

System Wide Information Management (SWIM)

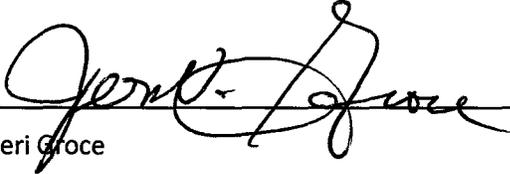
Governance Policies



Version 3.0

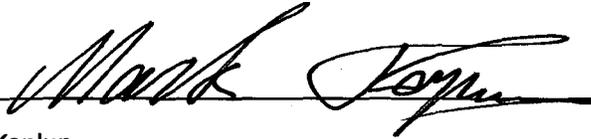
September 14, 2016

SIGNATURE PAGE



Date 9/14/16

Jeri Groce
SWIM Program Manager



Date 9/14/2016

Mark Kaplun
SWIM Governance Lead

DOCUMENT CHANGE HISTORY

Version	Date	Description of Changes
1.0	07/27/2009	Addressed comments from numerous stakeholders to Drafts.
1.1	08/13/2010	Addressed additional stakeholder comments and lessons learned from creating process documentation.
2.0	02/07/2014	Modified and changed Governance policies to accommodate changes in NAS SWIM environment.
3.0	09/14/2016	Removed policies related to Service Consumers. Added/modified policies based on the new implementation of the NSRR.

Table of Contents

1	SCOPE.....	5
1.1.	Background	5
1.2.	Applicability.....	5
2	APPLICABLE DOCUMENTS.....	5
2.1.	Government Documents.....	5
2.2.	Non-Government Documents.....	6
2.3.	Order of Precedence	8
3	TERMS AND DEFINITIONS	8
3.1	Key Words	8
3.2	Terms and Definitions	8
3.3	Acronyms and Abbreviations	9
4	GENERAL POLICIES	11
5	DETAILED POLICIES.....	11
5.1	Processing Policies	11
5.1.1	SOA Suitability Assessment Policies.....	11
5.1.2	Service Lifecycle Policies	12
5.1.2.1	Proposed Stage Policies	12
5.1.2.2	Definition Stage Policies.....	13
5.1.2.3	Development Stage Policies.....	13
5.1.2.4	Verification Stage Policies.....	14
5.1.2.5	Production Stage Policies.....	14
5.1.2.6	Deprecated Stage Policies.....	14
5.1.2.7	Retired Stage Policies.....	14
5.1.3	Documentation Policies	14
5.1.3.1	Human-readable Documentation	14
5.1.3.2	XML-Based Documentation	15
5.1.4	Service Registration Policies	15
5.1.4.1	Proposed Stage	15
5.1.4.2	Definition Stage.....	16

- 5.1.4.3 Development Stage..... 16
- 5.1.4.4 Verification Stage..... 16
- 5.1.4.5 Production Stage..... 16
- 5.1.4.6 Deprecated Stage..... 16
- 5.1.4.7 Retired Stage..... 16
- 5.1.5 Waiver Policies..... 17
- 5.2 Interoperability Policies 17
 - 5.2.1 Interface Policies..... 17
 - 5.2.2 Namespaces Policies..... 17
 - 5.2.3 Semantic Interoperability Policies 18
 - 5.2.4 Information Exchange Models Policies..... 18
- 5.3 Security Policies 18
- 5.4 Versioning Policies 19
- APPENDIXES 20
 - Appendix A. Service Provider Checklist 20
 - Appendix B. Example of a Waiver Request..... 22

1 SCOPE

This document specifies the policies, rules, and standards for identifying, designing, implementing, deploying, and managing services that are enabled and/or supported by the Federal Aviation Administration (FAA) System Wide Information Management (SWIM) program.

1.1. Background

In the last decade, the National Airspace System (NAS) has undergone transformation from the traditional modes of information exchange (including system-to-system interaction) to a paradigm of [service-oriented architecture](#) (SOA).

To facilitate delivery of [SOA-based services](#), the FAA established the SWIM program. The goal of the SWIM program is to support information sharing among NAS stakeholders by providing a communications infrastructure and architectural solutions for identifying, developing, provisioning, and operating shareable and reusable services. SWIM leverages the [FAA Telecommunications Infrastructure \(FTI\)](#) that provides network-level connectivity, security and communication capability. SWIM presents a model for a next-generation computing infrastructure with a special emphasis on fielding SOA services that permits integration and consolidation of information systems.

The most challenging aspect of establishing a mature SOA-based enterprise framework of reusable [business services](#) is an effective governance model. [SOA governance](#) ensures that all of the independent SOA-based efforts (whether in the design, development, deployment, or operation of a service) come together to meet enterprise requirements.

