

System Wide Information Management (SWIM)

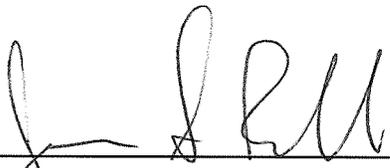
Governance Policies



Version 2.0

March 12, 2014

SIGNATURE PAGE



Jim Robb
SWIM Program Manager

3/12/2014

Date



Mark Kaplun
SWIM Governance Lead

3/12/2014

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	03/12/2014	Modified and changed Governance policies to accommodate changes in NAS SWIM environment.

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..... 7
 - 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 10
- 4 GENERAL POLICIES 13
- 5 DETAILED POLICIES..... 13
 - 5.1 Processing Policies 13
 - 5.1.1 SOA Suitability Assessment Policies..... 13
 - 5.1.2 Service Provider Lifecycle Policies 14
 - 5.1.2.1 Service Provider Proposed Stage Policies 14
 - 5.1.2.2 Service Provider Definition Stage Policies..... 15
 - 5.1.2.3 Service Provider Development Stage Policies..... 15
 - 5.1.2.4 Service Provider Verification Stage Policies..... 16
 - 5.1.2.5 Service Provider Production Stage Policies..... 16
 - 5.1.2.6 Service Provider Deprecated Stage Policies..... 16
 - 5.1.2.7 Service Provider Retired Stage Policies..... 16
 - 5.1.3 Service Consumer Policies 16
 - 5.1.4 Service Documentation Policies..... 16
 - 5.1.5 Service Registration Policies 18
 - 5.1.6 Waiver Policies 18
 - 5.2 Technical Policies 18
 - 5.2.1 Service Description Policies 18

- 5.2.2 Semantic Interoperability Policies 19
- 5.2.3 Canonical Model Usage Policies..... 19
- 5.3 Security Policies 20
- APPENDIXES 21
- Appendix A. Service Provider Checklist 21
- 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 the resources, assets, and processes that are enabled and/or supported by the Federal Aviation Administration (FAA) System Wide Information Management (SWIM) program.

1.1. Background

The National Airspace System (NAS) is in the process of evolving 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/about/office_org/headquarters_offices/ato/service_units/techops/atc_comms_services/swim/governance/standards/
- [3] FAA-STD-070, Preparation of Web Service Requirements Documents, 12 July 2012.
http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/atc_comms_services/swim/governance/standards/
- [4] FAA-STD-073, Preparation of JAVA Message Service Description Documents, 30 September 2013.
http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/atc_comms_services/swim/governance/standards/
- [5] FAA-STD-063, XML Namespaces, 1 May 2009.
<http://www.tc.faa.gov/its/worldpac/standards/faa-std-063.pdf>
- [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>
- [9] FAA Order 1370.98, ATO Information Technology Infrastructure Requirements for Non-FAA Connectivity, 17 April 2007.
http://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/15195
- [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>.

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/javase/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/>
- [18] XML Schema Part 1: Structures Second Edition, W3C Recommendation, 28 October 2004.
<http://www.w3.org/TR/xmlschema-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] SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), W3C Recommendation, 27 April 2007.
<http://www.w3.org/TR/soap12-part1/>

- [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 5.1, EUROCONTROL/FAA, 1 February 2010.
http://www.aixm.aero/public/standard_page/download.html
- [24] Weather Information Exchange Model (WXXM) Version 1.1.1, EUROCONTROL/FAA, 19 March 2010.
<https://wiki.ucar.edu/display/NNEW/WXXM>
- [25] Flight Information Exchange Model (FIXM) Version 2.0, EUROCONTROL/FAA, 22 August 2013.
http://www.fixm.aero/fixm_20

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: terms labeled "CV" may be found in the SWIM Controlled Vocabulary [1] along with information about terms' sources and relationships to other terms.

