



National Aeronautics and  
Space Administration

**John C. Stennis Space Center**  
Stennis Space Center, MS  
39529-6000

**SPR 8739.1 Rev B-1**  
**April 2012**

## **COMPLIANCE IS MANDATORY**

### **John C. Stennis Space Center (SSC) Software Assurance Procedural Requirements**

Stennis Procedural Requirements	SPR 8739.1	B-1
	<i>Number</i>	<i>Rev.</i>
	Effective Date: April 1, 2012	
	Expiration Date: April 1, 2017	
Responsible Office: Office of Safety and Mission Assurance		
<b>SUBJECT: Software Assurance Procedural Requirements</b>		

## Document History Log

Status/Change/ Revision	Change Date	Originator/Phone	Description
Basic	11/02/2007	Charles Fallo/8-2553	Initial Release
Rev A	06/09/2010	Charles Fallo/8-2553	Updated Center Director signature block. Added section 2.9.h
Rev B	12/27/2011	Rae Lyn Anderson/8-1945	Updated sections P.1-P.4, 1.1 and all subsections, 1.2 and all subsections, 2.1-2.7. 2.9, 2.11, 2.13 and 2.15. Added sections 2.8. 2.10. 2.12. 2.14. Removed section 1.2.6 Contractor SMA. Changes made to address audit findings.
Rev B-1	6/13/2012	Rae Lyn Anderson/8-1945	Administration changes.

Stennis Procedural Requirements	SPR 8739.1	B-1
	<i>Number</i>	<i>Rev.</i>
	Effective Date: April 1, 2012	
	Expiration Date: April 1, 2017	
Responsible Office: Office of Safety and Mission Assurance		
<b>SUBJECT: Software Assurance Procedural Requirements</b>		

## Table of Contents

<b>PREFACE</b> .....	<b>5</b>
<b>P.1 PURPOSE</b> .....	<b>5</b>
<b>P.2 APPLICABILITY and SCOPE</b> .....	<b>5</b>
<b>P.3 AUTHORITY</b> .....	<b>6</b>
<b>P.4 APPLICABLE DOCUMENTS</b> .....	<b>7</b>
<b>P.5 MEASUREMENT AND VERIFICATION</b> .....	<b>7</b>
<b>P.6 CANCELLATION</b> .....	<b>7</b>
<b>CHAPTER 1 ORGANIZATION</b> .....	<b>8</b>
1.1 Organizational Structure .....	8
1.2 Roles and Responsibilities .....	9
1.2.1 Project Management .....	9
1.2.2 Safety and Mission Assurance (SMA) Manager .....	9
1.2.3 Software Assurance Manager .....	10
1.2.4 Project SMA Representatives .....	10
1.2.5 System Hazard Engineer/System Safety Engineer .....	10
1.2.6 Software Acquirer .....	11
1.2.7 Software Provider .....	11
1.2.8 SSC Independent Verification and Validation (IV&V) Liaison.....	11
<b>CHAPTER 2 SOFTWARE ASSURANCE PROCESS</b> .....	<b>12</b>
2.1 Definition .....	12
2.2 Implementation .....	12
2.3 Training.....	12
2.4 NASA SSC Software Life Cycle Management Requirement.....	13
2.5 Tailoring, Deviations, and Waivers .....	13
2.6 Functional SA Role Assignment and Resources .....	14
2.7 Software Assurance Classification Assessment.....	14
2.8 Software Quality Assurance .....	14
2.9 Software Safety Criticality.....	15
2.10 Software Reliability .....	15
2.11 Software Assurance Plan .....	16
2.12 Software Assurance Metrics .....	16
2.13 Software Assurance Task Review Process .....	17
2.14 Software Assurance Acquirer and Provider.....	17
2.15 Software Assurance Task-Developed Products/Documents.....	17
<b>APPENDIX A – Abbreviations and Acronyms</b> .....	<b>18</b>

Stennis Procedural Requirements	SPR 8739.1	B-1
	<i>Number</i>	<i>Rev.</i>
	Effective Date: April 1, 2012	
	Expiration Date: April 1, 2017	
		Page 4 of 18
Responsible Office: Office of Safety and Mission Assurance		
<b>SUBJECT: Software Assurance Procedural Requirements</b>		

**FIGURES**

**Figure 1 Organizational Chart for Management of Software Assurance Reporting  
Activities..... 8**

**Figure 2 Governing Lines of Authority for Resolving NASA SSC SA Issues ..... 8**

Stennis Procedural Requirements	SPR 8739.1	B-1
	<i>Number</i>	<i>Rev.</i>
	Effective Date: April 1, 2012	
	Expiration Date: April 1, 2017	
Page 5 of 18		
Responsible Office: Office of Safety and Mission Assurance		
<b>SUBJECT: Software Assurance Procedural Requirements</b>		

## PREFACE

The Software Assurance (SA) procedural requirements cover the entire software life cycle for both the acquirer and provider ultimately to provide safe, quality, and cost effective software products and systems.

