



NASA Standard Operating Procedure

Master Information Technology Security Plan Template, Requirements, Guidance and Examples

ITS-SOP-0032

Version: 20060711

Effective Date: 11 July, 2006

Expiration Date: 11 July, 2008

Responsible Office: Office of the Chief Information Officer

Revision Record

ITEM NO.	REVISION	DESCRIPTION	DATE
1	V.1.0	First Publication	Oct. 05, 2005
2	V.2.0	Sotiris Baxevanis, Updated for NIST 800-18 Rev. 1	Mar. 24, 2006
3	V.2.1	Sotiris Baxevanis, Updated per OCIO comments	May 4, 2006
4	V.2.2	Andrew Boncek, Content update and format changes	May 5, 2006
5	V2.3	Sotiris Baxevanis, Updated per OCIO comments	May 10, 2006
6	V2.4	Andrew Boncek, Content update to OCIO comments, 800-53 references	May 11, 2006
7	V2.5	Andrew Boncek, Update to include 800-53 examples	May 22, 2006
8	V2.5	Andrew Boncek, Update to include OCIO comments	June 5, 2006
9	V2.6	Marion Meissner, Andrew Boncek, Update for 2810.1A and table	June 28, 2006
10	V2.7	Marion Meissner, Andrew Boncek, Update to address changes in ITS-SOP-0016 and 0019	July 11, 2006

Master Information Technology Security Plan Template, Requirements, Guidance and Examples

1. Introduction

This document defines the information technology (IT) security plan template for Master systems and provides requirements, guidance and examples for the completion of these plans. The template acts as an outline to capture information regarding the Master system's function, operational concept, type and category of information residing in the Subordinate systems associated with the Master plan, and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 controls that the associated Subordinate systems will inherit from the Master plan.

The Master security plan template defined in this standard operating procedure (SOP) is based on Federal Information Processing Standard (FIPS) 199, FIPS 200, NIST SP 800-18 Rev. 1 and other NIST 800 series guidance. The NASA Senior Agency Information Security Officer (SAISO) is responsible for updating this SOP to address published updates by NIST as well NASA policy requirements.

ITS-SOP-0011 Procedure for Master Security Plans defines the procedure in detail for creating a Master security plan per NPR 2810.1 requirements. The approval process for Master security plans described in ITS-SOP-0011 is analogous to the certification and accreditation (C&A) process for Subordinate systems.

2. References

- NPD 2810.1 "NASA Information Security Policy"
- NPR 2810.1 "Security of Information Technology"
- NIST SP 800-18 Rev. 1 "Guide for Developing Security Plans for Federal Information Systems"
- NIST SP 800-53, "Recommended Security Controls for Federal Information Systems"
- NIST SP 800-60 "Guide for Mapping Types of Information and Information Systems to Security Categories"
- FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems"
- FIPS 199 "Standards for Security Categorization of Federal Information and Information Systems"

3. Template, Requirements and Examples

Appendix A of this SOP provides a complete Master security plan template including cover pages and associated appendices and contains instructions and examples specific to Master security plans. This template is the definitive source of the security plan template for Master systems in NASA's IT Security Reporting Repository and Documentation Database (ITSR2D2).

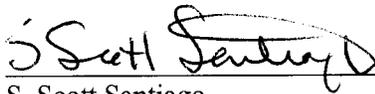
ITS-SOP-0016 provides a template and instructions for NASA Subordinate system security plans.

The templates for Master security plans and Subordinate system security plans both conform to NIST SP 800-18 Revision 1 and have the same structure, except for the addition, in the Master security plan template, of

- the section titled 'Subordinate Systems' in the Executive Summary and
- 'Appendix A' which lists Subordinate systems covered by the Master security plan.

All NASA Master security plans should be completed online using ITSR2D2. However, this SOP shall serve as the standard template for both manual and ITSR2D2 Master plans. In order to assist the plan writer, the template contains the following sections:

- Template – Any section of the template not included within brackets is mandatory and requires that the writer complete the information for the section or utilize the language provided; complete the defined table, address specific questions, etc.
- [INFORMATION to be filled in] – Text in brackets must be replaced by the appropriate information specific to the plan.
- *{Instructions: specific instruction text}* – Any section in italics and braces provides specific requirements, guidance, and examples for each plan section to ensure completeness and consistency among security plans. These instructions should be deleted from the final Master security plan.



S. Scott Santiago
Deputy CIO for IT Security

7/11/06
Date

Appendix A – Master Security Plan Template

Master IT Security Plan

National Aeronautics & Space Administration

[Center Name]

Master Security Plan for the [SYSTEM NAME] XX-*nnn*-Y-*ZZZ*-*nnnn*

Issue Date: [MM-DD-YYYY]

Effective Date: [MM-DD-YYYY]

Verify that this is the correct version before use.

