System Wide Information Management (SWIM)

Governance Policies

Version 3.1

February 6, 2020

SIGNATURE PAGE

2/6/2020

Melissa Matthews
SWIM Program Manager

Date

02/06/2020

Mark Kaplun
SWIM Governance Lead

Date

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	08/18/2016	Modified Service Registration Policies to provide a set of policies for every lifecycle. Expanded Service Documentation section by adding two sub-sections.
3.1	01/27/2020	Added Change Management policies. Remove dated policies. Updated reference to new versions of Governance's documents.

Table of Contents

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

The FAA National Airspace System (NAS) is in the process of evolving from the traditional model of information exchange systems 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 FAA stakeholders by providing a communications infrastructure and architectural solutions for identifying, developing, provisioning, and operating highly-distributed and reusable services. SWIM leverages the FAA's IP network 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 2019.
https://semantics.aero/pages/swim-vocabulary.html

[2] FAA-STD-065B, Web Service Description Document, 15 July 2019.
https://www.faa.gov/air_traffic/technology/swim/governance/standards/media/FAA-STD-065B%207_15_2019.pdf

[3] FAA-STD-070, Preparation of Web Service Requirements Documents, 12 July 2012.
https://www.faa.gov/air_traffic/technology/swim/governance/standards/media/FAA-STD-070%2007-12-12%20final.pdf

[4] FAA-STD-073A, Preparation of JAVA Message Service Description Documents, 9 December 2019.
https://www.faa.gov/air_traffic/technology/swim/governance/standards/media/FAA-STD-073A%20FINAL%2012_9_19.pdf

[5] (Reserved)

[6] FAA Order 1370.121 - FAA Information Security and Privacy Program & Policy, 23 December 2016.
https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/1030708

[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

[9] 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

[10] Software Specification SWIM-005, Artifacts Versioning for SWIM-Enabled Services, 1.0.0, December 2015.
https://www.faa.gov/air_traffic/technology/swim/governance/standards/media/SWIM%20Service%20Versioning%20Spec.pdf

[11] Syntax and Processing of XML-Based Documents in the Context of SWIM-Enabled Services, Software Specification, Version 1.0, 16 June 2015.
https://www.faa.gov/air_traffic/technology/swim/governance/standards/media/Syntax%20and%20Processing%20of%20XML-Based%20Documents%2006162015.pdf

[12] SWIM Controlled Vocabulary (CV) Frequently Asked Questions (FAQ).
https://semantics.aero/SWIM%20CV%20Guidelines.pdf

2.2. Non-Government Documents

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

[14] 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.

[15] 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

[16] RFC 3986, Uniform Resource Identifiers (URI): Generic Syntax, Network Working Group, January 2005.
https://tools.ietf.org/html/rfc3986

[17] Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language, W3C Recommendation, 26 June 2007.
http://www.w3.org/TR/wsdl20/

[18] 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/

[20] DCMI Metadata Terms, Dublin Core Metadata Initiative, 14 June 2012.
http://dublincore.org/documents/dcmi-terms/

[21] Aeronautical Information Exchange Model (AIXM) Release 5.1/5.1.1, EUROCONTROL/FAA, April 2016.
http://www.aixm.aero/page/aixm-51-511

[22] Weather Information Exchange Model (WXXM) Release 2.1, EUROCONTROL/FAA, 15 December 2017.
http://wxxm.aero/page/documents-0

[23] Flight Information Exchange Model (FIXM) Version 4.1.0, EUROCONTROL/FAA, 22 August 2013.
http://www.fixm.aero

[24] 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 in this document and the references cited herein, the text in 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 [15].

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

All terms used in this document are defined in the SWIM Controlled Vocabulary [1] along with information about terms’ sources and relationships to other terms.