### P.1 PURPOSE

a. This Stennis Procedural Requirement (SPR) specifies SA requirements for National Aeronautics and Space Administration (NASA) Stennis Space Center (SSC) projects, programs, facilities, and activities. NASA SSC is a unique facility that consists of several full scale rocket engine/motor test facilities, component and small engine test facilities to support engine test programs such as the NASA lead, commercial focused, private venture, and engine testing for NASA's next generation of rockets for Lunar and Mars exploration. The primary purpose of this SPR is to support the office responsible for overseeing the safe operation of these unique national test facilities.

b. This SPR establishes the procedures necessary to comply with the SA requirements for software developed and/or acquired by NASA SSC, including open source, Government off-the-Shelf (GOTS) software, Modified off-the-Shelf (MOTS) software, and Commercial off-the-Shelf (COTS) software, when included in a NASA system. It is intended to provide a common SA framework across the Center and establishes consistency from project to project and test facility to test facility. It also describes procedures and processes for analyzing and applying the appropriate software assurance techniques and methods to software throughout its lifecycle. The primary audience for this SPR is Project Managers, Project Safety and Mission Assurance (SMA) Representatives, SA Managers and Engineers, and Software Engineers.

### P.2 APPLICABILITY and SCOPE

a. This SPR supports the implementation of NASA Policy for software as defined in the NASA Policy Directive (NPD) 7120.4, NASA Engineering and Program/Project Management Policy. NPD 7120.4 is an overarching document that establishes policies for all software created, acquired, and maintained by or for NASA. The NASA SSC SMA Manager is the technical authority for this SPR in accordance with SPLN-1200-0003 SSC SMA Technical Authority Implementation Plan and ensures compliance with NASA SMA related policies.

b. This SSC Procedural Requirement is applicable to all NASA SSC personnel, NASA SSC contractors and subcontractors. It is applicable to all software and firmware including GOTS, MOTS, and COTS when included in a NASA SSC system. Applicable NASA SSC systems include, but are not necessarily limited to, facilities and projects including the Test Complex Facility, Hazardous Gas Detection & Warning System, High Pressure Gas Facility, High Pressure Industrial Water Plant, Applied Science Projects, Test Complex Management Systems, Design and Data Management System (DDMS), and Master Work Control, test beds, ground

Stennis Procedural Requirements	SPR 8739.1	B-1
	<i>Number</i>	<i>Rev.</i>
	Effective Date: April 1, 2012	
	Expiration Date: April 1, 2017	
Page 6 of 18		
Responsible Office: Office of Safety and Mission Assurance		
<b>SUBJECT: Software Assurance Procedural Requirements</b>		

support systems, other facility systems, and software projects that support or perform NASA specific missions.

c. The SA requirements in this SPR flow down from NPD 7120.4 through NASA Procedural Requirements (NPRs) and NASA Standards (STDs):

- NPR 7150.2, Software Engineering which establishes a set of software engineering requirements to be applied throughout NASA;
- NPR 2210.1, Release of NASA Software which establishes procedures and responsibilities for the reporting, review, assessments, and release of software created by NASA;
- NASA-STD-8739.8, Software Assurance Standard that describes the processes and procedures for analyzing and applying appropriate software assurance techniques and methods to software; and
- NASA-STD-8719.13, Software Safety Standard that describes the activities necessary to ensure that safety is designed into the software that is acquired or developed by NASA.

d. The focus of this SPR is SA Classifications A-H as applicable. SA Classifications as provided in NPR 7150.2 are:

Class A - Human Rated Space Software Systems

Class B - Non-Human Space Rated Software Systems or Large Scale Aeronautics Vehicles

Class C - Mission Support Software or Aeronautic Vehicles, or Major Engineering/Research Facility Software

Class D - Basic Science/Engineering Design and Research and Technology Software

Class E - Small Light Weight Design Concept and Research and Technology Software

Class F - General Purpose Computing Software (Multi-Center or Multi-Program/Project)

Class G - General Purpose Computing Software (Single-Center or Project)

Class H - General Purpose Desktop Software

According to NASA-STD-8739.8, Software Assurance requirements for Classes F, G, and H are designated by the Chief Information Officer (CIO). As such at this time, SA is only performed on these classes upon request or as designated by the CIO.

d. SA consists of five software assurance disciplines; Quality, Safety, Reliability, Verification and Validation (V&V) and Independent Verification and Validation (IV&V) as defined in NASA-STD-8739.8. The results of the SA Classification Assessment for each NASA SSC project will assist in determining the scope of the SA effort including the level of effort for each discipline.

e. In the event of a conflict between a NPD, NPR, or a STD with this SPR, the information provided in the NPD, NPR, or STD takes precedence.