***WARNING:** This document is SENSITIVE BUT UNCLASSIFIED (SBU). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with NASA policy relating to SBU information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized NASA official.*



National Aeronautics and
Space Administration

Master Plan Approval Decision Letter

From: [Name], Authorizing Official

Date:

To: [Name], Master Security Plan Owner

Subject: Master Security Plan Approval Decision for [SYSTEM NAME]

In accordance with FISMA requirements, the attached Master security plan has been developed to address Federal Information Processing Standards (FIPS) 199 & 200 requirements for all information systems identified as subordinate to this plan. I have reviewed this Master security plan for the [SYSTEM NAME], including a detailed review of the following critical plan sections:

- System description,
- Combined information types resident across all Subordinate systems,
- FIPS 199 security categorization,
- Identified interconnections between the [SYSTEM NAME] system and other systems within or outside of NASA,
- NASA tailored security controls,
- [SYSTEM NAME] risk assessment,
- and the Plan of Action and Milestones (POA&M)

I have determined that the risk to Agency operations, Agency assets, and/or individuals resulting from the inheritance by all identified Subordinate information systems of the information types, FIPS 199 security categorization and security controls in this plan is acceptable. Accordingly, I am issuing an approval for this plan, its FIPS 199 security categorization and its identified security requirements and controls.

Each Subordinate to this Master security plan shall inherit the information types, FIPS 199 security categorization and security controls from this plan. Any variances between the security controls of this Master security plan and a Subordinate shall be addressed in each Subordinate's POA&M and the Subordinate shall be brought into compliance with this Master security plan within twelve (12) months of the Subordinate's Authorization to Operate (ATO) date.

The approval of this Master security plan will remain in effect as long as: (i) the Senior Agency Information Security Official (SAISO) does not issue additional requirements, controls or enhancements, including in response to NIST FIPS and Special Publication updates; (ii) the vulnerabilities reported during the continuous monitoring process do not result in additional Agency-level risk which is deemed unacceptable; and (iii) this plan has not exceeded five (5) years between security approvals.

A copy of this letter with all supporting documentation should be retained in accordance with the Agency's record retention schedule.

[Name],
[Title]

Date

Executive Summary

{Instructions: Provide an overall description of the Master information system. Identify and briefly describe the Subordinate information systems}

IT Security Strategy

{Instructions: Brief description of the Master system's business functionality and its relevance to the overall NASA Information Technology Enterprise Architecture.}

Information System Name /Title

System Name: [SYSTEM NAME]

System Abbreviation: [SYSTEM ABBREVIATION]

System Unique Identifier: [NASA SUI]

Information System Type

[] Major Application – Mission Essential Infrastructure

[] Major Application – NOT Mission Essential Infrastructure

[] General Support System

Information System Security Categorization

[Low/Moderate/High]

Information System Operational Status

{Instructions: Brief summary of the status (IATO, ATO, No C&A, etc.) of all Subordinate systems identified in section 7 of this plan.}

Residual Risks & Mitigations

{Instructions: Brief summary of residual Master level risks and key subordinate risks with specific references to Subordinate plans.}

Subordinate Systems

{Instructions: Attach a list of all Subordinate systems to this Master security plan as described in Appendix A of the template.}

See List of Subordinate Systems in Appendix A

TABLE OF CONTENTS

MASTER PLAN APPROVAL DECISION LETTER	1
EXECUTIVE SUMMARY	2
IT Security Strategy	2
Information System Name /Title	2
Information System Type	2
Information System Security Categorization.....	2
Information System Operational Status	2
Residual Risks & Mitigations	2
Subordinate Systems	2
DOCUMENT REVISION LOG.....	3
TABLE OF CONTENTS.....	4
1.0 INFORMATION SYSTEM NAME/TITLE	6
2.0 INFORMATION SYSTEM CATEGORIZATION	6
2.1 Information Types.....	6
2.2 Security Categorization.....	6
3.0 INFORMATION SYSTEM OWNER	7
4.0 AUTHORIZING OFFICIAL	7
5.0 SUBORDINATE SYSTEM CONTACTS	7
6.0 ASSIGNMENT OF SECURITY RESPONSIBILITY	7
7.0 SUBORDINATE INFORMATION SYSTEM OPERATIONAL STATUS.....	8
8.0 INFORMATION SYSTEM TYPE	8
9.0 GENERAL DESCRIPTION/PURPOSE.....	8
9.1 Function	8
9.2 Capabilities	8
9.3 Conformance to NASA IT Security Strategy	8
10.0 SYSTEM ENVIRONMENT	8
10.1 Hardware.....	9
10.2 Software	9
10.3 Firmware.....	9
10.4 Network Configuration	9
10.5 Accreditation Boundary.....	9
11.0 SYSTEM INTERCONNECTIONS/INFORMATION SHARING	9
12.0 RELATED LAWS/REGULATIONS/POLICIES	9
13.0 MINIMUM SECURITY CONTROLS.....	11
13.1 SCOPE	11