3.3 Acronyms and Abbreviations

AIS	Aeronautical Information Services
AIXM	Aeronautical Information Exchange Model
AMS	Acquisition Management System
CONOPS	Concept of Operations
FAA	Federal Aviation Administration
FIXM	Flight Information Exchange Model
GRID	Global Registry Identifier
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
ISD	In Service Decision
JMS	Java Message Service
JMSDD	Java Messaging Service Description Document
NAS	National Airspace System
NSRR	NAS Service Registry/Repository
OGC	Open Geospatial Consortium
PO	Program Office
SLMP	Service Lifecycle Management Process

SOA	Service-Oriented Architecture
SOAP	Originally “Simple Object Access Protocol”; the full spelling is no longer used
SRD	Service Requirements Document
URI	Uniform Resource Identifier
UTF-8	8-bit Unicode Transformation Format
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 communications network 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 register all their services, as prescribed in this document, 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 Service Provider Policies

5.1.1 Service Lifecycle Policies

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

Lifecycle Stage	***Description***
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.

5.1.1.1 Proposed Stage Policies

a. All service providers SHALL initiate the registration process in the NSRR as described in section 5.1.3.1 of this document.

5.1.1.2 Definition Stage Policies

a. All service providers SHALL submit a Solution Concept of Operations (CONOPS) for the new service or an artifact equivalent to this document.

b. All service providers SHALL prepare a Service Requirements Document (SRD)[1] for the service as described in section 5.1.2.1 of this document.

c. All service providers SHALL upload the SRD to the NSRR.

d. All service providers SHALL enter the service metadata in the NSRR in accordance with section 5.1.3.2 of this document.

5.1.1.3 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 5.1.2.1 of this document.

Note: For the purposes of this document, all Open Geospatial Consortium (OGC)-compliant services are considered 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.

[1] The SWIM Governance Team is developing a new FAA standard 074, *Preparation of Service Description Documents (SRD)*, which will supersede FAA-STD-070, *Preparation of Web Service Requirements Documents (WSRD)* [3]. When preparing a service requirements document, the provider is advised to contact the SWIM Governance Team for the most current and appropriate version of the standard.

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 SHOULD prepare and upload to the NSRR a sample of data to be used for testing the service in a controlled environment.
f. All service providers SHALL augment the service metadata in the NSRR in accordance with section 5.1.3.3 of this document.

5.1.1.4 Verification Stage Policies

a. All service providers SHALL prepare and upload to the NSRR a Test Report describing the results of testing the service at the WSDL and message level.

5.1.1.5 Production Stage Policies

a. All service providers SHALL upload the ISD documentation to the NSRR.
b. To develop ISD documentation, the service providers are RECOMMENDED to use guidance and templates that can be found on the ISD Executive Secretariat webpage: https://my.faa.gov/org/linebusiness/ato/safety/isd.html.

5.1.1.6 Deprecated Stage Policies

a. If a service is planned to be deprecated, service providers SHALL provide a Deprecation Impact Analysis to SWIM Governance for review and approval.
b. In the Deprecation Impact Analysis, the service providers SHALL indicate the service retirement date.
c. All service providers SHALL upload the Deprecation Impact Analysis to the NSRR.

5.1.1.7 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.

5.1.2 Documentation Policies

5.1.2.1 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. SRD
3. WSDD or JMSDD
4. Deprecation Impact Analysis (deprecated services only)

5. Retirement Impact Analysis (retired services only)

b. All SRDs SHALL be prepared in accordance with FAA-STD-074, "Preparation of Service Requirements Documents" [3].[2]

c. All WSDDs SHALL be prepared in accordance with FAA-STD-065B, "Preparation of Web Service Description Documents" [2].

d. All JMSDDs SHALL be prepared in accordance with FAA-STD-073A, "Preparation of Java Messaging Service Description Documents" [4].

5.1.2.2 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 Definition Language1.1 Recommendation [18].

d. All XML service description documents SHALL conform to the structure and constraints specified in the WSDL 2.0 Specification [17].

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" [11].

f. All XML-based documents SHALL conform to the namespace policies described in section 5.1.5 of this document.

5.1.3 Service Registration Policies

This document asserts service 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-065B, "Preparation of Web Service Description Documents (WSDD)" [2] and FAA-STD-073A, "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.