### P.3 AUTHORITY

NPD 7120.4, NASA Engineering and Program/Project Management Policy

Stennis Procedural Requirements	SPR 8739.1	B-1
	<i>Number</i>	<i>Rev.</i>
	Effective Date: April 1, 2012	
	Expiration Date: April 1, 2017	
Page 7 of 18		
Responsible Office: Office of Safety and Mission Assurance		
<b>SUBJECT: Software Assurance Procedural Requirements</b>		

#### P.4 APPLICABLE DOCUMENTS

All references are assumed to be the latest version unless otherwise specified.

- a. NPD 7120.4, NASA Engineering and Program/Project Management Policy
- b. NPR 1441.1, NASA Records Retention Schedules
- c. NPR 2210.1 Release of NASA Software
- d. NPR 7120.5, NASA Space Flight Program and Project Management Requirements
- e. NPR 7150.2, NASA Software Engineering Requirements
- f. NPR 8715.3, NASA General Safety Program Requirements
- g. NASA-STD-8719.13, Software Safety Standard
- h. NASA-STD-8739.8, Software Assurance Standard
- i. SBCC-1150-0013, Risk Review Panel (RRP) Charter
- j. SPLN-1200-0003, SSC SMA Technical Authority Implementation Plan
- k. SPR 1440.1, Records Management Program Requirements
- l. SSTD-8070-0007-CONFIG, Variance and Alternate Standard Requests
- m. SOI-8080-0008, Documentation and Configuration Control of Test Complex Software
- n. SOI-8080-0052, Software Life Cycle and Development Process
- o. SPLN 3410-0004, Personnel Training Plan for Safety and Mission Assurance
- p. SCWI-3410-0002, Training and Development Plan
- q. SSP-8715-0001, SSC Safety and Health Handbook
- r. SCWI-8710-0001, System Safety and Health
- s. SWI-2800-0004, Management of SDC Application Development Projects

#### P.5 MEASUREMENT AND VERIFICATION

Compliance with this procedure will be monitored through the SSC Management System (SMS) and Office of Safety and Mission Assurance by objective evidence, such as Training records, Functional SMA Organization Chart, SA Role Assignment provided, Annual Operating Agreement (AOA), SMA Work Instructions generated, and SA Task Developed Products/Documents (reference Section 2.11).

#### P.6 CANCELLATION

SPR\_8739.1 Rev A.

*Signature on file*

Patrick E. Scheuermann  
Director

#### DISTRIBUTION

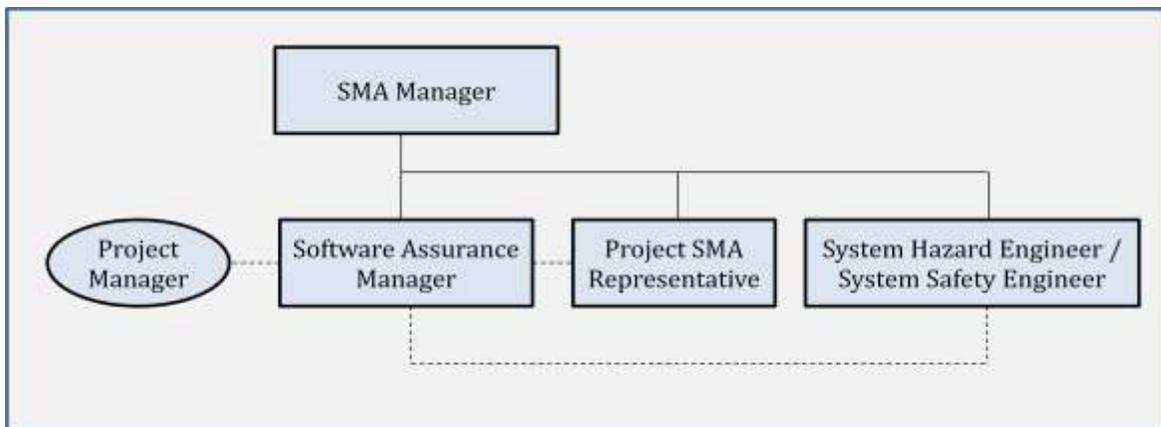
Approved for public release via NASA Online Directives Information System (NODIS); distribution is unlimited.