This document establishes SOA governance policies, processes, and standards for managing the lifecycle of services, service acquisitions, service components and [registries](#), [service providers](#), and [service consumers](#).

1.2. Applicability

The policies specified in this document apply to all current and prospective [SWIM-enabled programs](#) responsible for identifying, acquiring, designing, implementing, consuming and deploying services supported and/or enabled by the SWIM program.

2 APPLICABLE DOCUMENTS

2.1. Government Documents

- [1] SWIM Controlled Vocabulary, March 2013.
<http://www.faa.gov/go/swimvocabulary>

- [2] FAA-STD-065A, Web Service Description Document, 1 July 2013.
<http://www.faa.gov/nextgen/programs/swim/governance/standards/>
- [3] FAA-STD-070, Preparation of Web Service Requirements Documents, 12 July 2012.
<http://www.faa.gov/nextgen/programs/swim/governance/standards/>
- [4] FAA-STD-073, Preparation of JAVA Message Service Description Documents, 30 September 2013.
<http://www.faa.gov/nextgen/programs/swim/governance/standards/>
- [6] 1370.113 - FAA Web Security Policy, Federal Aviation Administration, 16 April 2012.
http://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/698459
- [7] FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, National Institute of Standards and Technology, February 2004.
<http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>
- [8] FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, National Institute of Standards and Technology, March 2006.
<http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>
- [10] [NIST](#) Special Publication 800-95, Guide to Secure Web Services, National Institute of Standards and Technology, August 2007.
<http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf>.
- [26] Software Specification SWIM-005, Artifacts Versioning for SWIM-Enabled Services, 1.0.0, December 2015. <https://www.faa.gov/nextgen/programs/swim/governance/standards/media/SWIM%20Service%20Versioning%20Spec.pdf>
- [27] Syntax and Processing of XML-Based Documents in the Context of SWIM-Enabled Services, Software Specification, Version 1.0, 16 June 2015. <http://www.faa.gov/nextgen/programs/swim/governance/standards/media/Syntax%20and%20Processing%20of%20XML-Based%20Documents%2006162015.pdf>
- [28] SWIM Controlled Vocabulary (CV) Frequently Asked Questions (FAQ).
<http://www.faa.gov/nextgen/programs/swim/governance/servicesemantics/FAQ/>

2.2. Non-Government Documents

- [11] RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2, Network Working Group, August 2008.
<http://tools.ietf.org/html/rfc5246>

- [12] Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), OASIS Standard Specification, 1 February 2006.
<http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>.
- [13] RFC 2119, Key words for Use in RFCs to Indicate Requirement Levels, Network Working Group, March 1997.
<http://www.rfc-editor.org/rfc/rfc2119.txt>
- [14] Web Services Architecture, W3C Working Group Note, 11 February 2004.
<http://www.w3.org/TR/ws-arch>
- [15] Java 2 Platform, Enterprise Edition, v 1.3 API Specification
<http://docs.oracle.com/javaee/1.3/api/>
- [16] Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language, W3C Recommendation, 26 June 2007.
<http://www.w3.org/TR/wsdl20/>
- [17] XML Schema Definition Language (XSD) 1.1 Part 1: Structures, W3C Recommendation, 5 April 2012.
<http://www.w3.org/TR/xmlschema11-1/>
- [19] Extensible Markup Language (XML) 1.0 (Fifth Edition), W3C Recommendation, 26 November 2008.
<http://www.w3.org/TR/2008/REC-xml-20081126/>
- [21] DCMI Metadata Terms, Dublin Core Metadata Initiative, 14 June 2012.
<http://dublincore.org/documents/dcmi-terms/>
- [22] OWS-9 CCI Semantic Mediation Engineering Report, Open Geospatial Consortium, 2013.
https://portal.opengeospatial.org/files/?artifact_id=51840?
- [23] Aeronautical Information Exchange Model (AIXM) Release 5.0, EUROCONTROL/FAA, 6 March 2008.
http://www.aixm.aero/public/standard_page/download.html
- [24] Weather Information Exchange Model (WXXM) Version 2.0, EUROCONTROL/FAA
<http://www.wxmx.aero/wxxm/2.0>

- [25] Flight Information Exchange Model (FIXM) Version 2.0, EUROCONTROL/FAA, 22 August 2013.
<http://www.fixm.aero>
- [29] Namespaces in XML 1.0 (Third Edition), W3C Recommendation, 8 December 2009.
<http://www.w3.org/TR/REC-xml-names/>

2.3. Order of Precedence

In the event of a conflict between the text of this document and the references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

3 TERMS AND DEFINITIONS

3.1 Key Words

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [13].

These key words are capitalized when used to unambiguously specify requirements. When these words are not capitalized, they are meant in their natural-language sense.