[2] As noted previously, FAA-STD-074 will supersede FAA-STD-070 [3]. When preparing a service requirements document, the provider is advised to contact the SWIM Governance Team for the most current and appropriate version of the standard.

c. For each lifecycle stage identified in section 5.1.1 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 5.1.4) 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 the metadata to be entered in the NSRR at each lifecycle stage.

5.1.3.1 Proposed Stage

After SWIM Governance has worked with the service provider to establish a service name and service global registry identifier (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 brief description of the service.

c. All service providers SHALL identify a SWIM service category.

d. All service providers SHALL identify a service interface type.

e. All service providers SHALL identify a service criticality level.

f. All service providers SHALL provide a description of the service provider organization.

g. All service providers SHALL identify at least one point of contact.

h. All service providers MAY identify current or potential service consumers.

5.1.3.2 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 (QoS).

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.

5.1.3.3 Development Stage

a. All service providers SHOULD provide a description of the service 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 service fault messages.

e. All service providers SHALL provide a description of the data shared between providers and consumers.

f. All service providers SHOULD provide a description of the service bindings.

g. All service providers SHOULD provide a description of the service end points.

5.1.3.4 Verification Stage

No entries in the NSRR are required.

5.1.3.5 Production Stage

No entries in the NSRR are required.

Note: No changes to the service metadata are allowed at this stage. However, if the provider has sufficient reason for any change, he/she should contact an NSRR Administrator for assistance.

5.1.3.6 Deprecated Stage

No entries in the NSRR are required.

5.1.3.7 Retired Stage

No entries in the NSRR are required.

5.1.4 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. A waiver request form is available from SWIM Governance at https://www.faa.gov/air_traffic/technology/swim/governance/standards/media/FAA-SWIM-Governance-Policies-Waiver-Request-Template.pdf.
- **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.

5.1.5 Namespace Policies

- **a.** A declaration of a namespace in SWIM XML-based documentation SHALL follow the guidelines set forth in “Namespaces in XML 1.0” [24].
- **b.** A namespace identifier SHALL adhere to the generic URI syntax prescribed by RFC-3986 [16].
- **c.** A namespace URI identifier SHALL use the hypertext transfer protocol (HTTP) scheme (e.g., http://swim.faa.gov/fps).
- **d.** The values of the namespace URI identifier SHOULD be dereferenceable.
- **e.** 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.

5.1.6 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 exchanged across systems is understood in the same way by those systems as well as by 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 [20], FAA-STD-065B [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 [12].

5.1.7 Information Exchange Model Conformance 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 [21].
- **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 [22].
- **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 [23].
- **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 5.1.4 of this document.

5.1.8 Security Policies

- **a.** All SWIM-enabled programs SHALL comply with NIST Special Publication 800-95 "Guide to Secure Web Services" [9].
- **b.** All SWIM-enabled programs SHALL comply with FAA Order 1370.121 "FAA Information Security and Privacy Program & 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 [13].

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) [14].

5.1.9 Change Management Policies

The intrinsically agile nature of SWIM as a multi-organizational service-oriented framework places special emphasis on the need for managing changes to services and service-related artifacts. These changes usually originate from new business requirements, constantly evolving technological solutions, or modifications or upgrades to a common infrastructure.

To maintain interoperability among independently developed components, SWIM implementers must be cognizant of a) how the changes will impact existing (and potentially future) service consumers and b) how the changes should be communicated to the consumers to avoid potential interruptions of interactions with services.

This document recognizes three types of changes based on their significance:

1) **Major changes** - Changes or updates that are not backward-compatible; that is, they force a consumer agent to change in order to use the new version of the service. It is said that these changes "break" a consumer agent.
2) **Minor changes** - Changes that allow a consumer agent to continue to use the existing version of the service (they do not "break" the consumer agent), although the consumer agent is unable to use or is unaware of the new features. These changes are considered backward-compatible (e.g., a new capability, new optional request parameters).
3) **Patches** - Backward-compatible error corrections that do not affect in any way interaction between service and consumer agent (e.g., fixing a bug in a software, correcting a typographical error in an XML schema document).