Stennis Procedural Requirements	SPR 8739.1	B-1
	<i>Number</i>	<i>Rev.</i>
	Effective Date: April 1, 2012	
	Expiration Date: April 1, 2017	
Responsible Office: Office of Safety and Mission Assurance		
<b>SUBJECT: Software Assurance Procedural Requirements</b>		

## CHAPTER 1 ORGANIZATION

### 1.1 Organizational Structure

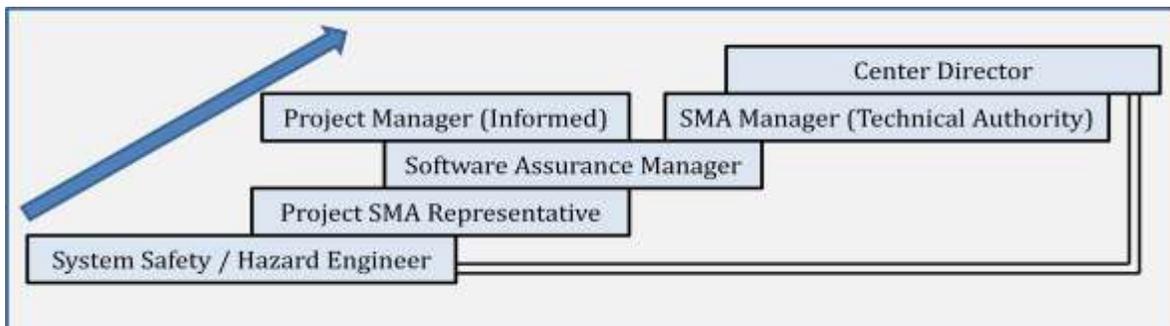
Successful compliance and management of all NASA SSC SA activities requires the involvement of various groups at many levels of the project and NASA SSC organization. Figure 1 provides a diagram that shows how the various NASA SSC personnel coordinate roles to assure SA reporting activities are implemented to comply with the SA and Software Safety (SS) standards.



**Figure 1 Organizational Chart for Management of Software Assurance Reporting Activities**

To assure that all unresolved SA issues are elevated to the appropriate governing authority, as provided in NPR 7150.2,

Figure 2 depicts the “directional steps” for the governing lines of authority for resolving SSC SA issues.



**Figure 2 Governing Lines of Authority for Resolving NASA SSC SA Issues**

Stennis Procedural Requirements	SPR 8739.1	B-1
	<i>Number</i>	<i>Rev.</i>
	Effective Date: April 1, 2012	
	Expiration Date: April 1, 2017	
Responsible Office: Office of Safety and Mission Assurance		
<b>SUBJECT: Software Assurance Procedural Requirements</b>		

## 1.2 Roles and Responsibilities

- a. This section of the SPR identifies and describes the SA roles and responsibilities of the various NASA SSC personnel. For clarification the terms *assuring* and *ensuring* have the following usage:
  - Assuring is used when SA practitioners make certain that the specified SA activities have been performed by others.
  - Ensuring is used when SA practitioners themselves perform the specified SA activities.

### 1.2.1 Project Management

- a. Project Management is responsible for making sure the appropriate criteria is in place to assure compliance with the NPD 7120.4, NPR 7150.2, NPR 2210.1 and this SPR. Additionally Project Management is responsible for ensuring the Project SMA Representatives perform SA functions with support from the software developing organization(s) according to this SPR throughout the project lifecycle relative to software classification level. Lastly, Project Management assures and enables (through appropriate project authority and funding) SA cohesiveness of and compliance with Stennis processes, e.g., SBCC-1150-0013 Risk Review Panel (RRP) Charter, SPLN-7120-0004 Project Directorate Risk Management Implementation Plan, SOI-8080-0008 Documentation and Configuration Control of Test Complex Software, SOI-8080-0052 Software Life Cycle and Development Process and SWI-2800-0004 Management of SDC Application Development Projects.
- b. Project Management shall appropriately fund the effort to develop the Preliminary Hazard Analysis (PHA), Hazard Analysis (HA), and/or System Hazard Analysis (SHA) as defined in SCWI-8710-0001, including the funding of Software Engineering personnel to provide expertise to the System Hazard Engineer/System Safety Engineer during the development of these artifacts.

### 1.2.2 Safety and Mission Assurance (SMA) Manager

- a. SMA Manager is responsible for ensuring compliance with the NPD 7120.4, NASA Engineering and Program/Project Management Policy (NASA Software Policy), NPR 7150.2, NASA Software Engineering Requirements, NPR 2210.1, Release of NASA Software and this SPR, at NASA SSC on all the software related projects. The SMA Manager is responsible for ensuring that SA project Staff, including both the acquirer and provider, are performing the tasks according to the NASA-STD-8739.8, NASA-STD-8719.13, SA plan and the contract. Additionally, the SMA Manager will identify trained SA Managers and provide the appropriate resources that will ensure project compliance with NASA SA Policy.