13.1.1	Control Descriptions	11
13.1.2	Minimum Assurance Requirements.....	14
13.2	MANAGEMENT CONTROLS.....	15
13.2.1	Risk Assessment (RA).....	15
13.2.2	Planning (PL).....	17
13.2.3	System and Services Acquisition (SA).....	18
13.2.4	Certification, Accreditation, and Security Assessments (CA).....	19
13.3	OPERATIONAL CONTROLS	19
13.3.1	Personnel Security (PS)	19
13.3.2	Physical and Environmental Protection (PE).....	20
13.3.3	Contingency Planning (CP)	20
13.3.4	Configuration Management (CM)	21
13.3.5	Maintenance (MA).....	21
13.3.6	System and Information Integrity (SI).....	21
13.3.7	Media Protection (MP)	21
13.3.8	Incident Response (IR)	21
13.3.9	Awareness and Training (AT)	22
13.4	TECHNICAL CONTROLS.....	22
13.4.1	Identification and Authentication (IA).....	22
13.4.2	Access Control (AC).....	22
13.4.3	Audit and Accountability (AU)	22
13.4.4	System and Communications Protection (SC).....	22
13.5	NASA SPECIFIC CONTROLS	22
13.5.1	NASA National Security Criticality	22
14.0	PLAN COMPLETION	23
15.0	PLAN APPROVAL EFFECTIVE DATE	23
16.0	REVIEW OF SECURITY CONTROLS	23
APPENDIX A – LIST OF SUBORDINATE SYSTEMS		24

1.0 Information System Name/Title

System Name: [SYSTEM NAME]
 System Abbreviation: [SYSTEM ABBREVIATION]
 System Unique Identifier: [NASA SUI]

2.0 Information System Categorization

{Instructions: The information Master system categorization is determined by the combination of Information Types processed, handled or stored by Subordinate information system.}

2.1 Information Types

{Instructions: The following table identifies the combination of information types that are processed, handled or stored by all Subordinate information systems. The selection of the information types is based on procedure provided by ITS-SOP-0019 "Procedure for the FIPS 199 Categorization of Information Systems."}

NIST SP 800-60 Information Categories	Security Objectives & NIST Provisional Impact Level		
	Confidentiality	Integrity	Availability
NIST SP 800-60 Information Types			
[NIST 800-60 #] [NIST 800-60 Information Type Name]	Low/Moderate/High	Low/Moderate/High	Low/Moderate/High
{Example: C.2.6.2 Official Information Dissemination Information}	Low	Low	Low}
[Insert rows as needed]			
System High-Water Mark FIPS-199 Impact Level	{Example: Low	Example: Low	Example: Low}

Table: NIST 800-60 Volume II Information Types

Table: Information Type Processed by [SYSTEM ABBREVIATION]

2.2 Security Categorization

Based on the information provided in section 2.1, the security impact levels for each of the three security objectives of confidentiality, integrity, and availability are identified below.

Security Objective	Security Impact Level (L/M/H)
Confidentiality:	
Integrity:	
Availability:	

Table: Security Impact

Based on the information provided in the Security Impact table above, the required protection level for [SYSTEM ABBREVIATION] has been identified and is reflected in the following High Water Mark table. The high water mark represents the minimum level of security controls appropriate for [SYSTEM ABBREVIATION].

[SYSTEM ABBREVIATION] High Water Mark	[HIGH/MODERATE/LOW]
---------------------------------------	---------------------

Table: High Water Mark

3.0 Information System Owner

The following individual is designated as the Master security plan owner. This designated person is the key point of contact (POC) for this Master security plan and is responsible for coordinating system development life cycle (SDLC) activities specific to this Master plan and all Subordinate information systems. The plan owner also has expert knowledge of the Master and Subordinate system capabilities and functionality.

- Name:
- Title:
- Organization:
- Address:
- Phone:
- E-Mail:

4.0 Authorizing Official

The following individual is designated as the Authorizing Official. This designated person is the senior management official who has the authority to approve this Master plan and accept any residual risk(s) associated with this Master plan and Subordinate information systems.

- Name:
- Title:
- Organization:
- Address:
- Phone:
- E-Mail:

5.0 Subordinate System Contacts

See Appendix A – List of Subordinate Systems.

6.0 Assignment of Security Responsibility

The following individual has been assigned security responsibility for this Master plan. This assignment has been officially designated in writing.

{Instructions: if multiple individuals have been assigned the security responsibilities within a system, simply repeat the table below as needed and differentiate each person's security role.}

- Name:
- Title:
- Organization:
- Address:
- Phone:

E-Mail:

7.0 Subordinate Information System Operational Status

See Appendix A – List of Subordinate Systems

8.0 Information System Type

The information system is of the following type:

- Major Application – Mission Essential Infrastructure
- Major Application – NOT Mission Essential Infrastructure
- General Support System

9.0 General Description/Purpose

{Instructions: The [SYSTEM NAME] provides a means of data transport for users assigned to [AGENCY]. The [SYSTEM NAME] provides unclassified but sensitive network services including e-mail, web browsing, office automation, and connectivity for specialized computer applications.}

9.1 Function

{Instructions: Describe the general functionality of the Master system and reference specific Subordinate systems for details.}

9.2 Capabilities

{Instructions: Describe the general capabilities of the Master system and reference specific Subordinate systems for details.}

9.3 Conformance to NASA IT Security Strategy

{Instructions: Describe how the Master system conforms to the NASA IT Security Strategy.

- *High-level design schematic of the system*
- *Security characteristics of the system*
 - *Types of data*
 - *User communities*
 - *Interconnectivity*
 - *Data Flows*
- *Desired information management goals and objectives*

Describe what was done as the initiation phase of the information system in regards to IT Security.

Describe how the information system provides end-to-end IT Security.

Describe how the IT Security strategy for this information system captures each of the following choices:

- *Value of information*
- *Loss of information financial or otherwise}*

10.0 System Environment

The system environment is defined in Subordinate plan(s) where hardware, software and firmware exist.