Figure 1 below illustrates how the significance of these types of changes affects the usage and versioning of a typical service.

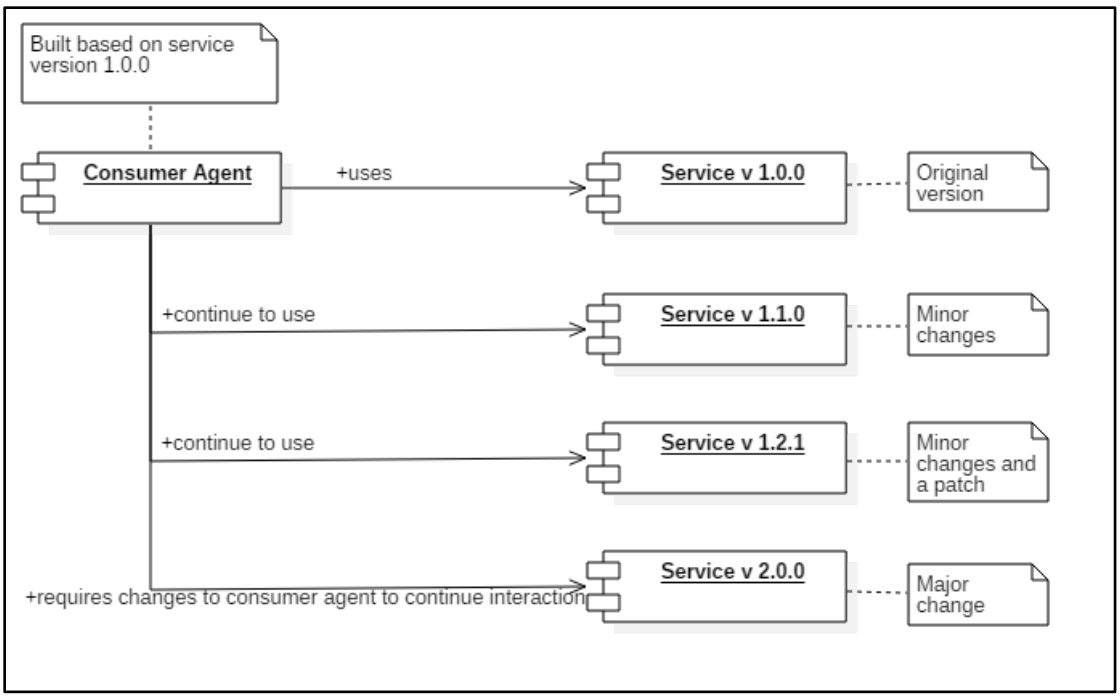

Figure 1 Example of applying changes of increasing significance

a. The service provider SHALL notify the SWIM Governance and Engineering leads about planned modifications to the service.

b. The service provider SHALL notify known service consumers about changes to the service.

c. The service provider SHALL create a notification in the NSRR describing the purpose, character and potential impact of changes and indicating the target date on which the new version is expected to become operational.

d. If the changes planned for a service are identified as *major*, the service provider SHALL notify service consumers as prescribed in policies "**b**" and "**c**" at the beginning of the planning stage or six months prior to the target date on which the new version will become operational, whichever comes first.

Figures 2 and 3 below show the menu command used to create a notification followed by an example of the notification itself. The NSRR will send the notification in the form of an email to all consumers who have registered their intent to consume the service.