Stennis Procedural Requirements	SPR 8739.1	B-1
	<i>Number</i>	<i>Rev.</i>
	Effective Date: April 1, 2012	
	Expiration Date: April 1, 2017	
Responsible Office: Office of Safety and Mission Assurance		
<b>SUBJECT: Software Assurance Procedural Requirements</b>		

### 1.2.3 Software Assurance Manager

- a. The SA Manager is responsible for ensuring the appropriate SA requirements are specified in the project requirements documentation with the objective of ensuring SA compliance throughout the project lifecycle. Additionally the SA Manager shall ensure the software acquirer and provider understand the SA requirements. The SA Manager's key tasks are:
  - Executing, directing and managing the SA procedural requirements according to the Software Assurance Plan (SAP) or Software Safety and Assurance Plan.
  - Conducting and documenting periodic reviews, audits, and assessments throughout the projects lifecycle.
- b. Additionally, the SA Manager will assure that the SA Classification is identified and the appropriate level of SA effort is applied. Tailoring the implementation of the SA effort for a specific project is dependent upon the software's SA Classification(s).

### 1.2.4 Project SMA Representatives

- a. The Project SMA Representatives are responsible for performing SA and SS functions on their assigned projects throughout the project lifecycles. These functions are accomplished through inspections, witnessing of activities, conducting surveillance, and verification of artifacts and processes. Additionally, a key role for the Project SMA Representative is to coordinate with the respective project's team to ensure that all software assurance and software safety (safety, quality, reliability, verification and validation) requirements and procedures are being satisfied.

### 1.2.5 System Hazard Engineer/System Safety Engineer

- a. The System Hazard Engineer/System Safety Engineer is responsible for performing Preliminary Hazard Analysis (PHA), Hazard Analysis (HA), and System Hazard Analysis (SHA) according to NPR 8715.3, SSP-8715-0001 SSC Safety and Health Handbook and identifying the hazards within a system, including software, and determining the software's safety-criticality. A key role, throughout the project lifecycle, is to coordinate with other project safety and software engineers and project management to identify system hazards and determine the software's contribution to safety, controls, design features, verifications, and requirements needed to assure safer software operation within the system.

Stennis Procedural Requirements	SPR 8739.1	B-1
	<i>Number</i>	<i>Rev.</i>
	Effective Date: April 1, 2012	
	Expiration Date: April 1, 2017	
Responsible Office: Office of Safety and Mission Assurance		
<b>SUBJECT: Software Assurance Procedural Requirements</b>		

### 1.2.6 Software Acquirer

- a. The Software Acquirer (or customer) is the entity or individual who specifies the requirements for the software and accepts the resulting software products. These are generally NASA SSC Civil Servants or Prime Contractor personnel.
- b. The Software Acquirer is responsible for addressing requirements as specified in the NASA SA Standard section 5.0 or to the extent specified in the contract or other agreement such as Memorandum of Agreement/Understanding. Specifically, the Software Acquirer is responsible for specifying the SA requirements for the entire life cycle of the product.
- c. The Software Acquirer shall contribute to the development of the Preliminary Hazard Analysis (PHA), Hazard Analysis (HA), and/or System Hazard Analysis (SHA) as defined in SCWI-8710-0001, by providing technical expertise to the System Hazard Engineer/System Safety Engineer during the development of these artifacts.

### 1.2.7 Software Provider

- a. The Software Provider (or supplier) refers to the entities or individuals that design, develop, implement, test, operate, and maintain the software products.
- b. The Software Provider is responsible for addressing requirements as specified in the NASA SA Standard section 6.0 or to the extent specified in the contract or other agreement such as Memorandum of Agreement/Understanding.
- c. The Software Provider is responsible for ensuring that acquisitions internal to NASA will follow the NASA SA standards.
- d. The Software Provider shall contribute to the development of the Preliminary Hazard Analysis (PHA), Hazard Analysis (HA), and/or System Hazard Analysis (SHA) as defined in SCWI-8710-0001, by providing technical expertise to the System Hazard Engineer/System Safety Engineer during the development of these artifacts.

### 1.2.8 SSC Independent Verification and Validation (IV&V) Liaison

- a. In the event that a project warrants IV&V support, a Liaison to the IV&V facility from the SMA organization will be assigned. The IV&V Liaison serves as the project Point of Contact (POC) to support and coordinate the planning, execution, and scoping of the IV&V effort. The specific software components, exchange of information/data and tasks to be performed will be documented in an IV&V execution plan. The key role for the SMA IV&V Liaison will be facilitating the communication and exchange of information and data between the project and the IV&V project representatives.

Stennis Procedural Requirements	SPR 8739.1	B-1
	<i>Number</i>	<i>Rev.</i>
	Effective Date: April 1, 2012	
	Expiration Date: April 1, 2017	
Responsible Office: Office of Safety and Mission Assurance		
<b>SUBJECT: Software Assurance Procedural Requirements</b>		

## **CHAPTER 2 SOFTWARE ASSURANCE PROCESS**

### **2.1 Definition**

NASA SSC is a unique facility that consists of several one of a kind full scale rocket engine/motor test facilities that are national assets. The NASA SSC SA process is a planned and systematic set of activities to ensure the conformance of SA life cycle processes and products. SA assures that the software and its related products meet their specified requirements, conform to standards and regulations, are consistent, complete, correct, safe, secure and reliable as warranted for the system and operating environment, and satisfy customer needs.