See Appendix A – List of Subordinate Systems

10.1 Hardware

{Instructions: The Master Plan must cover the type of hardware used by all Subordinate systems. This is typically addressed by listing the Subordinate security plan that contains the detailed hardware listing. Master Plans, as a part of the Enterprise Architecture development and during the course of the evolution of Master Systems, may detail the common hardware deployments [typical in a “type accreditation” scenario or Agency-wide system deployment] for the Master System and required for support by all Subordinate systems.}

See Appendix A – List of Subordinate Systems

10.2 Software

{Instructions: The Master Plan must cover the type of software used by all Subordinate systems. This is typically addressed by listing the Subordinate security plan that contains the detailed software listing. Master Plans, as a part of the Enterprise Architecture development and during the course of the evolution of Master Systems, may detail the common software deployments [typical in a “type accreditation” scenario or Agency-wide system deployment] for the Master System and required for support by all Subordinate systems.}

See Appendix A – List of Subordinate Systems

10.3 Firmware

{Instructions: The Master Plan must cover the types of firmware used by all Subordinate systems. This is typically addressed by listing the Subordinate security plan that contains the detailed firmware listing. Master Plans, as a part of the Enterprise Architecture development and during the course of the evolution of Master Systems, may detail the common firmware deployments [typical in a “type accreditation” scenario or Agency-wide system deployment] for the Master System and required for support by all Subordinate systems.}

See Appendix A – List of Subordinate Systems

10.4 Network Configuration

{Instructions: Describe the set of minimum network connections, protocols, methods, etc. requirements and/or a specific network architecture that shall be implemented for all Subordinate systems}

10.5 Accreditation Boundary

Not applicable to Master security plans.

11.0 System Interconnections/Information Sharing

{Instructions: Identify any interconnections, information sharing or relevant requirements for all Subordinate systems under this Master Plan.}

12.0 Related Laws/Regulations/Policies

{Instructions: The following are laws, regulations and policies that affect the system.

- Computer Security Act of 1987 (40 USC 759) (PL 100-235), January 8, 1988
- Export Administration Regulations (EAR) (15 CFR Parts 730-774), April 24, 1996
- Freedom of Information Act (5 USC 552), Privacy Act of 1974 (5 USC 552a(e)(10)) (PL 93-579), December 31, 1974; October 2, 1997
- International Traffic in Arms Regulation (ITAR) (22 CFR Parts 120-130), April 1, 1992
- Trade Secrets Act (18 USC 1905)

- Office of Management and Budget Circular A-130, June 28, 1993
- NPR 2800.1, *Managing Information Technology*, September 17, 1998, Expires June 30, 2006
- NPR 2810.1A, *Security of Information Technology*, May 16, 2006, Expires May 16, 2011
- NPD 2820.1, *NASA Software Policies*, August 30, 2005, Expires August 30, 2010
- NASA HQ ITS Contingency Plan
- NPD 7120.5C, *NASA Program and Project Management Processes and Requirements*, March 22, 2005, Expires March 22, 2010
- Public Law 107-347, E-Government Act of 2002
- Title III of Public Law 107-347, E-Government Act of 2002, Federal Information Security Management Act (FISMA)
- 18 U.S.C. 1831-1839, The Economic Espionage Act of 1996
- 18 U.S.C. 2510, et seq., the Electronic Communications Privacy Act of 1986, as amended
- 22 U.S.C. 2751, et seq., the Arms Export Control Act, as implemented by the International Traffic in Arms Regulations, 22 CFR Parts 120-130
- 40 U.S.C. 1401, et seq., Section 808 of Public Law 104-208, the Clinger-Cohen Act of 1996 [renaming, in pertinent part, the Information Technology Management Reform Act (ITMRA), Division E of Public Law 104-106]
- 42 U.S.C. 2451, et seq., the National Aeronautics and Space Act of 1958, as amended
- 44 U.S.C. 3501, et seq., Paperwork Reduction Act of 1995, Public Law. 104-13, as amended, 1995
- 50 U.S.C. Appendix 2401-2420, the Export Administration Act of 1979, as amended, as implemented by the Export Administration Regulations, 15 CFR Parts 730-774
- OMB Circular No. A-130, Appendix III, Management of Federal Information Resources
- National Telecommunications and Information System Security (NTISS) 1, National Policy on Application of Communications Security to U.S. Civil and Commercial Space Systems, June 17, 1985
- NTISS 100, National Policy on Application of Communications Security to Command Destruct Systems, February 17, 1988
- Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization and Protection, December 17, 2003
- Health Insurance Portability and Accountability Act (HIPPA) of 1996
- NPR 1600.1, Security Program Procedural Requirements, Nov 8, 2005
- FIPS PUB 199, Standards for Security Categorization of Federal Information Systems, December 2003
- FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- NIST Special Publication 800-18 Revision 1, Guide for Developing Security Plans for Information Technology Systems, February 2006
- NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, July 2002
- NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, February 2005
- NIST Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004
- NIST Special Publication 800-34, Contingency Planning Guide for IT Systems, June 2002
- NIST Special Publication 800-37, Guide for the Security Certifications and Accreditation of Federal Information Systems, May 2004
- HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004

}

13.0 Minimum Security Controls

13.1 SCOPE

{Instructions: Per NPR 2810.1, NASA Master security plans are responsible for tailoring controls, detailed in FIPS 200 and NIST SP 800-53, appropriate for their Subordinate systems and in compliance with Federal and Agency control selections. Each Master system develops, tests, and details in the security plan, appropriate customizations and requirements that must be met by all Subordinate systems under its purview. The Authorizing Official (AO) and/or Master security plan owner shall tailor security controls as much as possible for each Master security plan.

