Office 2011 for Mac must be upgraded to Office 2016 for Mac by August 31, 2016 on all OS X 10.10 systems or newer.

5.1.5 LibreOffice

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

5.1.6 Office 365

Future Expected Updates: NASA has initiated an effort to migrate core enterprise email, calendaring, and instant messaging services to the Microsoft Office 365 cloud environment. A phased approach will be implemented starting with a limited pilot then moving onto full production for email, calendaring, and instant messaging. Later phases will be initiated to evaluate, and if approved, provide further migration to additional options with a goal of moving to a full E3 implementation. NASA anticipates significant changes will be required to our software licensing approach, end user training and outreach, and communications.

5.2 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.

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.

Note that interoperability issues exist with Apple Mail and S/MIME and 4-cert smartcard compatibility. At this time, it is not recommended to send encrypted mail using Apple Mail.

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, 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 NASA Electronic Forms System (NEFS) portal that 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 require:

- Adobe Reader DC
- Standard NASA supported browser (configured to open PDF documents with Adobe Reader)

Future Expected Updates: Electronic forms integration with four certificate FIPS 201-2 smartcards for document electronic signature.

5.4 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. The current version of VMware must be installed, 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.

5.5 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.

5.5.1 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

Web browser vendors have changed the browser delivery model. The frequency of 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 and Firefox ESR must be available on Agency interoperable Windows systems; Safari and Firefox ESR must be available on Agency interoperable Macs; and Firefox ESR on Linux systems.

For Internet Explorer, NASA will maintain support for the most recent production version. 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. 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/

Future Expected Updates: Of special note to web application developers is that browser vendors have dropped support, or are dropping support for NPAPI, impacting plugins for Silverlight, Java applets, Facebook Video and other similar NPAPI based plugins. Chrome no longer supports NPAPI, and Mozilla intends to remove support for most NPAPI plugins in Firefox by the end of 2016.

6.1.1 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.

6.1.2 Microsoft Edge

Since Microsoft Edge is bundled with Windows 10 it is available but not recommended for use at this time due to interoperability issues with some Agency applications. See the Windows 10 assessment website for up to date information. https://etads.nasa.gov/research/windows10-enterprise-assessment/

6.1.3 Mozilla Firefox Extended Support Release

Mozilla Firefox Extended Support Release (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.

6.1.4 Apple Safari

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

6.1.5 Google Chrome

Google Chrome is approved for use on all interoperable Windows and OS X systems, and is 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.

7 ICAM DEVICE INTEGRATION CONFIGURATION REQUIREMENTS

The Identity, Credential and Access Management (ICAM) 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.

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

Future Expected Updates: User authentication with PIV-derived x.509 soft-certificate credentials for use on managed mobile devices.

Future Expected Updates: The NASA Smartcard (NSc) will provide strong authentication, and S/MIME capability for NASA workers who are ineligible for being issued a PIV smartcard.

ICAM Device Integration configuration requirements, which include settings for operating system, browser, and middleware, can be found at: http://etads.nasa.gov/idi/

Future Expected Updates: Over the past several years, the NASA ETADS and ICAM teams have developed the end user device smartcard login capability to meet the mandates and specifications of HSPD-12, FIPS 201, OMB M11-11 and other related technical specifications. The solutions meet interoperability guidelines and include infrastructure enhancements and

enterprise level management tools. The planned implementation for non-Windows systems are based on the Centrify DirectManage Access Software, which provides the most comprehensive suite of capabilities for enterprise-wide deployment. The agency team is developing solutions in alignment with the PIV Mandatory Implementation Plan, and are in the process of finalizing the solutions for Mac OS X systems and RHEL Linux end user systems.

Capabilities of the Centrify DirectManage based solution:

- Enables non-Windows platforms to utilize Active Directory authentication.
- Enables Active Directory based policy management via Group Policy Objects for effective centralized management on non-Windows client systems.
- Enables the use and enforcement of smartcard login for NCAD basic user and resource administrator accounts in accordance with PIV Mandatory login requirements.
- Allows for the proper UNIX User Identifier (UID) to be assigned to user client systems based on the agency Universal Uniform Personal Identification Code (UUPIC).
- Enables NAMS to be used to control PIV requirement provisioning for Mac OS X and RHEL Linux end user systems.

A final assessment of the solution for smartcard system login for Mac OS X and RHEL is planned once the upcoming release of the Centrify DirectManage Access Software is available, tentatively May 2016. The assessment and findings, as well as up-to-date information on application interoperability and proposed development schedule can be found at:

https://etads.nasa.gov/research/centrify-directmanage-assessment

Once the final version of the Centrify DirectManage Client and corresponding configuration guidance are known, this information will be published in an addendum to NASA-STD 2804 and incorporated into a revision of the standard.

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 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 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/ntam

7.4   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 issues FIPS 201-2 PIV smartcards 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.

7.5   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.

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 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 systems, the Smartcard Middleware package, DSI version 3.x is required to be on all interoperable systems. 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.] The DSI version 3.x is required to be on interoperable Windows 10 systems; however, use of the smartcard on the Edge browser is not yet supported. An update to the DSI package which support for the Edge browser is expected by August 2016.

7.7   Password Management

For password management information, see the IT Security Standard at:

https://etads.nasa.gov/ascs/it-security-standard/

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 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 specifies software that is 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. For detailed security information for NASA IT systems, see the IT Security Standard available at:

https://etads.nasa.gov/ascs/it-security-standard/

8.1   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 systems (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, Department of Defense (DoD) Security Technical Implementation Guides (STIGs), 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.

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.