### **2.2 Implementation**

- a. This SPR shall apply to and be referenced in new contracts and subcontracts which develop software for NASA SSC systems.
- b. The procuring NASA SSC Directorate shall comply with this SPR and work with the SSC SMA Manager and SSC SA Manager to make a conscious, documented decision as to how best to apply these requirements to current contracts and ongoing projects.

### **2.3 Training**

- a. All personnel who manage, develop, implement and/or perform SA activities shall be trained and possess the proper skills for the SA endeavors. Refer to SPLN 3410-0004, Personnel Training Plan for Safety and Mission Assurance, and SCWI-3410-0002, Training and Development Plan.
- b. Types of training include, but not limited to, items shown below:
  - Software Assurance
  - Software Safety
  - Software System Safety
  - Software Engineering Design Methods and Languages
  - Software Processes
  - Software Development Environments
  - Software Tools
  - Software Testing Techniques
- c. Program and/or Project Software Assurance Plans shall identify and tailor the training requirements to meet the needs of the Program or Project for implementing the Software Assurance Activity.
- d. Appropriate records of training shall be maintained in the System for Administration, Training and Education Resources for NASA (SATERN).

Stennis Procedural Requirements	SPR 8739.1	B-1
	<i>Number</i>	<i>Rev.</i>
	Effective Date: April 1, 2012	
	Expiration Date: April 1, 2017	
Responsible Office: Office of Safety and Mission Assurance		
<b>SUBJECT: Software Assurance Procedural Requirements</b>		

## 2.4 NASA SSC Software Life Cycle Management Requirement

- a. The NASA SSC personnel shall conform to the applicable sections of software life cycle management requirements in NPR 7120.5, NASA Space Flight Program and Project Management Requirements. Life cycle phases determine which activities will be performed. The NASA SA Standard requirements shall be incorporated to assure adherence to each of the software assurance disciplines throughout the project life cycle.
- b. Management of NASA SSC SA activities shall be implemented as part of the project formulation stage.
- c. The NASA SSC SA requirements shall be assured for the duration of the software's life cycle which includes acquisition, development, acceptance, operation, maintenance, and retirement for the Software Classification and Software Safety Criticality. The NASA-STD-8739.8, Appendix C, Requirements Compliance Matrix shall be used as a SA requirements life cycle compliance checklist.
- d. The Program / Project Software Assurance Plan shall define the following key software assurance disciplines as described in NASA-STD-8739.8:
  - Software Quality (Assurance, Control and Engineering)
  - Software Safety
  - Software Reliability
  - Software V&V
  - Software IV&V

## 2.5 Tailoring, Deviations, and Waivers

- a. Implementation of the NASA SSC SA requirements may be tailored based on the NASA SSC Software Assurance Classification Report (SACR), SSC Form SSC-809, as well as size, complexity, criticality, and risk as defined in the project's Software Management Plan (SMP) and/or SAP. The tailoring shall be performed in accordance with NASA-STD-8739.8 and NPR 7150.2. NASA-STD-8739.8, Appendix A.4 and Table A-3, Determination of Software Assurance Level of Effort, shall be used to determine and prioritize the SA effort. Instructions for completing Form SSC-809 are accessed by selecting the "instructions" button on the form.
- b. SSC SA waivers and/or variances shall be documented on the SSC Form SSC-517 and processed in accordance with the NASA Safety Manual NPR 8715.3, the NASA-STD-8739.8 and the governing Technical Authority (TA) per Variance and Alternate Standard Requests, SSTD-8070-0007-CONFIG. Instructions for completing Form SSC-517 are documented in SSTD-8070-0007-CONFIG.

Stennis Procedural Requirements	SPR 8739.1	B-1
	<i>Number</i>	<i>Rev.</i>
	Effective Date: April 1, 2012	
	Expiration Date: April 1, 2017	
Responsible Office: Office of Safety and Mission Assurance		
<b>SUBJECT: Software Assurance Procedural Requirements</b>		

## 2.6 Functional SA Role Assignment and Resources

- a. Prior to performing any SA Process activities, the SMA Manager shall assure that all functional SA roles are assigned and resources provided as described in Section 1.2 above.
- b. Functional SA roles shall include the respective SA Project Representatives, the SA Manager, and the System Hazard Engineer/System Safety Engineer.

## 2.7 Software Assurance Classification Assessment

- a. The SA Manager and the Project SMA Representatives shall perform and participate in a Software Assurance Classification Assessment of the project software and software components. The Software Classification Assessment shall be performed according to NASA-STD 8739.8 Appendix A, The Software Classification Assessment and SOI 8080-0052.
- b. The NASA SSC SACR (SSC Form SSC-809) shall be placed under configuration control by the appropriate authorizing board as defined in center policies. Instructions for completing Form SSC-809 are accessed by selecting the “instructions” button on the form.
- c. The SA Classification Report shall be used to prioritize SA level of effort for NASA SSC software as previously discussed in Section 2.5.