In addition to Master controls, NASA has designated and tailored some 800-53 controls as Agency controls. These Agency controls are issued at least annually by the NASA Office of the CIO and must be included in each Master plan and Subordinate plan. ITSR2D2 automatically incorporates the current version of Agency controls into a Master security plan template when a Master C&A package is created.}

Sections 13.2, 13.3, and 13.4 contain the management, operational, and technical controls that have been selected and/or tailored for the [SYSTEM NAME]. The controls were taken from NIST SP 800-53 and are based on the system's security categorization per FIPS 199. All Subordinates to this security plan inherit all controls described in sections 13.2, 13.3, and 13.4, which include Agency controls and Master controls.

13.1.1 Control Descriptions

{Instructions: The tailoring guidance in NIST SP 800-53 strongly recommends specific controls for tailoring and others which should not be tailored. Master security plan authors shall take the NIST SP 800-53 recommendations into account and may define additional tailoring or tailoring requirements for their Subordinate systems. Additional tailoring guidance for Master security controls is given in ITS-SOP-0011.}

Each control section details how this Master security plan has tailored the control for all Subordinates of this plan and how the control is being implemented or shall be implemented. The following template is used for each of the controls described in [annex 1/ annex 2/annex 3] of NIST SP 800-53.

[Control #] [Control Name]

This control is:

Agency Defined (see Control, Control Enhancement or NASA Control Enhancement)

Implemented and Verified by the Agency - no system owner action required (see Implementation Detail)

Selected for Annual Review by Agency

Master Plan Defined (see Control, Control Enhancement or NASA Control Enhancement)

Implemented and Verified by the Master system - no Subordinate system owner action required (see Implementation Detail)

Selected for Annual Review by Master Plan

Site Plan Defined

Implemented and Verified by the Site plan - no system owner action required (see Implementation Detail)

Selected for Annual Review by Site Plan

- Implemented and Verified by Subordinate System Owner (see Implementation Detail)**
 Selected for Annual Review by System Owner

- Not Applicable to this System (see Implementation Detail for justification)**
 Not Accepted (see Implementation Detail for justification)

Control:

Supplemental Guidance:

NASA Control Enhancement:

Implementation Detail:

{Instructions: For each control to be tailored by this Master plan, use the entire control template and fill out the appropriate sections. Master plans created in ITSR2D2 will already have the Agency controls filled in. Master plans created manually must incorporate the current version of the Agency controls, as issued by the NASA Office of the CIO.}

[Control #] [Control Name]

{Instructions: Use the baseline control requirements from NIST SP 800-53, annex 1, 2 or 3, as appropriate for the system's FIPS 199 security category.}

This control is:

Agency Defined (see Control, Control Enhancement or NASA Control Enhancement)

{Instructions: This indicates that this control is tailored at the Agency level and all systems, Master and Subordinate, must meet the requirements if the control is accepted. If a control is "Agency Defined," the Master plan may not uncheck this box. An example of this is AC-08, where the required system use notification is the warning banner defined in NPR 2810.1.}

Implemented and Verified by the Agency - no system owner action required (see Implementation Detail)

{Instructions: This indicates that the control is implemented at the Agency and has been verified as meeting the NIST SP 800-53 requirements. by the Agency. No tailoring is necessary by Master security plans, and no additional implementation detail is required. An example of this is RA-1, which is met by sections of NPR 2810.1.}

Selected for Annual Review by Agency

{Instructions: This indicates that the control will be reviewed annually during the continuous monitoring between C&As. This review can be part of the annual self-assessment by the system owner and shall include verifying that the control is still applicable, reasonable, effective and functioning as intended.}

Master Plan Defined (see Control, Control Enhancement or NASA Control Enhancement)

{Instructions: This indicates that this control is tailored by the Master plan and the requirements must be met by all Subordinate systems under the Master's purview. The Master plan should provide details of the tailoring in the Control, Control Enhancement or NASA Control Enhancement section. An example of this would be a collaboration security mechanism control mandated for all Messaging and Collaborations systems.}

Implemented and Verified by the Master system - no Subordinate system owner action required (see Implementation Detail)

{Instructions: This indicates that the control is implemented by the Master plan and has been verified as meeting the NIST SP 800-53 requirements. An example of this would be CA-03, if a Master plan were to

establish interconnection agreements with all other systems that its Subordinates could connect to (e.g. the Master OAIT WAN plan could establish interconnection agreement(s) with OAIT LANs).}

[] Selected for Annual Review by Master Plan

{Instructions: This indicates that the control will be reviewed annually during the continuous monitoring between C&As. This review can be part of the annual self-assessment by the system owner and shall include verifying that the control is still applicable, reasonable, effective and functioning as intended.}