<i>Business Service</i>	A business function or capability that is offered as a service . (CV)
<i>Consumer Agent</i>	A software agent that is designed to interact with a service in order to request that a task be performed on behalf of its owner, the service consumer . (CV)
<i>Java Message Service (JMS)</i>	A Java-based application programming interface (API) that provides a common way for Java programs to create, send, receive, and read an enterprise messaging system's messages. (CV)
<i>NAS Service Registry/Repository (NSRR)</i>	A SWIM-supported capability for making services visible, accessible, and understandable across the NAS. NSRR supports a flexible mechanism for service discovery, an automated policies-based way to manage services throughout the services lifecycle, and a catalog for relevant artifacts. (CV)
<i>On-Ramping</i>	The process of configuring and enabling a connection between a service or consumer agent and the NAS Enterprise Messaging Service (NEMS) .
<i>Organization</i>	A unique framework of authority within which a person or persons act, or are designated to act, towards some purpose. Any department, service, or other entity within an organization which needs to be identified for information exchange. (CV)
<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>Service</i>	A mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description . (CV)
<i>Service Consumer</i>	An organization that seeks to satisfy a particular need through the use of capabilities offered by means of a service . (CV)
<i>Service Provider</i>	An organization that offers the use of capabilities by means of a service . (CV)

<i>Service Registry</i>	An enabling infrastructure that uses a formal registration process to store, catalog, and manage metadata relevant to a service . A registry supports the search, identification, and understanding of resources, as well as query capabilities. (CV)
<i>Service-Oriented Architecture (SOA)</i>	A paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. A SOA provides a uniform means to offer, discover, interact with, and use capabilities to produce desired effects consistent with measurable preconditions and expectations. (CV)
<i>SOA Governance</i>	The application of policies, rules, and standards needed to ensure that all of the independent SOA-based efforts (whether in the design, development, deployment, or operations of a service) come together to meet enterprise requirements.
<i>SOA-Based</i>	Something that is designed, developed, or operated according to principles of Service-Oriented Architecture .
<i>SWIM-Enabled Program</i>	A program that provides or consumes, or intends to provide or consume, NAS SOA-based services and which uses SWIM common computing and infrastructure assets.
<i>Taxonomy</i>	A controlled list of well-defined concepts organized into a hierarchical structure.
<i>Web Service</i>	A platform-independent, loosely-coupled software component designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format. Other systems interact with the Web service in a manner prescribed by its description by means of XML-based messages conveyed using Internet transport protocols in conjunction with other Web-related standards. (CV)

3.3 Acronyms and Abbreviations

<i>AIM</i>	Aeronautical Information Management
<i>AIS</i>	Aeronautical Information Services
<i>AIXM</i>	Aeronautical Information Exchange Model

AMS	Acquisition Management System
API	Application Programming Interface
BCD	Baseline Change Decision
CONOPS	Concept of Operations
ESB	Enterprise Service Bus
EES	Enterprise Engineering Services
FAA	Federal Aviation Administration
FID	Final Investment Decision
FIXM	Flight Information Exchange Model
FNTB	FTI National Test Bed
FPRD	Final Program Requirements Document
FTI	FAA Telecommunications Infrastructure
HTTP	Hypertext Transfer Protocol
IARD	Investment Analysis Readiness Decision
IID	Initial Investment Decision
IPR	Initial Program Requirements
ISD	In Service Decision
ISPD	Implementation Strategy and Planning Document
JMS	Java Message Service
JRC	Joint Resources Council
JMSDD	Java Messaging Service Description Document
MOA	Memorandum of Agreement
NAS	National Airspace System
NEMS	NAS Enterprise Messaging Service
NSRR	NAS Service Registry/Repository
OGC	Open Geospatial Consortium
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 services and/or [consumer agents](#) discoverable, searchable, and retrievable by registering them in the [NAS Service Registry/Repository \(NSRR\)](#).
- 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 (EES) Assessment submitted to the JRC Secretariat

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

5.1.2 Service Provider 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 provider](#) lifecycle stages. Policies relevant to each stage are described more fully in corresponding subsections following Table 1.

Table 1 Service Provider 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 Service Provider 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 seeking enablement by SWIM SHALL request creation of a user account in the [NSRR](#) for the program's point of contact
- d. All programs seeking enablement by SWIM as Service Providers and/or [Service Consumers](#) SHALL submit a request to SWIM Governance for creation of an [Organization](#) entity in the NSRR.
- e. The proposed Service Providers SHALL enter the following information in the NSRR:
 1. Service URI (namespace) that uniquely identifies the service (see FAA-STD-063 "XML Namespaces" [\[5\]](#) for information on assigning namespaces)
 2. Service name consisting of the full name spelled out followed by the acronym, if any, by which the service is commonly recognized within FAA
 3. Brief description of the service

For information about service registration policies, see [section 5.1.5](#) of this document.