3.2 Terms and Definitions

Note: most of the terms used in this document are defined in the SWIM Controlled Vocabulary [1] along with information about terms' sources and relationships to other terms.

<i>Semantic Interoperability</i>	The aspect of interoperability that assures that the content of the data being transferred across two systems is understood in the same way in both systems, including by those humans interacting with the systems in a given context. [22]
<i>SOA-Based</i>	Something that is designed, developed, or operated according to principles of Service-Oriented Architecture .
<i>Taxonomy</i>	A controlled list of well-defined concepts organized into a hierarchical structure.

3.3 Acronyms and Abbreviations

<i>AIM</i>	Aeronautical Information Management
<i>AIS</i>	Aeronautical Information Services
<i>AIXM</i>	Aeronautical Information Exchange Model
<i>AMS</i>	Acquisition Management System
<i>API</i>	Application Programming Interface
<i>BCD</i>	Baseline Change Decision
<i>CONOPS</i>	Concept of Operations
<i>ESB</i>	Enterprise Service Bus
<i>EIS</i>	Enterprise Infrastructure Services
<i>FAA</i>	Federal Aviation Administration
<i>FID</i>	Final Investment Decision
<i>FIXM</i>	Flight Information Exchange Model
<i>FNTB</i>	FTI National Test Bed
<i>FPRD</i>	Final Program Requirements Document
<i>FTI</i>	FAA Telecommunications Infrastructure
<i>GRID</i>	Global Registry Identifier
<i>HTTP</i>	Hypertext Transfer Protocol
<i>IARD</i>	Investment Analysis Readiness Decision
<i>IID</i>	Initial Investment Decision
<i>IPR</i>	Initial Program Requirements
<i>ISD</i>	In Service Decision
<i>ISPD</i>	Implementation Strategy and Planning Document
<i>JMS</i>	Java Message Service
<i>JRC</i>	Joint Resources Council
<i>JMSDD</i>	Java Messaging Service Description Document
<i>MOA</i>	Memorandum of Agreement
<i>NAS</i>	National Airspace System
<i>NEMS</i>	NAS Enterprise Messaging Service
<i>NSRR</i>	NAS Service Registry/Repository

OGC	Open Geospatial Consortium
OIB	Operational Integration Board
PO	Program Office
PRD	Program Requirements Document
SLMP	Service Lifecycle Management Process
SOA	Service-Oriented Architecture
SOAP	Originally “Simple Object Access Protocol”; the full spelling is no longer used
URI	Uniform Resource Identifier
WSDD	Web Service Description Document
WSDL	Web Service Description Language
WSRD	Web Service Requirements Document
W3C	World Wide Web Consortium
WXXM	Weather Information Exchange Model
XML	eXtensible Markup Language
XSD	XML Schema Definition

4 GENERAL POLICIES

This section describes the general policies for instituting governance mechanisms of [SOA-based](#) implementations in the context of SWIM. These policies are further elaborated in [section 5](#) of this document.

- a. All [SWIM-enabled programs](#) SHALL conform to the SOA practices, architectural principles, and government regulations as identified and established by this document.
- b. All SWIM-enabled programs SHOULD adhere to the processes and procedures as defined in the FAA Acquisition Management System (AMS) where applicable.
- c. All SWIM-enabled programs SHALL conform to the FAA Telecommunications Infrastructure (FTI) policies and procedural guidelines.
- d. All SWIM-enabled programs SHALL provide required documents and artifacts to the SWIM Program Office (PO) for review and approval throughout all stages of a [service's](#) lifecycle as identified and established by this document.
- e. All SWIM-enabled programs SHALL make all developed, acquired and modified business services discoverable, searchable, and retrievable by registering them in the [NAS Service Registry/Repository \(NSRR\)](#) located at <https://nsrr.faa.gov/>.
- f. All SWIM-enabled programs SHALL conform to the set of FAA and industry standards as identified and referenced by this document.

5 DETAILED POLICIES

5.1 Processing Policies

5.1.1 SOA Suitability Assessment Policies

The goal of the [SOA](#) suitability assessment process is to discover SOA-suitable program initiatives early in their analysis phase. This early discovery is critical for the program's architecture and requirements development and ensures appropriate integration of SWIM infrastructure in the program solution architecture.

- a. All programs seeking enablement by SWIM SHALL undergo a SOA suitability assessment, conducted by the SWIM Program Office (PO), before each of the following Joint Resources Council (JRC) decision points:
 1. Investment Analysis Readiness Decision (IARD)
 2. Initial Investment Decision (IID)
 3. Final Investment Decision (FID)
 4. Baseline Change Decision (BCD)
- b. Upon completion of the SOA suitability assessment, all programs SHALL obtain the following documents from the SWIM PO:
 1. SOA Suitability Scorecard

2. SOA Suitability Assessment as a section of the Enterprise Infrastructure Services (EIS) Assessment submitted to the JRC Secretariat

Additional information on SOA suitability assessment is available at the [SWIM Governance Website](#).