[] Site Plan Defined

{Instructions: This indicates that this control is tailored by the Site plan. Processes and procedures are currently being established.}

[] Implemented and Verified by the Site plan - no system owner action required (see Implementation Detail)

{Instructions: This indicates that the control is implemented by the Site plan and has been verified as meeting the NIST 800-53 requirements. Processes and procedures are currently being established.}

[] Selected for Annual Review by Site Plan

{Instructions: This indicates that the control will be reviewed annually during the continuous monitoring between C&As. This review can be part of the annual self-assessment by the system owner and shall include verifying that the control is still applicable, reasonable, effective and functioning as intended.}

[] Implemented and Verified by Subordinate System Owner (see Implementation Detail)

{Instructions: This indicates that the control is implemented by the Subordinate system and the implementation is described in the Implementation Detail.}

[] Selected for Annual Review by System Owner

{Instructions: This indicates that the control will be reviewed annually during the continuous monitoring between C&As. This review can be part of the annual self-assessment by the system owner and shall include verifying that the control is still applicable, reasonable, effective and functioning as intended.}

[] Not Applicable to this System (see Implementation Detail for justification)

{Instructions: This indicates that the control is deemed “not applicable” to the plan, Master or Subordinate. Justification must be provided in the Implementation Detail section and approved by the Master system’s AO.}

[] Not Accepted (see Implementation Detail for justification)

{Instructions: This indicates that the control is not implemented on the system, for example due to cost constraints or because it is not necessary to adequately protect the system. Justification must be provided in the Implementation Detail section and approved by the system’s AO. An example would be CP-07 for a system with a confidentiality impact level of High (giving the whole system a FIPS 199 security category of High) and an availability impact level of Low.}

Control:

{Instructions: Insert the control description from NIST SP 800-53. If the NIST 800-53 control has “organization defined parameters,” such parameters should be defined by Agency, Master, or Site and specified in the Control section.}

Supplemental Guidance:

{Instructions: if applicable, description from NIST SP 800-53}

NASA Control Enhancement:

{Instructions: Describe any NASA-specific control tailoring or enhancements by Agency, Master or Site. Additional tailoring guidance is given in ITS-SOP-0011 for Master controls.}

Implementation Detail:

{Instructions: description of implementation by Agency, Master, Site or Subordinate; OR reference to POA&M for actions to be completed; OR justification for Not Applicable; OR justification for Not Accepted}
}

13.1.2 Minimum Assurance Requirements

In accordance with SP 800-53, Appendix E, the minimum assurance requirements specified in this section are intended to increase the level of confidence that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. The assurance requirements are applied on a control-by-control basis. The developer/implementer of each control is expected to perform all required design, development, implementation, and component/integration testing of the controls and to produce associated design and implementation documentation.

{Instructions: Select the appropriate baseline statements from NIST 800-53 based on the security categorization of the Master security plan for inclusion in Section 13.1.2 in the plan. Ensure that the appropriate baseline requirements are met for each control specified in this Master security plan.

The Low Baseline Assurance Requirement states:

“The security control is in effect and meets explicitly identified functional requirements in the control statement.

Supplemental Guidance: For security controls in the low baseline, the focus is on the control being in place with the expectation that no obvious errors exist and that, as flaws are discovered, they are addressed in a timely manner.”

The Moderate Baseline Assurance Requirement states:

“The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties of the control with sufficient detail to permit analysis and testing of the control.

The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions to ensure that when the control is implemented, it will meet its required function or purpose. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.

Supplemental Guidance: For security controls in the moderate baseline, the focus is on ensuring correct implementation and operation of the control. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer/implementer incorporates, as part of the control, specific capabilities and produces specific documentation to ensure the control meets its required function or purpose..”

The High Baseline Assurance Requirement states:

"The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties and design/implementation of the control with sufficient detail to permit analysis and testing of the control (including functional interfaces among control components).

The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions to ensure that when the control is implemented, it will continuously and consistently (i.e., across the information system) meet its required function or purpose and support improvement in the

effectiveness of the control. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.

Supplemental Guidance: For security controls in the high baseline, the focus is expanded to require, within the control, the capabilities that are needed to support ongoing consistent operation of the control and continuous improvement in the control's effectiveness. The developer/implementer is expected to expend significant effort on the design, development, implementation, and component/integration testing of the controls and to produce associated design and implementation documentation to support these activities. For security controls in the high baseline, this same documentation is needed by assessors to analyze and test the internal components of the control as part of the overall assessment of the control."

Additional Requirements for Enhancing the Moderate and High Baselines:

"The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties and design/implementation of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, actions to ensure that when the control is implemented, it will continuously and consistently (i.e., across the information system) meet its required function or purpose and support improvement in the effectiveness of the control. These actions include requiring the development of records with structure and content suitable to facilitate making this determination. The control is developed in a manner that supports a high degree of confidence that the control is complete, consistent, and correct.

Supplemental Guidance: The additional high assurance requirements are intended to supplement the minimum assurance requirements for the moderate and high baselines, when appropriate, in order to protect against threats from highly skilled, highly motivated, and well-financed threat agents. This level of protection is required for those information systems where the organization is not willing to accept the risks associated with the type of threat agents cited above."