## 2.8 Software Quality Assurance

- a. The SA Manager and Project SMA Representatives shall ensure that quality is built into the software products by reviewing, evaluating and supporting the development of project software related products and processes (i.e., plans, procedures, requirements, design documents, verification documents, reports, metrics, schedules, and records) for SA compliance.
- b. The SA Manager and/or Project SMA Representatives shall investigate, audit, review and/or evaluate the execution of project software life cycle processes for SA compliance and adherence to the Project SA plan. The results and/or findings for each event shall be documented in a report(s) and maintained in the project records or as defined in center processes.
- c. The SA Manager shall participate, conduct, and attend formal reviews, audits and inspections and conduct informal project meetings to assure software quality issues are addressed. The results and/or findings for each event shall be documented in a report(s) and maintained in the project records.

Stennis Procedural Requirements	SPR 8739.1	B-1
	<i>Number</i>	<i>Rev.</i>
	Effective Date: April 1, 2012	
	Expiration Date: April 1, 2017	
Page 15 of 18		
Responsible Office: Office of Safety and Mission Assurance		
<b>SUBJECT: Software Assurance Procedural Requirements</b>		

## 2.9 Software Safety Criticality

- a. Safety Critical Systems, as defined in NPR 8715.3, which include software must be evaluated for software's contribution to the system safety early in the acquisition or planning phase. Unless the evaluation proves that the software is NOT involved in system safety of the project, the software shall be assumed to be safety-critical; therefore, NASA-STD-8719.13 and NPR 7150.2A SWE-134 are to be followed. NASA-STD-8719.13 requirements must be met, but the implementation and approach may vary dependent upon the risk posed by the safety critical software on the safety functions of the system. The NASA-STD-8719.13 Appendix B, Software Safety Requirements Compliance Matrix shall be used as a checklist to ensure requirements coverage.
- b. The project System Hazard Engineer/System Safety Engineer shall conduct a PHA, HA, and/or SHA per NPR 8715.3, SSP-8715-0001 SSC Safety and Health Handbook and NASA-STD-8719.13 and develop a report(s). The PHA or root cause analysis tool is used to determine if the software is safety critical. The HA or SHA is used to establish the Risk Assessment Code (RAC).
- c. The SA Manager and Project SMA Representative shall participate in the review of the system software PHA / HA report(s).
- d. The project shall fund the Software Engineer's (both Acquirer and Provider) time to participate in the development of the PHA, HA, and/or SHA and review of the system software PHA / HA report(s).
- e. Software shall be analyzed by the System Hazard Engineer / System Safety Engineer and SA Manager to determine if software has a potential for causing a hazard, and/or is part of a system that controls, monitors or mitigates a hazard.
- f. During operational phase all system discrepancies and configuration changes shall be reviewed and analyzed for system safety impacts by the project SA Manager and Project SMA Representatives. If adverse system safety effects are expected and/or exist, the HA shall be updated.

## 2.10 Software Reliability

- a. The SA Manager and Project SMA Representatives shall ensure that quantifiable software reliability requirements are defined and then measure and compare the results to assure reliability products are produced though out the project life cycle.
- b. The SA Manager and/or Project SMA Representatives shall support the development and review of project software related documents (i.e., plans, procedures, requirements, design documents, verification documents, reports, schedules, and records) to assure

Stennis Procedural Requirements	SPR 8739.1	B-1
	<i>Number</i>	<i>Rev.</i>
	Effective Date: April 1, 2012	
	Expiration Date: April 1, 2017	
Page 16 of 18		
Responsible Office: Office of Safety and Mission Assurance		
<b>SUBJECT: Software Assurance Procedural Requirements</b>		

reliability has been specified, implemented correctly, and verified by testing (i.e., fault detection, isolation, tolerance, and recovery).

- c. The SA Manager and Project SMA Representatives shall identify and analyze defect-related data to support reliability analysis, trends and metrics products. They shall then document this data to support software quality metrics and trend analysis as defined in the SAP as described in Section 2.11 below.