5.1.2 Service Lifecycle Policies

The ability to effectively manage all stages of the [service](#) lifecycle is fundamental to the success of governing SOA services. This document asserts the Service Lifecycle Management Process (SLMP) to contain a set of controlled and well-defined activities performed at each stage of a service's lifecycle for any and all versions of any given service.

Table 1 lists the sequential service lifecycle stages. Policies relevant to each stage are described more fully in corresponding subsections following Table 1.

Table 1 Service Lifecycle Stages

<i>Lifecycle Stage</i>	<i>Description</i>
Proposed	The stage during which the business needs for the proposed service are identified and assessed as to whether needs can be met through the use of SOA.
Definition	The stage during which the service's business requirements are gathered and the service design is produced based on these requirements.
Development	The stage during which the service specifications are developed and the service is built.
Verification	The stage during which the service is being inspected and/or tested to confirm that the service is of sufficient quality, complies with the prescribed set of standards and regulations, and is approved for use.
Production	The stage during which the service is available for use by its intended consumers.
Deprecated	The stage during which the service can no longer be used by new consumers.
Retired	The stage during which the service is disposed of and is no longer used.

5.1.2.1 Proposed Stage Policies

- a. Prior to IARD, all NAS programs seeking enablement by SWIM SHALL provide the following documents to SWIM Governance for review:
 1. Preliminary Requirements Document (PRD)
 2. Range of Alternatives document
- b. Prior to IID, all NAS programs seeking enablement by SWIM SHALL provide the following documents to SWIM Governance for review:
 1. Initial Program Requirements Document (IPR)

2. Solution Concept of Operations (CONOPS)
- c. All programs going through the AMS and seeking enablement by SWIM shall incorporate SWIM requirements into their Final Program Requirements Document (FPRD).
- d. All programs going through the AMS and seeking enablement by SWIM shall incorporate SWIM requirements into their Initial Implementation Strategy and Planning Document (ISPD).
- e. All Service Providers shall initiate the registration process in the NSRR as described in section [5.1.4](#) of this document.

5.1.2.2 Definition Stage Policies

- a. All Service Providers SHALL modify the following documents to accommodate requirements for compliance with SWIM Governance policies:
 1. ISPD
 2. FPRD
- b. Prior to FID, all Service Providers SHALL provide SWIM Governance with the following documents for review:
 1. Solution CONOPS
 2. FPRD
 3. ISPD
- c. SWIM candidate programs outside of the AMS SHALL provide artifacts equivalent to the CONOPS and Initial Program Requirements Document (IPR).
- d. All Service Providers SHALL prepare a Web Service Requirements Document (WSRD) for each service.
- e. All Service Providers SHALL upload the WSRD to the NSRR prior to FID.
- f. All Service Providers SHALL augment the service metadata in the NSRR in accordance with [section 5.1.4.2](#) of this document.

5.1.2.3 Development Stage Policies

- a. Depending on whether a new service is implemented as a [Web Service](#) or a [Java Messaging Service \(JMS\)](#), all Service Providers SHALL prepare a Web Service Description Document (WSDD) and/or a Java Messaging Service Description Document (JMSDD) as described in [section 5.1.4](#) of this document. Note: for the purpose of this document, all Open Geospatial Consortium (OGC)-compliant services are considered to be Web Services.
- b. Section 5.1.4 describes circumstances whereby a Service Provider can request a waiver from having to prepare a separate WSDD and/or JMSDD if all requisite metadata has been entered in the NSRR. All Service Providers who have not obtained such a waiver SHALL upload the WSDD (or the JMSDD) to the NSRR.
- c. When implementing a Web Service, the Service Provider SHALL upload a Web Service Description Language (WSDL) document to the NSRR.
- d. When an XML schema is used to describe information exchanged by a service, the Service Provider SHALL upload the XML schema to the NSRR.
- e. All Service Providers SHALL augment the service metadata in the NSRR in accordance with [section 5.1.4.3](#) of this document.

5.1.2.4 Verification Stage Policies

- a. All Service Providers SHALL prepare an Operational Test Plan.
- b. All Service Providers SHALL complete an OIB (Operational Integration Board) checklist as required by EIS.

5.1.2.5 Production Stage Policies

- a. All Service Providers SHALL provide an In Service Decision (ISD) action plan to SWIM Governance for review and approval.
- b. All Service Providers SHALL submit the ISD action plan to the NSRR.