(from NIST Special Publication 800-53, pgs. 43-44) }

13.2 MANAGEMENT CONTROLS

The Management security controls section of this security plan identifies the management safeguards and countermeasures in-place or planned for [SYSTEM NAME]. Management Controls are those safeguards and countermeasures that focus on the management of risk and the management of the information security system. They are actions that are performed primarily to support information system security management decisions.

13.2.1 Risk Assessment (RA)

Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

(FIPS 200, Section 3, Minimum Security Requirements)

{Instructions: Example of an Agency control. No change or action by the Master plan owner or Subordinate system owners is required.}

RA-1 Risk Assessment Policy and Procedures

This control is:

Agency Defined (see Control, Control Enhancement or NASA Control Enhancement)

Implemented and Verified by the Agency - no system owner action required (see Implementation Detail)

Selected for Annual Review by Agency

Master Plan Defined (see Control, Control Enhancement or NASA Control Enhancement)

Implemented and Verified by the Master system - no Subordinate system owner action required (see Implementation Detail)

Selected for Annual Review by Master Plan

Site Plan Defined

Implemented and Verified by the Site plan - no system owner action required (see Implementation Detail)

Selected for Annual Review by Site Plan

Implemented and Verified by Subordinate System Owner (see Implementation Detail)

Selected for Annual Review by System Owner

Not Applicable to this System (see Implementation Detail for justification)

Not Accepted (see Implementation Detail for justification)

Control:

The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

Supplemental Guidance:

None

NASA Control Enhancement:

None

Implementation Detail:

Item (i) Control satisfied via NPR 2810.1, Section 12.2 - Risk Management Process Requirements. Item (ii) Control satisfied via NASA ITS-SOP-0005B.

}

{Instructions: Example of a control defined in the Master plan.

RA-2 Security Categorization

This control is:

Agency Defined (see Control, Control Enhancement or NASA Control Enhancement)

Implemented and Verified by the Agency - no system owner action required (see Implementation Detail)

Selected for Annual Review by Agency

Master Plan Defined (see Control, Control Enhancement or NASA Control Enhancement)

Implemented and Verified by the Master system - no Subordinate system owner action required (see Implementation Detail)

Selected for Annual Review by Master Plan

- Site Plan Defined**
- Implemented and Verified by the Site plan - no system owner action required (see Implementation Detail)**
 - Selected for Annual Review by Site Plan**
- Implemented and Verified by Subordinate System Owner (see Implementation Detail)**
 - Selected for Annual Review by System Owner**
- Not Applicable to this System (see Implementation Detail for justification)**
- Not Accepted (see Implementation Detail for justification)**

Control:

The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199 and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.

Supplemental Guidance:

None

NASA Control Enhancement:

NASA ITS-SOP-0019 shall be utilized to for all information system security categorizations.

Implementation Detail:

}

13.2.2 Planning (PL)

Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems. (*FIPS 200, Section 3, Minimum Security Requirements*)

{Instructions: In this example, the Agency has defined a parameter (every three (3) years) in the Control and the Agency has developed a NASA Control Enhancement that requires the Master system and Subordinate system to comply with a specific NASA policy to gain accreditation. All Master security plans must include such controls within the development of the plan. The current Agency Control list will be updated in ITS-SOP-0016 on an annual basis or as major changes mandate a release update.

PL-3 System Security Plan Update

This control is:

- Agency Defined (see Control, Control Enhancement or NASA Control Enhancement)**
- Implemented and Verified by the Agency - no system owner action required (see Implementation Detail)**
 - Selected for Annual Review by Agency**
- Master Plan Defined (see Control, Control Enhancement or NASA Control Enhancement)**
- Implemented and Verified by the Master system - no Subordinate system owner action required (see Implementation Detail)**
 - Selected for Annual Review by Master Plan**

- Site Plan Defined**
- Implemented and Verified by the Site plan - no system owner action required (see Implementation Detail)**
 - Selected for Annual Review by Site Plan**

- Implemented and Verified by Subordinate System Owner (see Implementation Detail)**
 - Selected for Annual Review by System Owner**

- Not Applicable to this System (see Implementation Detail for justification)**
- Not Accepted (see Implementation Detail for justification)**

Control:

The organization reviews the security plan for the information system every three (3) years and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.

Supplemental Guidance:

None

NASA Control Enhancement:

Changes in the information system s categorization level and security control assessment results can result in annual review cycles for SSP's.

Implementation Detail:

}

13.2.3 System and Services Acquisition (SA)

Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

(FIPS 200, Section 3, Minimum Security Requirements)

{Instructions: In this example, a Master system has developed a NASA Control Enhancement that requires the Subordinate system to comply with a specific NASA policy to gain accreditation.

SA-7 User-Installed Software

This control is:

- Agency Defined (see Control, Control Enhancement or NASA Control Enhancement)**
- Implemented and Verified by the Agency - no system owner action required (see Implementation Detail)**
 - Selected for Annual Review by Agency**
- Master Plan Defined (see Control, Control Enhancement or NASA Control Enhancement)**
- Implemented and Verified by the Master system - no Subordinate system owner action required (see Implementation Detail)**
 - Selected for Annual Review by Master Plan**

- Site Plan Defined**
- Implemented and Verified by the Site plan - no system owner action required (see Implementation Detail)**
 - Selected for Annual Review by Site Plan**
- Implemented and Verified by Subordinate System Owner (see Implementation Detail)**
 - Selected for Annual Review by System Owner**
- Not Applicable to this System (see Implementation Detail for justification)**
- Not Accepted (see Implementation Detail for justification)**

Control:

The organization enforces explicit rules governing the downloading and installation of software by users.