8.2.1   System Configuration Reporting and Patch Management

The Agency's Patch and Configuration Management Reporting Agent is currently provided by Dell KACE. Agency policy requires this software to be installed on all NASA end-user devices for which a vendor supported agent is available. 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/

Future Expected Updates: As a result of the Federal Government's CDM Program, NASA is currently in the process of transitioning from the Dell KACE software and moving to the IBM BigFix software to meet the patch and configuration management reporting requirements. The NASA CDM project team will work with each center, mission and service office to coordinate the transition from KACE to BigFix on all end-user devices. At the conclusion of the transition, Dell KACE will be decommissioned and IBM BigFix will be the official solution for the Agency.

8.2.2   Whitelisting

Future Expected Updates: As part of the Federal Government's Continuous Diagnostics and Mitigation (CDM) Program, NASA is implementing a whitelisting capability through the deployment of the RES agent on all end-user devices for which a vendor supported agent is available. The RES agent is a piece of software which will provide the capability to prevent unauthorized software from running on the end-user device and will be required to run on all end-user devices for which there is a vendor supported agent. The NASA CDM Project team is currently working with the Department of Homeland Security (DHS) to finalize the details of the deployment and operations of the RES software on NASA devices.

8.3   Anti-Exploitation Tool

NASA is required to implement control baselines as defined in NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations". In order to meet the System and Information Integrity Controls for memory protection (SI-16), an organizationally defined value (ODV) has been created for the installation of the Enhanced

Mitigation Experience Toolkit (EMET) on all Microsoft Windows systems. This is also a FISMA 2016 reportable metric "3.9: Number of GFE endpoints covered by an anti-exploitation tool".

8.4   Incident Response

The Mandiant Intelligent Response (MIR) agent is an incident response investigation and evidence collection tool. It is designed by and for incident responders to collect evidence from possibly compromised machines anywhere in a network. At this time the Agency only requires the MIR agent for all Windows systems.

8.5   Data Encryption

8.5.1   Data at Rest (DAR) Encryption

All Agency systems shall implement a DAR encryption solution. Symantec PGP Desktop, FileVault 2, and Microsoft BitLocker are acceptable solutions for Data at Rest (DAR) encryption. Please refer to the Client Reference Configurations for specific operating systems.

DAR encryption solutions shall 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 4.
- 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.

Future Expected Updates: As described in section 7.1, Authentication Configuration Requirements, the agency is developing the smartcard login solution for Mac OS X end user systems based on the Centrify DirectManage Access Software Suite. To support smartcard login and to ensure proper use of passwords for pre-boot authentication, FileVault will need to be reconfigured, per DAR configuration guidelines (in development).

The configuration guidelines will initially be published on the ICAM Device Integration Mac OS X page:

https://etads.nasa.gov/idi/os-x/

8.6   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/groups/STM/cmvp/documents/140-1/140val-all.htm

9 NETWORK

9.1 Internet Protocol version 6 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.

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 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.

9.2 Network Access Control

9.2.1 Enterprise External Border Protection

Future Expected Updates: The Enterprise External Border Protection Project (EBPro) will deploy a set of solutions designed to improve the security posture of NASA's corporate networks and IT infrastructure, one of which is Cisco's Adaptive Security Appliance (ASA) as an Agency VPN solution. The ASA requires deployment on the Cisco AnyConnect Secure Mobility Client.

The Communication Service Office's EBPro Project team will deploy the infrastructure necessary to support the Agency VPN solution. The Project team will then work with the VPN Service Line to identify existing profiles, and begin transitioning users in September 2016. Centers currently using a Cisco VPN client are already moving to the Project's recommended version in order to meet ICAM requirements for PIV. The schedule for transitioning the remaining centers is in the planning stage, but tentatively planned for September – December, 2016.

9.2.2 Agency Virtual Private Network

Future Expected Updates: As part pf the EBPro Project, the Agency will provide a Cisco AnyConnect Secure Mobility Client as the standard Virtual Private Network (VPN) client. The timeframe is tentatively scheduled for September-December, 2016, transitioning pilot users as early as September, 2016.

9.2.3 Enterprise Internal Border Protection

Future Expected Updates: The CSO's Enterprise Internal Border – Network Access Control (EIB-NAC) Project will implement a network access control solution that authenticates, assesses, validates, and places network-connecting endpoints and users into network zones commensurate with applicable security policy. The posturing capabilities provided by the Cisco AnyConnect client will be provided as part of EIB-NAC Release 4, currently scheduled for October, 2016.

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. 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.

10.1.1 Section 508 Tools

Section 508 Tools			
Function	**Windows**	**OS X**	**Linux**
Screen Reading Software	JAWS 17.x or higher, VoiceOver, Window Eyes 9.x or higher, NVDA 2015.1 or higher (IE or Firefox), ChromeVox (Chrome)	VoiceOver (Safari, Firefox, Chrome)	ORCA (Gnome 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 14	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,	Adobe Acrobat 8.x or higher	

Section 508 Tools			
Function	**Windows**	**OS X**	**Linux**
	NetCentric Technologies, CommonLook Plug-in for Acrobat		
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)	
HTML accessibility validator	Total Validator	Total Validator	Total Validator

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 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.

10.2.2 Printers

All clients must be configured for duplex printing by default.

11 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 Enterprise Technology Assessments and Digital Standards (ETADS) Office. 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.

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:

http://etads.nasa.gov/dcs

14 COMMENTS

NASA-STD-2804, Minimum Interoperability Software Suite, includes information from teams and projects across the Agency. If information from your team or project is referenced in the Standard, please review and provide updated information to your Center Chief Information Office.

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
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 Management 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
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
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, OS X, 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 4.0, Client Reference Configurations.