5.1.2.6 Deprecated Stage Policies

- a. All Service Providers SHALL indicate the service retirement date.
- b. All Service Providers SHALL provide a Deprecation Impact Analysis to SWIM Governance for review and approval.
- c. All SWIM Service Providers SHALL upload the Deprecation Impact Analysis to the NSRR.

5.1.2.7 Retired Stage Policies

- a. All Service Providers SHALL provide a Retirement Impact Analysis to SWIM Governance for review and approval.
- b. All Service Providers SHALL upload the Retirement Impact Analysis to the NSRR.

For a comprehensive Service Provider checklist, see [Appendix A](#).

5.1.3 Documentation Policies**5.1.3.1 Human-readable Documentation**

- a. All Service Providers SHALL provide SWIM Governance with the following documents for review and subsequent uploading to the NSRR:
 1. CONOPS
 2. WSRD
 3. WSDD or JMSDD
 4. Deprecation Impact Analyses
 5. Retirement Impact Analyses
- b. All Service Providers SHALL prepare a WSRD in accordance with FAA-STD-070, "Preparation of Web Service Requirements Documents" [\[3\]](#).
- c. When preparing a WSRD for a non-Web Service implementation (e.g., a JMS-based service), all Service Providers SHALL tailor the WSRD to fit the implementing technology.
- d. All WSDDs SHALL be prepared in accordance with FAA-STD-065A, "Preparation of Web Service Description Documents" [\[2\]](#).
- e. All JMSDDs SHALL be prepared in accordance with FAA-STD-073, "Preparation of Java Messaging Service Description Documents" [\[4\]](#).

5.1.3.2 XML-Based Documentation

- a. All XML documents SHALL be developed in compliance with XML version 1.0 [19].
- b. All XML documents SHALL use UTF-8 encoding.
- c. All XML schemas SHALL conform to the structure and constraints specified in the XML Schema 1.0 Recommendation [17].
- d. All XML service definition documents SHALL conform to the structure and constraints specified in the WSDL 1.1 Specification [16].
- e. All XML-based documentation produced by a Service Provider SHALL be developed in compliance with Software Specification “Syntax and Processing of XML-Based Documents in the Context of SWIM-Enabled Services, Version 1.0” [27].

5.1.4 Service Registration Policies

This document asserts [NSRR](#) registration to be a formal process of storing, cataloging and managing of SOA services metadata and relevant artifacts in the NSRR. Use of the NSRR is mandated for the development and acquisition of all new or modified [SWIM-enabled programs](#). The process of entering information in the NSRR is aligned with service lifecycle management in a way that ensures that the information and documentation entered in the registry is in compliance with the SWIM Governance Policies.

The NSRR captures all service metadata required by FAA-STD-065A, “Preparation of Web Service Description Documents (WSDD)” [2] and FAA-STD-073, “Preparation of Java Messaging Service Description Documents (JMSDD)” [4].

- a. All SWIM-enabled programs SHALL request creation of one or more user accounts in the NSRR for individual(s) who will perform the functions of Service Provider for each proposed service.
- b. All Service Providers SHALL work with SWIM Governance to establish a service name and a service GRID (Global Registry Identifier) for each proposed service.
- c. For each lifecycle stage identified in the section [5.1.2](#) of this document, all Service Providers SHALL initiate requests to SWIM Governance to promote their registered services from one lifecycle stage to the next.
- d. After the Service Provider has entered all of the required metadata in the NSRR and is satisfied with its quality and completeness, the Provider MAY request a waiver from SWIM Governance (see [section 5.1.5](#)) for an exemption from having to submit a separate WSDD or JMSDD to the SWIM PO, with the understanding that this waiver does not release the Provider from any requirements imposed by the Provider organization or other FAA authority to prepare a separate WSDD or JMSDD for approval by that authority.

The following sections specify what metadata should be entered in the NSRR at each lifecycle stage.

5.1.4.1 Proposed Stage

After SWIM Governance has worked together with the Service Provider to establish a service name and a service GRID:

- a. All Service Providers SHALL identify the service version as described in [section 5.4](#) of this document.
- b. All Service Providers SHALL provide a description of the service.
- c. All Service Provider SHALL identify at least one ATM Service Category.
- d. All Service Providers SHALL identify at least one SWIM Service Product Category.
- e. All Service Providers SHALL identify a Service Interface Type.
- f. All Service Providers SHALL identify a Service Criticality Level.
- g. All Service Providers SHALL provide a description of the Service Provider organization.
- h. All Service Providers SHALL identify at least one Point of Contact.
- i. All Service Providers MAY identify current or potential Service Consumers.

5.1.4.2 Definition Stage

- a. All Service Providers SHALL provide a description of the Service Functionality.
- b. All Service Providers SHALL provide a description of the Service Security.
- c. All Service Providers SHALL provide a description of the Qualities of Service.
- d. All Service Providers SHOULD provide a description of the Service Policies.
- e. All Service Providers SHOULD provide a description of the Service Operations.
- f. All Service Providers SHALL provide a description of the Service Messages.