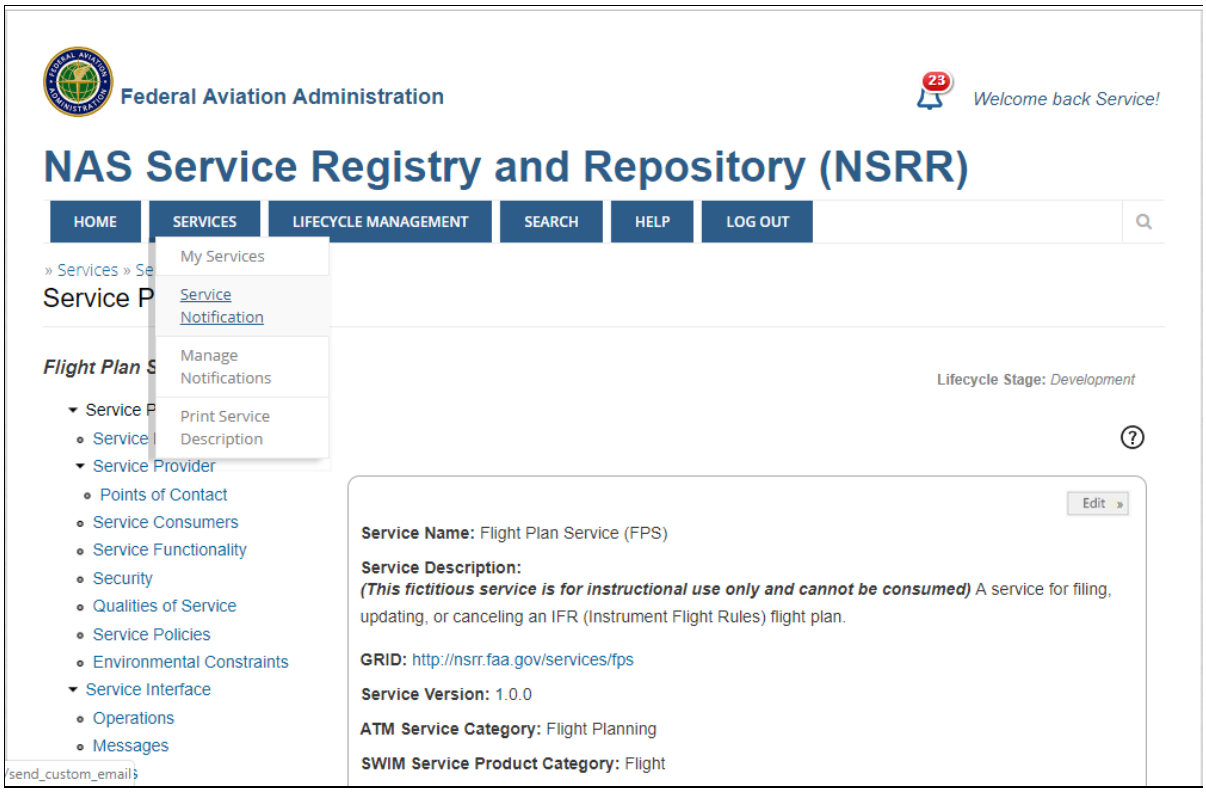

Figure 2 Example of invoking custom notifications module in the NSRR

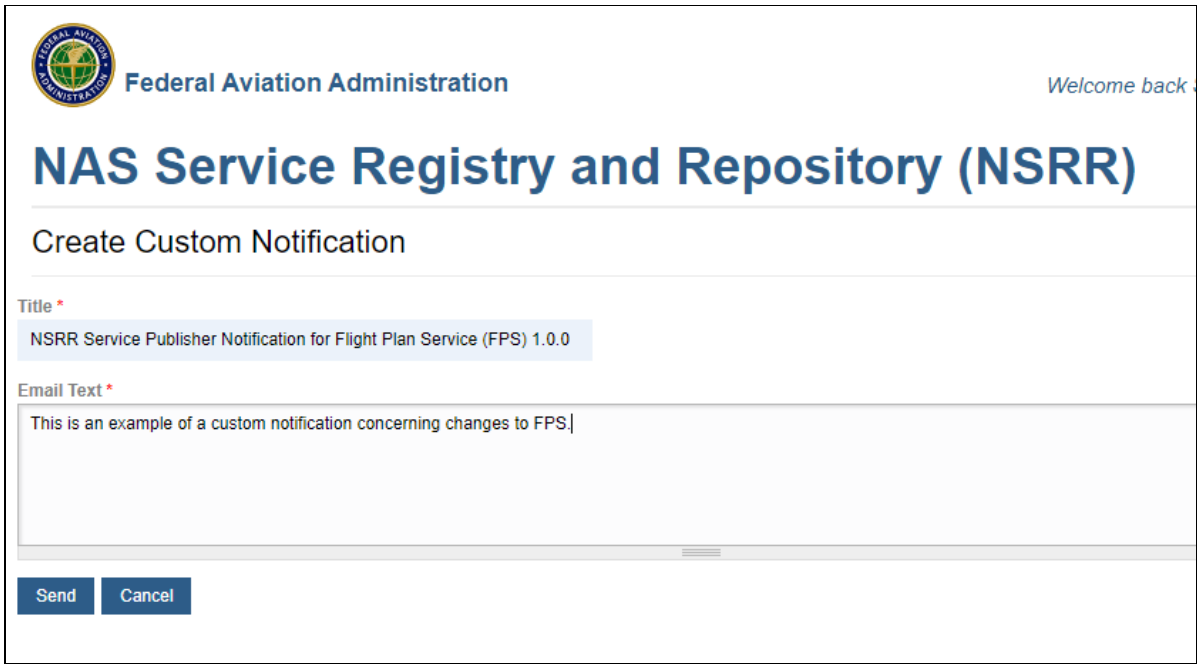

Figure 3 Example of creating a custom notification

5.1.9.1 Versioning Policies

In a service-centric environment such as SWIM, service versioning is a critical factor in managing changes to services or service-related artifacts and mitigating the impact of these changes on service consumers.

In SWIM, versioning is defined as “the process of managing multiple releases of a service or its artifacts for the purpose of managing the service’s evolution” [10].

a. Each release of a SWIM service or service-related artifact will be versioned according to the guidance set forth in Software Specification SWIM-005 "Artifacts Versioning for SWIM-enabled Services", Version 1.0.0 [10].
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. No retroactive application of these guidelines is envisioned for currently published services’ versions. Existing version identifiers will be exempt.

5.2 Service Consumer Policies

In SWIM, a service consumer is defined as “an organization that seeks to satisfy a particular need through the use of capabilities offered by means of a service” [1]. However, in the context of the NSRR, the term *service consumer* is often used to describe a person that is affiliated with or employed by a consumer organization. In this section, we will use the term *service consumer* in the latter sense.

a) Each service consumer, current or prospective, SHALL request an account in the NSRR.
b) The service consumer SHALL indicate on the NSRR account request form whether he or she is or plans to be a service consumer.
c) The service consumer SHALL indicate, in the Note field of the account request form shown in Figure 4 below, what service(s) he or she consumes or intends to consume.