5.1.2.2 Service Provider Definition Stage Policies

- a. All Service Providers SHALL modify the following documents to accommodate requirements for compliance with SWIM Governance policies:
 1. Initial Implementation Strategy and Planning Document (ISPD)
 2. Final Program Requirements Document (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 proposed service. See [section 5.1.4](#) of this document for more information on WSRD preparation.
- e. All Service Providers SHALL upload the WSRD to the NSRR prior to FID.

5.1.2.3 Service Provider 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) 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. All Service Providers 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.

5.1.2.4 Service Provider Verification Stage Policies

- a. All Service Providers SHALL prepare an Operational Test Plan.

5.1.2.5 Service Provider 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 upload the ISD action plan to the NSRR.

5.1.2.6 Service Provider 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 Service Provider 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 Service Consumer Policies

This section specifies policies for [organizations](#) or programs that intend to consume services provided in the context of SWIM implementations. This document asserts two types of [Service Consumers](#): *internal* (FAA organizations), and *external* (FAA business partners).

- a. All Service Consumers, internal as well as external, SHALL register in the NSRR.
- b. All Service Consumers SHALL discover business services for consumption via the NSRR.
- c. All Service Consumers SHALL request service consumption via the NSRR.
- d. All Service Consumers SHALL receive from the Service Provider an acknowledgement of their service consumption request.
- e. All Service Consumers SHALL develop a consumer agent consistent with the service information as presented in the service description document (WSDD or JMSDD).
- f. All Service Consumers SHALL connect to the FAA Telecommunication Infrastructure (FTI) National Test Bed (FNTB) in order to complete the NAS Enterprise Messaging Service (NEMS)/FNTB Consumer Qualification procedure prior to service consumption in the FAA Operational Network.
- g. All Service Consumers SHALL provide official notification of ending service consumption to the Service Provider.

5.1.3.1 External Service Consumer Policies

In addition to the policies listed in section 5.1.3, external Service Consumers shall also comply with the following policies:

- a. All external Service Consumers SHALL comply with NAS Data Release policies specified in FAA Order 1370.98, "ATO Information Technology Infrastructure Requirements for Non-FAA Connectivity" [9].
- b. All external Service Consumers SHALL enter into a joint agreement with FAA via a Memorandum of Agreement (MOA). Note: this is a multistep process which may take 2-3 months to complete.
- c. All external Service Consumers SHALL attach the MOA to the service consumption request submitted via the NSRR.

5.1.3.2 Internal Service Consumer Policies

In addition to the policies listed in section 5.1.3, internal Service Consumers shall also comply with the following policies:

- a. All internal Service Consumers shall complete a SOA Assessment as part of the Enterprise Infrastructure Services (EES) process.
- b. All internal Service Consumers seeking approval by the JRC SHALL provide the following documents to SWIM Governance for review:
 1. Solution CONOPS
 2. fPRD
 3. ISPD
- c. All internal Service Consumers who are not receiving funding through the JRC SHALL provide a CONOPS or equivalent document describing their SWIM service consumption operations.

5.1.4 Service Documentation Policies

- a. All Service Providers SHALL provide SWIM Governance with the following documents for review and subsequent uploading to the NSRR:
 1. SOA Suitability Scorecard
 2. Request Form for registering provider's organization in the NSRR
 3. Copy of the CONOPS document
 4. WSRD
 5. WSDD or JMSDD
- 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].

5.1.5 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](#).

- a. All Service Providers SHALL register their service in the NSRR.
- b. All Service Providers SHALL update service registration data in the NSRR throughout the service lifecycle as prescribed in [section 5.1.2](#) of this document.
- c. All Service Providers SHALL upload the following artifacts to the NSRR at the appropriate lifecycle stages as prescribed in [Appendix A](#) of this document:
 1. SOA Suitability Scorecard
 2. Copy of CONOPS document
 3. WSRD
 4. WSDD or JMSDD
 5. WSDL document and data type definitions