5.1.4.3 Development Stage

- a. All Service Providers SHOULD provide a description of the Environmental Constraints.
- b. All Service Providers SHOULD provide a description of the Message Headers.
- c. All Service Providers SHALL provide a description of the Message Payloads.
- d. All Service Providers SHOULD provide a description of the Faults.
- e. All Service Providers SHALL provide a description of the Data.
- f. All Service Providers SHOULD provide a description of the Bindings.
- g. All Service Providers SHOULD provide a description of the Endpoints.

5.1.4.4 Verification Stage

No entries in the NSRR are required.

5.1.4.5 Production Stage

No entries in the NSRR are required.

5.1.4.6 Deprecated Stage

No entries in the NSRR are required.

5.1.4.7 Retired Stage

No entries in the NSRR are required.

5.1.5 Waiver Policies

- a. In cases where specific policies required by this document cannot be implemented, a SWIM-enabled program SHALL request a waiver from SWIM Governance. See [Appendix B](#) for an example of a waiver request.
- b. When requesting a waiver for exemption from specific policies, the SWIM-enabled program SHALL provide the reasons why those policies cannot be implemented and/or why another course should be chosen (e.g., to use non-mandated standards).
- c. When requesting a waiver, the SWIM-enabled program SHALL provide the date or condition upon which the waiver should expire.
- d. When a waiver is granted for not uploading a required artifact to the NSRR, the SWIM-enabled program SHALL upload the signed waiver in lieu of the required artifact.

5.2 Interoperability Policies

5.2.1 Interface Policies

NAS SOA implementations are based on two technological solutions: [Web Services](#) and [JMS](#)-based services. In the Web Service, a requester of a service accesses a remote system hosting the service (usually via HTTP) and invokes methods offered through a public interface (described in a XML-based file, usually WSDL). In the JMS, messages (specifically formatted sets of data) are exchanged through a messaging server, which acts as a message exchange service for client programs that produce or receive data.

- a. All [SWIM-enabled programs](#) implementing a Web Service architectural solution SHALL adhere to the architectural approach as described in the Web Services Architecture document [\[14\]](#) produced by the World Wide Web Consortium (W3C). For additional explanation about the concept of a Web Service as it is understood in FAA, see FAA-STD-070 section 1.3, Basic Concepts [\[3\]](#).
- b. All SWIM-enabled programs implementing a JMS architectural solution SHALL adhere to the interface defined by the JMS Application Programming Interface (API) version 1.3 [\[15\]](#).

5.2.2 Namespaces Policies

- a. XML document namespace declarations pursuant to the “Namespaces in XML” specification [\[29\]](#) SHOULD be defined as a URI using the HTTP scheme.
- b. The values of the namespace declarations in XML documents SHOULD be dereferenceable.
- c. Each namespace defined as a URI SHOULD resolve to a human or machine-processable document that directly or indirectly provides information about the document or dataset associated with the given namespace.

5.2.3 Semantic Interoperability Policies

This section addresses the policies that promote and facilitate [semantic interoperability](#) among SWIM-enabled programs. Semantic interoperability ensures that the content of information is understood in the same way between interacting systems, including by those humans interacting with the systems in a given context. In the context of SWIM SOA governance, semantic interoperability is achieved through the consistent use of description standards (e.g., Dublin Core [\[21\]](#), FAA-STD-065A [\[2\]](#)), shared vocabularies, common sets of [taxonomies](#), and ontologies.

- a. When developing SWIM-related documentation, all SWIM-enabled programs SHOULD adhere to the terms and their associated definitions as defined in the SWIM Controlled Vocabulary (CV) [\[1\]](#).
- b. In lieu of repeating CV terms and definitions in the glossary sections included in most SWIM documents, it is RECOMMENDED that SWIM-enabled programs hyperlink the terms directly to their CV definitions as described in the CV Frequently Asked Questions (FAQ) document [\[28\]](#).

5.2.4 Information Exchange Models Policies

- a. When designing a service to enable the collection, management or distribution of Aeronautical Information Services (AIS) data (i.e., data used to describe, manage and control the safety, regularity and efficiency of international and national air navigation), all SWIM-enabled programs SHALL conform to the structure and constraints specified in the Aeronautical Information Exchange Model (AIXM) release 5.x [\[23\]](#).
- b. When designing a service to enable the collection, management or distribution of weather data (i.e., data used to describe current or predicted atmospheric conditions), all SWIM-enabled programs SHALL conform to the structure and constraints specified in the Weather Exchange Model (WXXM) version 2.x [\[24\]](#).
- c. When designing a service to enable the collection, management or distribution of flight data (i.e., data used to describe, manage and control the safe movement of aircraft in the NAS), all SWIM-enabled programs SHALL conform to the structure and constraints specified in the Flight Information Exchange Model (FIXM) version 4.x [\[25\]](#).
- d. To use exchange models other than AIXM, WXXM, or FIXM in situations described in policies ‘a’, ‘b’, or ‘c’ respectively, all SWIM-enabled programs SHALL obtain a waiver from SWIM Governance as described in [section 5.1.5](#) of this document.