## 2.11 Software Assurance Plan

- a. Each program or project consisting of Class A-D software shall develop a SAP conforming to NASA-STD-8739.8, and document all the required software development and maintenance activities.
- b. Each program or project consisting of safety-critical software shall develop a Software Safety Plan (SSP) conforming to NASA-STD-8719.13, and document all the required software development and maintenance activities for safety-critical software. This plan may be combined with the SAP for that same program or project to improve efficiency. The combined document shall be known as a Software Safety and Assurance Plan (SSAP). For the remainder of this document, an SAP or SSAP will be referenced as SAP.
- c. The NASA-STD-8739.8 Appendix B, Software Assurance Plan Template or SSC SSAP Template stored in DDMS shall be used as an outline for the SAP development. For smaller projects, this may be incorporated in another project planning document or in the Project Quality Assurance Plan.
- d. The SAP shall be developed during the project planning phase by the SA Manager and/or Project SMA Representatives and formally staffed and approved by the project representatives identified in the NASA SSC SSAP Template.
- e. Each Program / Project shall follow their respective SAP.
- f. The SAP shall detail the organizational structure and SA activities required to accomplish software assurance and as defined in the NASA-STD-8739.8 Template.
- g. The SAP shall describe a software metrics collection and reporting process that complies with the SA and SS Standards.

## 2.12 Software Assurance Metrics

- a. The SA Manager and Project SMA Representatives will coordinate with the program or project team to assure the collection, analysis and documentation of metrics data.

Stennis Procedural Requirements	SPR 8739.1	B-1
	<i>Number</i>	<i>Rev.</i>
	Effective Date: April 1, 2012	
	Expiration Date: April 1, 2017	
Responsible Office: Office of Safety and Mission Assurance		
<b>SUBJECT: Software Assurance Procedural Requirements</b>		

- b. The project-specific SA metrics shall be defined in the project SAP. These metrics shall be tracked, updated and reviewed on a periodic basis (i.e., bi-weekly, monthly, bi-monthly) as defined in the SAP. Additionally, at a minimum, the metrics shall be presented and discussed at the appropriate management reviews as defined in the program / project SAP.
- c. The results shall be recorded and maintained as defined in the SAP.

### **2.13 Software Assurance Task Review Process**

- a. Throughout the program or project life cycle, which includes the acquisition, development, acceptance, operation, maintenance, and retirement phases, the SA task activities shall be monitored by the SA Manager, and/or the Project SMA Representatives to ensure that SA practices remain in place and are being followed accordingly.

### **2.14 Software Assurance Acquirer and Provider**

- a. The SA Acquirer and Provider participate and work together, the primary difference is that the Acquirer defines and ensures execution of the SA requirements and the Provider ultimately is responsible for the development of the software products and adherence to the project's software and SA requirements. The majority of the time, from a project perspective, the NASA SSC SMA, SA, and Project organization fulfills the Acquirer role.
- b. The Acquirer and Provider roles, as described in section 1.2, and defined in NASA-STD-8739.8, sections 5 and 6, shall be used as guidance to tailor the project requirements, contract and the SAP to assure SA compliance.

### **2.15 Software Assurance Task-Developed Products/Documents**

- a. The products and records developed by the SA activities shall, at a minimum, include the following:
  - NASA SSC SACR
  - Specific Project SA PHA, HA, and SHA Reports as applicable
  - Specific Program, Project or Facility SAP
  - Software Assurance Checklists
  - Process/Product Audit Reports
  - SA Status Reports
  - Deviations or Waivers as applicable
  - Metrics (and Metrics reports)
- b. Records shall be maintained in accordance with NPR 1441.1, NASA Records Retention Schedules and SPR 1440.1, SSC Records Management Program Requirements.

Stennis Procedural Requirements	SPR 8739.1	B-1
	<i>Number</i>	<i>Rev.</i>
	Effective Date: April 1, 2012	
	Expiration Date: April 1, 2017	
Page 18 of 18		
Responsible Office: Office of Safety and Mission Assurance		
<b>SUBJECT: Software Assurance Procedural Requirements</b>		

## APPENDIX A – Abbreviations and Acronyms

AOA	Annual Operating Agreement
CIO	Chief Information Officer
COTS	Commercial-off-the-Shelf software
DDMS	Document Data Management System
GOTS	Government-off-the-Shelf software
HA	Hazard Analysis
IV&V	Independent Verification & Validation
MOTS	Modified-off-the-Shelf software
NASA	National Aeronautics and Space Administration
NODIS	NASA Online Directives Information System
NPD	NASA Procedural Directive
NPR	NASA Procedural Requirement
PHA	Preliminary Hazard Analysis
POC	Point-of-Contact
RAC	Risk Assessment Code
RRP	Risk Review Panel
SA	Software Assurance
SACR	Software Assurance Classification Report
SAP	Software Assurance Plan
SATERN	System for Administration, Training and Education Resources for NASA
SHA	System Hazard Analysis
SMA	Safety and Mission Assurance
SMS	Stennis Space Center Management System
SOI	Stennis Organizational Instructions
SPR	Stennis Procedural Requirement
SS	Software Safety
SSAP	Software Safety and Assurance Plan
SSC	Stennis Space Center
SSP	Software Safety Plan
STD	Standard
TA	Technical Authority
V&V	Verification & Validation