Supplemental Guidance:

None

NASA Control Enhancement:

The System Owner shall maintain and disseminate (annually or when changes occur) a list of authorized software for the information system(s).

Components within the information system shall be reviewed annually for User Installed Software.

Any user installed software on the information system must comply with NASA policies including NPD 2540.1F.

Implementation Detail:

}

13.2.4 Certification, Accreditation, and Security Assessments (CA)

Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

(FIPS 200, Section 3, Minimum Security Requirements)

13.3 OPERATIONAL CONTROLS

The Operational security controls section of this security plan identifies the operational safeguards and countermeasures in-place or planned for [SYSTEM NAME]. Operational Controls are those safeguards and countermeasures that are primarily implemented and executed by people as opposed to systems and technology.

13.3.1 Personnel Security (PS)

Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

(FIPS 200, Section 3, Minimum Security Requirements)

13.3.2 Physical and Environmental Protection (PE)

Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

(FIPS 200, Section 3, Minimum Security Requirements)

13.3.3 Contingency Planning (CP)

Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

(FIPS 200, Section 3, Minimum Security Requirements)

{Instructions: In this example, a Master plan has defined a time period for the resumption of operations if the primary processing capabilities are unavailable.}

CP-7 Alternate Processing Sites

This control is:

Agency Defined (see Control, Control Enhancement or NASA Control Enhancement)

Implemented and Verified by the Agency - no system owner action required (see Implementation Detail)

Selected for Annual Review by Agency

Master Plan Defined (see Control, Control Enhancement or NASA Control Enhancement)

Implemented and Verified by the Master system - no Subordinate system owner action required (see Implementation Detail)

Selected for Annual Review by Master Plan

Site Plan Defined

Implemented and Verified by the Site plan - no system owner action required (see Implementation Detail)

Selected for Annual Review by Site Plan

Implemented and Verified by Subordinate System Owner (see Implementation Detail)

Selected for Annual Review by System Owner

Not Applicable to this System (see Implementation Detail for justification)

Not Accepted (see Implementation Detail for justification)

Control:

The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [12 hours] when the primary processing capabilities are unavailable.

The alternate processing site is geographically separated from the primary processing site so as not to be

susceptible to the same hazards.

The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Alternate processing site agreements contain priority-of-service provisions in accordance with the organization's availability requirements.

The alternate processing site is fully configured to support a minimum required operational capability and ready to use as the operational site.

Supplemental Guidance:

Equipment and supplies required to resume operations within the organization-defined time period are either available at the alternate site or contracts are in place to support delivery to the site.

NASA Control Enhancement:

None

Implementation Detail:

}

13.3.4 Configuration Management (CM)

Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

(FIPS 200, Section 3, Minimum Security Requirements)

13.3.5 Maintenance (MA)

Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

(FIPS 200, Section 3, Minimum Security Requirements)

13.3.6 System and Information Integrity (SI)

Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

(FIPS 200, Section 3, Minimum Security Requirements)

13.3.7 Media Protection (MP)

Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

(FIPS 200, Section 3, Minimum Security Requirements)

13.3.8 Incident Response (IR)

Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and

user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

(FIPS 200, Section 3, Minimum Security Requirements)

13.3.9 Awareness and Training (AT)

Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

(FIPS 200, Section 3, Minimum Security Requirements)

13.4 TECHNICAL CONTROLS

The Technical security controls section of this security plan identifies the technical safeguards and countermeasures in-place or planned for [SYSTEM NAME]. Technical Controls are those safeguards and countermeasures that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

13.4.1 Identification and Authentication (IA)

Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(FIPS 200, Section 3, Minimum Security Requirements)

13.4.2 Access Control (AC)

Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

(FIPS 200, Section 3, Minimum Security Requirements)

13.4.3 Audit and Accountability (AU)

Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

(FIPS 200, Section 3, Minimum Security Requirements)

13.4.4 System and Communications Protection (SC)

Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

(FIPS 200, Section 3, Minimum Security Requirements)

13.5 NASA SPECIFIC CONTROLS

13.5.1 NASA National Security Criticality

14.0 Plan Completion

This version of the [SYSTEM NAME] Master security plan was completed on _____.

15.0 Plan Approval Effective Date

The Authorizing Official's approval at the front of this Master security plan puts this plan into effect from the date of signature.

16.0 Review of Security Controls

The security controls of the [SYSTEM NAME] were reviewed on _____.

Appendix A – List of Subordinate Systems

{*Instructions: List all Subordinate systems to this Master security plan. Note that this section is not included in the Subordinate SSP template in ITS-SOP-0016 and must be added for Master security plans.*}

Subordinate System Name	System Unique Identifier	System Owner	Authorizing Official	Status of ATO/IAOT/Other	Certification Official
System X	OA-xxx-M-xxx-xxxx	Name Title Organization Address Phone E-Mail	Name	ATO dated xx/xx/xxxx, NIST-compliant documentation, native in ITS-R2D2	Name