5.3 Security Policies

- a. All [SWIM-enabled programs](#) SHALL comply with NIST Special Publication 800-95 “Guide to Secure Web Services” [\[10\]](#).
- b. All SWIM-enabled programs SHALL comply with FAA Order 1370.113 “FAA Web Security Policy” [\[6\]](#).

- c. All SWIM-enabled programs SHALL conform to the FIPS PUB 199 “Standards for Security Categorization of Federal Information and Information Systems” [7].
- d. All SWIM-enabled programs SHALL conform to the FIPS PUB 200 “Minimum Security Requirements for Federal Information and Information Systems” [8].
- e. All SWIM-enabled programs implementing JMS-based solutions SHALL deploy Transport Layer Security (TLS) Protocol Version 1.2. [11].
- f. All SWIM-enabled programs implementing [Web Service](#) solutions SHALL deploy the WS-Security 1.1 family of specifications as defined in Web Services Security: SOAP Message Security 1.1 (WS-Security 2004) [12].

5.4 Versioning Policies

In the SWIM environment, versioning regulations and policies support the creation and management of multiple releases of services and associated documentation and provide a way to communicate changes to [service consumers](#).

- a. All SWIM service artifacts SHALL conform to Software Specification SWIM-005 Artifact versioning for SWIM-enabled services [26].
- b. When a Service Provider intends to introduce a new version of a service, the Provider SHALL contact SWIM Governance for instructions on whether a new instance of the service should be registered in the NSRR.
- c. When a Service Provider intends to make changes to a service, the Provider SHALL notify consumers about the upcoming changes using the NSRR’s “Service Notification” feature. (See Figure 1.)