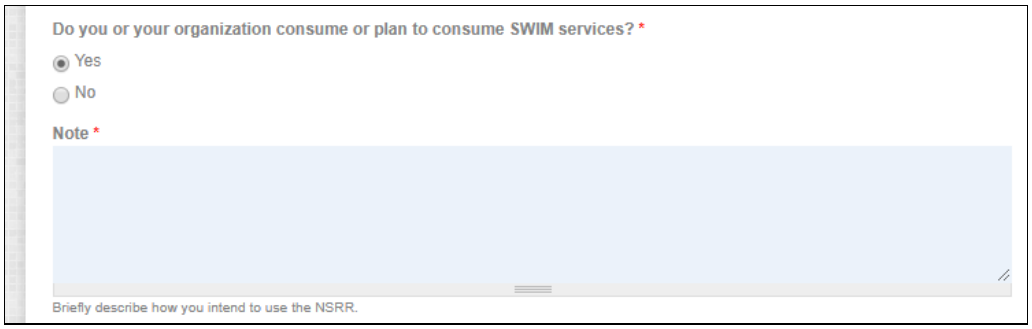

Figure 4 NSRR account request form excerpt

APPENDIXES

Appendix A. Service Provider Checklist

Lifecycle Stage	Type	Description	Comment
Proposed	NSRR entry	Service version	The service version shall be identified and entered in NSRR.
Proposed	NSRR entry	Service Description	A brief description of the service shall be entered in NSRR.
Proposed	NSRR entry	Service Provider Information	Information about the provider organization shall be entered in NSRR.
Proposed	NSRR entry	Service Provider Point of Contact	At least one PoC shall be entered in NSRR.
Proposed	NSRR entry	Service Consumers	Optional; information about current or proposed consumers.
Proposed	NSRR entry	SWIM Service Category	At least one value shall be selected in NSRR.
Proposed	NSRR entry	Service Criticality Level	One value shall be selected in NSRR.
Proposed	NSRR entry	Service Interface Type	One value shall be selected in NSRR.
Definition	Document	Concept of Operations	Service's Concept of Operations (CONOPS). Submit to NSRR.
Definition	Document	Service Requirements Document (SRD)	Service Requirements Document. Submit to NSRR.
Definition	NSRR entry	Service Functionality	Description of the Service Functionality shall be added to NSRR.
Definition	NSRR entry	Qualities of Service	Quality of Service parameters should be added to NSRR.
Definition	NSRR entry	Security Mechanisms	Description of the service's Security mechanisms should be added to NSRR.
Definition	NSRR entry	Service Policies	Description of the Service Policies should be added to NSRR.
Definition	NSRR entry	Operations	Operations description should be added to NSRR. Note: may not be applicable in JMS-based interfaces.
Definition	NSRR entry	Messages	Messages description shall be added to NSRR.
Development	NSRR entry	Environmental Constraints	Environmental Constraints should be added to NSRR.
Development	NSRR entry	Message Headers	Message header description should be added to NSRR where applicable.
Development	NSRR entry	Message Payloads	Message payload description shall be added to NSRR.
Development	NSRR entry	Faults	Faults description should be added to NSRR.
Development	Document	XML Schema Definitions for Types	Shall be uploaded to NSRR in the Service Documents section.
Development	Document	Data Description document	Data Description Document of unspecified format (optional). Should be uploaded to NSRR in the Service Documents section.

Development	NSRR entry	Data	Data descriptions shall be added to NSRR if no data description document exists.
Development	NSRR entry	Bindings	Bindings description should be added to NSRR.
Development	NSRR entry	End Points	End points description should be added to NSRR.
Development	Document	WSDL File	WSDL (when applicable) shall be validated in NSRR and subsequently uploaded in the Service Documents section.
Development	Document	Web Services Description Document (WSDD) or Java Messaging Service Description Document (JMSDD)	Generate the document and update as necessary (e.g., obtain signatures). Refer to FAA-STD-065B for WSDD and to FAA-STD-073A for JMSDD. Submit to NSRR.
Development	Document	Data Sample for Service Verification	Submit to NSRR for uploading to the Service Documents section.
Verification	Document	Test Report	Submit to NSRR for uploading to the Service Documents section.
Production	Document	In Service Decision (ISD) documentation	Submit to NSRR for uploading to the Service Documents section.
Deprecation	Document	Deprecation Impact Analysis	Submit to NSRR for uploading to the Service Documents section.
Retired	Document	Retirement Impact Analysis	Submit to NSRR for uploading to the Service Documents section.

Appendix B. Example of a Waiver Request

Note: this example is non-normative.

SWIM Governance Policies Waiver Request

FOR USE BY REQUESTER

Date of Request: August 21, 2020
Requester's Organization: En Route Services Modernization Group (ESMG)
Requester's Name: John D. Doe, ATO-X ESMG Manager
Requester's Telephone Number: (609) 444-5555
Requester's Email: **joe.doe@faa.gov**

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:

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 3.1, for the following reason:
During design of FPS version 1.0, the FIXM wasn't mature and ESMG 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, 2022.
Date or condition upon which this waiver can be expected to expire: _March 1, 2022_

FOR USE BY SWIM GOVERNANCE

Resolution of Request:

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.

Waiver Granted (X) / Disapproved ( ) on: September 4, 2020

Signed: Mark Kaplun, SWIM Governance Lead (mark.kaplun@faa.gov)