5.1.6 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 Technical Policies

5.2.1 Service Description 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].
- c. All Service Providers of SWIM-enabled Web Services SHALL provide a formal specification of the Web Service interface using syntax prescribed by WSDL 2.0 [16]. Other structured data service messages SHALL be described using the XML Schema Definition (XSD) [17].
- d. All Service Providers SHALL validate all WSDL files in the NSRR before proceeding with [on-ramping](#) activities.
- e. All Service Providers SHALL use XML Schema 1.0 Recommendation [18] as the basis of user-defined data types and structures.
- f. All Service Providers using XML for data exchange SHALL use XML version 1.0 [19].
- g. All Service Providers SHALL use SOAP protocol version 1.2 [20] as a message exchange protocol.
- h. All Service Providers implementing a JMS client SHALL deploy the following software:
 1. Oracle WebLogic JMS version 10 or later
 2. Apache ActiveMQ version 5 or later
- i. When it is deemed necessary by a Service Provider to use software other than that specified in policy 'h.', the Service Provider SHALL obtain a waiver from SWIM Governance as described in [section 5.1.6](#) of this document.

5.2.2 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 employing taxonomies, all SWIM-enabled programs SHALL use the common set of taxonomies as identified by FAA and/or SWIM.
- b. When developing glossaries for SWIM-related documentation, all SWIM-enabled programs SHALL default to the terms defined in the SWIM Controlled Vocabulary [1].

5.2.3 Canonical Model Usage 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 deploy the Aeronautical Information Exchange Model (AIXM) [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 deploy the Weather Exchange Model (WXXM) [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 deploy the Flight Information Exchange Model (FIXM) [25].
- d. To use exchange models other than AIXM, WXXM, or FIXM in situations described in policies ‘a’, ‘b’, or ‘c’ respectively, all Service Providers SHALL obtain a waiver from SWIM Governance as described in [section 5.1.6](#) 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].

APPENDIXES

Appendix A. Service Provider Checklist

Lifecycle Stage	Type	Description	Comment
Proposed	Deliverable	SOA Suitability Scorecard	SOA suitability memo and score is developed as part of the SOA Suitability Assessment. The SOA Suitability Assessment is conducted by EES for ARB. Submit to NSRR.
	Deliverable	Organization Entity Request Form	A form completed by the Program to provide SWIM Governance with necessary information to create an Organizational entity for the Program in NSRR. Submit to SWIM Governance.
	Checkpoint	Organization URI	An Organization URI registered by an FAA registration authority. Refer to FAA-STD-063 [5].
	Checkpoint	IARD and/or IID	Service Provider passed AMS Investment Analysis Readiness Decision (IARD) and Initial Investment Decision (IID). Applicable only to Service Providers in the AMS.
	Deliverable	Concept of Operations	Solution CONOPS is an AMS deliverable. Submit to NSRR.
Definition	Checkpoint	FID	Service Provider passed AMS Final Investment Decision. Applicable only to Service Providers in the AMS.
	Deliverable	Web Service Requirements Document (WSRD)	Provides a series of requirements for the Program's Service interface. Refer to FAA-STD-70. Submit to NSRR.
Development	Deliverable	Web Services Description Document (WSDD) or Java Messaging Service Description Document (JMSDD)	Provides technical specification regarding interface specifics of the SOA Service. Refer to FAA-STD-065A or FAA-STD-073. Submit to NSRR.
	Deliverable	XML Schema Definitions for Types	A description of constraints, structure, and content of the data products of the SOA Service. Refer to FAA-STD-065A. Submit to NSRR.
	Deliverable	Web Services Description Language (WSDL)	An XML description for defining the functionality offered by the Web Service. Not applicable to JMS Services. Submit to NSRR.
	Deliverable	Enterprise Engineering Service and Cost Agreement (EESCA)	Program Level agreement between EES and program inclusive of SWIM service requirements and costing (formerly known as TPP). Submit to EES.
Verification	Checkpoint	Test Plan/ Producer Review	SWIM T&E Team will review and approve test plans and procedures specifically related to SWIM requirements.
Production	Checkpoint	ISD Action Plan	Submit to NSRR. ISD Action Plan describes deployment activities such as product installation and certification for operational use. ISD Action Plan supports ISD in the AMS.
	Deliverable	Memorandum of Agreement (MOA)	MOA for each non FAA consumer, submit to NSRR for each external Service Consumer.
Deprecation	Deliverable	Deprecation Impact Analysis	Submit to NSRR.
Retired	Deliverable	Retirement Impact Analysis	Submit to 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>	