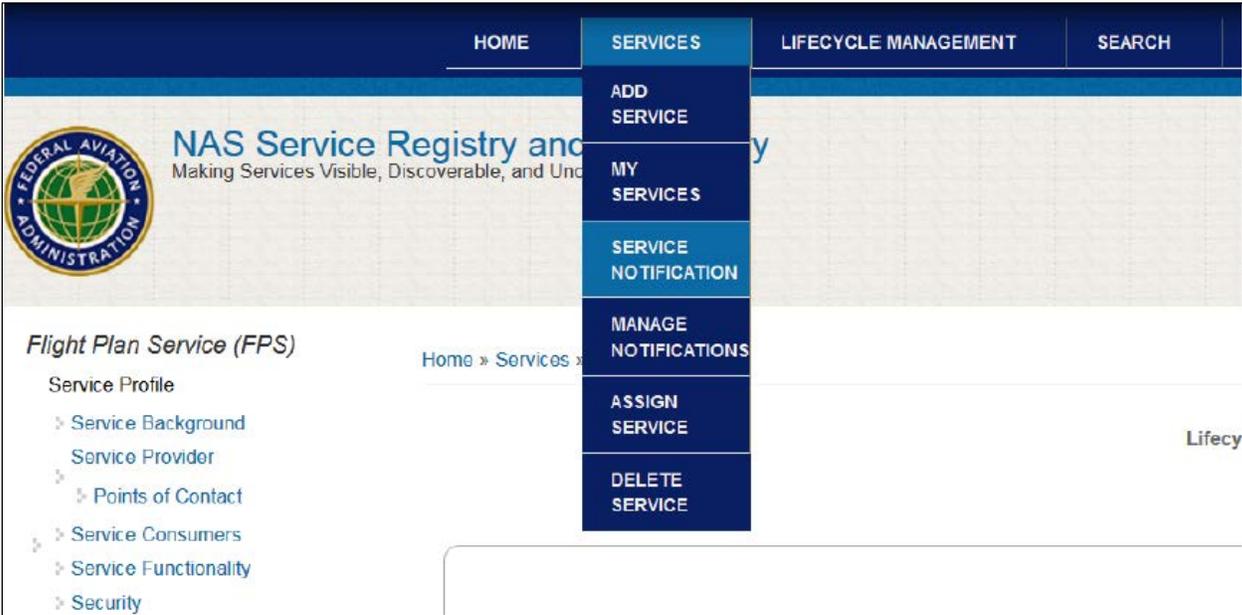


Figure 1 Creating custom notifications in the NSRR

APPENDIXES

Appendix A. Service Provider Checklist

Lifecycle Stage	Type	Description	Comment
Proposed	Document	Concept of Operations	Solution CONOPS is an AMS deliverable. Submit to NSRR.
	NSRR entry	Service version	The service version shall be identified and entered in the NSRR
	NSRR entry	Service Description	The description of the service shall be entered in the NSRR
	NSRR entry	Service Provider Point of Contact	At least one PoC shall be entered in the NSRR.
	NSRR entry	Service Consumers	Optional.
	NSRR entry	ATM Service Category	At least one value shall be selected in the NSRR
	NSRR entry	SWIM Service Product Category	At least one value shall be selected in the NSRR
	NSRR entry	Service Interface Type	One value shall be selected in the NSRR
Definition	Checkpoint	FID	Service Provider passed AMS Final Investment Decision. Applicable only to Service Providers in the AMS.
	Document	Web Service Requirements Document (WSRD)	Provides a series of requirements for the Program's Service interface. Refer to FAA-STD-70. Submit to NSRR.
	NSRR entry	Service Functionality	Description of the Service Functionality shall be added to the NSRR.
	NSRR entry	Qualities of Service	Quality of Service parameters should be added to the NSRR.
	NSRR entry	Security Mechanisms	Description of the service's Security mechanisms should be added to the NSRR.
	NSRR entry	Policies	Description of the Service Policies should be added to the NSRR.
	Deliverable	Environmental Constraints	Environmental Constraints should be added to the NSRR.
Development	NSRR entry	Interface	Interface description shall be added to the NSRR.
	NSRR entry	Operations	Operations description shall be added to the NSRR. Note: may not be applicable in JMS-based interfaces.
	NSRR entry	Messages	Messages description shall be added to the NSRR including Headers and Payloads where applicable.
	NSRR entry	Faults	Faults description shall be added to the NSRR.
	Deliverable	Web Services Description Document (WSD) or Java Messaging Service Description Document (JMSDD)	WSDL (when applicable) shall be validated in the NSRR and subsequently uploaded in the Service Documents section.
	Deliverable	XML Schema Definitions for Types	Shall be uploaded in the NSRR in the Service Documents section.

	NSRR Entry	Data Description document	Data Description Document of unspecified format (optional). Should be uploaded in the NSRR in the Service Documents section.
	NSRR entry	Data	Data description shall be added to the NSRR.
Verification	Checkpoint	Test Plan/ Producer Review	Submit to NSRR
Production	Checkpoint	ISD Action Plan	Submit to NSRR.
Deprecation	Deliverable	Deprecation Impact Analysis	Submit to the NSRR.
Retired	Deliverable	Retirement Impact Analysis	Submit to the NSRR.

Appendix B. Example of a Waiver Request

Note: this example is non-normative.

	<h3>SWIM Governance Policies Waiver Request</h3>
FOR USE BY REQUESTER	
<p>Date of Request: <u>August 21, 2013</u></p> <p>Requester's Organization: <u>En Route Services Modernization Group (ESMG)</u></p> <p>Requester's Name: <u>John D. Doe, ATO-X ESGM Manager</u></p> <p>Requester's Telephone Number: <u>(609) 444-5555</u></p> <p>Requester's Email: joe.doe@faa.gov</p> <p>Short description of request, including specific policy or policies to be waived, together with a justification of the request and alternative policies to be followed or actions to be taken:</p> <p>ESMG requests a waiver from using the Flight Information Exchange Model (FIXM) as the data exchange format for the Flight Plan Service (FPS), as prescribed by SWIM Governance Policies version 2.0, for the following reason:</p> <p>During design of FPS version 1.0, the FIXM wasn't mature and ESGM decided to use a custom-built XML-based model to describe flight plan data provided by the service. Although FIXM has since achieved a sufficient level of maturity, the transition to FIXM will significantly affect the cost of implementing FPS version 1.0 and will make it impossible to meet its release date. The transition to FIXM will be implemented in the next release of FPS, currently scheduled for March 1, 2015.</p> <p>Date or condition upon which this waiver can be expected to expire: <u>March 1, 2015</u></p>	
FOR USE BY SWIM GOVERNANCE	
<p>Resolution of Request:</p> <p>Given the information and analysis referenced above, it is considered that the use of a custom-built model instead of FIXM does not constitute a material defect in the Flight Plan Service implementation. The SWIM Governance Policies requirement to demonstrate compliance with canonical models, specifically FIXM, is hereby waived. The FPS may proceed to the Service Lifecycle Production stage.</p> <p>Waiver Granted (X) / Disapproved () on: <u>September 4, 2013</u></p> <p>Signed: <u>Mark Kaplun, SWIM Governance Lead (mark.kaplun@faa.gov)</u></p>	